Universidad Peruana los Andes

Facultad de Ingeniería

Escuela Profesional de Ingeniería de Sistemas y Computación

Tesis

PORTAL CAUTIVO PARA ADMINISTRAR LA SEGURIDAD DE DATOS DE LA RED INALAMBRICA DEL IESTP SAN PEDRO

Para optar el Título Profesional de Ingeniero de Sistemas y Computación

Autor

Christian Ayala Bendezu

Asesor

Mg. Raúl Enrique Fernández Bejarano

Ing. Alex Albert Zuñiga Manrique

Línea de Investigación Institucional

Ingeniería de Infraestructura Tecnológica

Huancayo - Perú

2022

HOJA DE CONFORMIDAD DEL JURADO

_____

DR. RUBEN DARIO TAPIA SILGUERA

PRESIDENTE

_____

MG. CAROL JOSEFINA FABIAN CORONEL

JURADO 01

_____

MG. WALTER DAVID ESTARES VENTOCILLA

JURADO 02

_____

MG. YUDITH MARLENI ECHAVIGURIN TORRES

JURADO 03

_____

MG. LEONEL UNTIVEROS PEÑALOZA

SECRETARIO DOCENTE

DEDICATORIA

Dedico este trabajo a mi familia, lo más importante en este mundo, en especial a mis hermanos, hijos, padres por su gran esfuerzo brindado a lo largo de los años.

AGRADECIMIENTO

Debo expresar mi sincero agradecimiento a quienes hicieron lo posible para culminar con esta etapa importante de mi existencia.

A MIS PADRES

Edilberto, desde el cielo y Digna, por su gran apoyo, en todos los aspectos

A MIS HIJOS

Por ser la motivación a seguir adelante

A MI CASA DE ESTUDIOS

Por contribuir con mi enseñanza para mi formación profesional y actuar de forma competitiva y de calidad.

A MIS MAESTROS Y ASESORES

Por brindarme el conocimiento profesional. El cual demuestro en el proyecto.

CONSTANCIA 038

DE SIMILITUD DE TRABAJOS DE INVESTIGACIÓN POR EL SOFTWARE DE PREVENCIÓN DE PLAGIO TURNITIN

La Dirección de Unidad de Investigación de la Facultad de Ingeniería, hace constar por la presente, que el informe final de tesis titulado:

"PORTAL CAUTIVO PARA ADMINISTRAR LA SEGURIDAD DE DATOS DE LA RED INALÁMBRICA DEL IESTP SAN PEDRO"

Cuyo autor(es) : Christian, Ayala Bendezu

Facultad : Ingeniería

Escuela Profesional : Ingeniería de Sistemas y Computación

Asesor(a) : Mg. Raúl Enrique Fernández Bejarano
Ing. Alex Albert Zuñiga Manrique

Que, fue presentado con fecha 27.01.2023 y después de realizado el análisis correspondiente en el software de prevención de plagio Turnitin con fecha 30.01.2023; con la siguiente configuración de software de prevención de plagio Turnitin:

- [X] Excluye bibliografía.
- [X] Excluye citas.
- [X] Excluye cadenas menores de a 20 palabras.
- [ ] Otro criterio (especificar)

Dicho documento presenta un porcentaje de similitud de **05 %**. En tal sentido, de acuerdo a los criterios de porcentajes establecidos en el artículo N°11 del Reglamento de uso de software de prevención de plagio, el cual indica que no se debe superar el **30%**. Se declara, que el trabajo de investigación: si contiene un porcentaje aceptable de similitud. Observaciones: ninguna.

En señal de conformidad y verificación se firma y sella la presenta constancia.

Huancayo 31 de Enero del 2023

UNIVERSIDAD PERUANA LOS ANDES
DIRECCIÓN DE LA UNIDAD DE INVESTIGACIÓN
FACULTAD DE INGENIERÍA

Dr. Santiago Zevallos Salinas
Director de la Unidad de Investigación

CONTENIDO

CONTENIDO DE FIGURAS

CONTENIDO DE TABLAS

RESUMEN

La implementación del portal cautivo para administrar la seguridad de datos, ya que se requiere que los usuarios se autoricen en el servidor antes de conectarse a la red inalámbrica, los portales cautivos se usan para asegurar la red, proporcionar información sobre la red y controlar el tráfico de usuarios. El presente estudio aborda la problemática ¿De qué manera influye el Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO? para ello se plantea el objetivo general fue determinar de qué manera influye el Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO; en respuesta al problema planteado se formula la hipótesis "El Portal Cautivo influye significativamente para administrar la seguridad de datos de la Red Inalámbrica del IESTP San Pedro**".** Se utilizo la siguiente metodología: el método de investigación es el Científico, el tipo de investigación es la aplicada, el alcance de la investigación en el nivel explicativo, el diseño de la investigación es el diseño pre experimental con pre test y post test, la población del estudio es de 256 usuarios y la muestra es de 154 usuarios. La técnica que se utiliza es la observación y los instrumentos son ficha de observación, el software Nessus y el Packet Loss. Se concluye, que en esta investigación se determinó la influencia del Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP San Pedro, después de obtener resultados satisfactorios de los indicadores de estudio, se concluye que la implementación del portal cautivo mejora significativamente la administración de la seguridad de datos de la red inalámbrica del IESTP San Pedro.

PALABRAS CLAVE: Portal Cautivo, Seguridad de datos, red inalámbrica, PFSense.

ABSTRACT

Captive portal implementation to manage data security, since users are required to authorize themselves on the server before connecting to the wireless network, captive portals are used to secure the network, provide information about the network, and control the user traffic. The present study addresses the problem: How does the Captive Portal influence to manage the data security of the Wireless Network of the IESTP SAN PEDRO? For this, the general objective was to determine how the Captive Portal influences to manage the data security of the Wireless Network of the IESTP SAN PEDRO; In response to the problem raised, the hypothesis "The Captive Portal significantly influences to manage the data security of the Wireless Network of the IESTP San Pedro" is formulated. The following methodology was used: the research method is Scientific, the type of research is applied, the scope of the research at the explanatory level, the research design is the pre-experimental design with pre-test and post-test, the Study population is 256 users and the sample is 154 users. The technique used is observation and the instruments are observation sheet, Nessus software and Packet Loss. It is concluded that in this investigation the influence of the Captive Portal was determined to manage the data security of the IESTP San Pedro Wireless Network, after obtaining satisfactory results of the study indicators, it is concluded that the implementation of the captive portal improves significantly. data security administration of the IESTP San Pedro wireless network.

KEYWORDS: Captive Portal, Data security, wireless network, PFSense.

INTRODUCCIÓN

La presente investigación busca determinar de qué manera influye el portal cautivo en la administración de la seguridad de datos en la red inalámbrica del IESTP San Pedro, entiéndase por administración de seguridad de datos a la gestión y monitoreo constante de los recursos de la red. Los usuarios tienen acceso a la red inalámbrica sin ningún control es decir no existe un control de usuarios, tampoco las páginas web se encuentran restringidas. Las características fundamentales de la seguridad informática son la confiabilidad, disponibilidad e integridad. Para analizar esta problemática es fundamental mencionar las causas. Una de ellas es el uso indiscriminado de los recursos de la red. Se entiende por el uso indiscriminado de la red inalámbrica, que los usuarios que se conectan a la red inalámbrica no tienen una correcta administración de las cuentas de los usuarios, también que no existe una administración y gestión del acceso a las diferentes páginas web, por lo tanto, no existe una administración optima de la red priorizando el tráfico de la información.

Este trabajo de investigación de realizo por el interés de conocer el por qué la administración de seguridad informática es muy importante, ya que el mal manejo de la información puede tener consecuencias muy delicadas para los usuarios como robo y mal uso de dicha información. Por otra parte, se puede aportar datos cuantitativos con el objeto de establecer un precedente para posteriores trabajos de investigación en el ámbito de la seguridad informática en una red inalámbrica.

La metodología de la investigación que se plantea utilizar es el método científico, tipo aplicada, nivel explicativo, diseño pre experimental, con la utilización del instrumento de fichas de observación, Nessus y Packet Loss Test para la recolección datos y para su posterior análisis, la población estuvo conformada por 256 usuarios con una muestra de 154 usuarios, estos usuarios son los estudiantes, personal administrativo y docentes del ISTP San Pedro. Para el procesamiento de la información se utilizó el programa SPSS.

Se busca alcanzar los siguientes objetivos: Identificar de qué manera influye el Portal Cautivo para administrar la confidencialidad de datos en la Red Inalámbrica; Identificar de qué manera influye el Portal Cautivo para administrar la disponibilidad de datos en la Red Inalámbrica; Identificar de qué manera influye el Portal Cautivo para administrar la integridad de datos en la Red Inalámbrica.

Esta investigación está compuesta de seis capítulos:

Primer capítulo: denominado planteamiento del problema de investigación donde se muestra el planteamiento y formulación del problema, justificación de la investigación, limitaciones y objetivos general y específicos.

Segundo capítulo: denominado Marco teórico, donde se detallan los antecedentes nacionales e internacionales, el marco conceptual, definición de términos, hipótesis general y específicos y la operacionalización de las variables de la investigación.

Tercer capítulo: denominado Hipótesis, en la cual tenemos la hipótesis general, El Portal Cautivo influye significativamente para administrar la seguridad de datos de la Red Inalámbrica del IESTP San Pedro, por otro lado, definimos las dos variables tanto independiente como dependiente, también realizamos la operacionalización de variables.

Cuarto capítulo: denominado metodología de la investigación, en la cual se desarrolla el método de la investigación, tipo de investigación, nivel de investigación, diseño de la investigación, población, muestra, técnicas e instrumentos de recolección de datos, procesamiento de la información, finalmente las técnicas y análisis de datos.

Quinto capítulo: denominado administración resultados, se define la descripción del diseño y resultados se realiza el análisis descriptivo de los datos que se obtuvieron en el pre test y post test, se realiza la contrastación de las hipótesis.

Sexto Capitulo: denominado análisis y discusión de resultados, se define la discusión de resultados con los datos obtenidos por los indicadores comparando con los antecedentes.

Finalmente se define las conclusiones, recomendaciones, referencias bibliográficas, por último, se considera los anexos utilizados en el proyecto de investigación.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

Las organizaciones enfrentan frecuentemente desafíos de seguridad informática al intentar acceder a la información mediante redes inalámbricas. Según los datos recogidos, 30.000 sitios son hackeados a diario, el 64% de las compañías ha sufrido al menos un intento de ciberataque y cada 39 segundos se completa un ataque en alguna parte de la empresa. Además, 23.000 ataques DDoS tienen lugar cada día, y el 91% de los delitos informáticos emplean mensajes de correo electrónico como vectores de propagación (KASPERSKY 2022).

Las personas que se conectan a redes WiFi públicas deberían ser conscientes de los riesgos de seguridad que esto conlleva. Los datos revelan que el 78% de la población total utiliza redes WiFi abiertas sin considerar si dicha red es segura o no. El informe también muestra que el 72% de los usuarios de redes WiFi públicas son vulnerables a ataques, ya sea a través de una configuración errónea o a partir del administrador de la red. Es importante recordar que, para evitar tener problemas de seguridad, los usuarios deben estar siempre atentos y asesorados para mejorar la configuración de sus redes (ECN 2018).

También (LEÓN LÓPEZ 2021) Nos comenta que la seguridad de las redes inalámbricas es uno de los principales desafíos. El uso cada vez mayor de dispositivos conectados al internet para la comunicación y colaboración nos hace más propensos a la exposición a amenazas internas y externas. Estas amenazas incluyen el robo de información, la manipulación de datos, la suplantación de identidad y la interrupción del servicio. Por lo

tanto, se requiere una vigilancia permanente y una configuración adecuada de todos los dispositivos conectados para evitar cualquier problema de seguridad.

Los datos recientes en América Latina y el Caribe reflejan la preocupación de los gobiernos y las empresas por mejorar la seguridad informática. El 40% de las compañías informan haber sufrido un incidente de seguridad en los últimos 24 meses, mientras que sólo un 3% realiza simulaciones para probar la efectividad de sus procesos de respuesta. Por otro lado, las organizaciones están dispuestas a asignar presupuestos adecuados para la gestión de seguridad y el 89% le otorga una importancia muy alta a este tema (DELOITTE 2019).

Refiriéndonos a Perú y Latinoamérica tenemos una imagen que representa el nivel de protección de seguridad en las organizaciones como muestra figura Nº 1.1

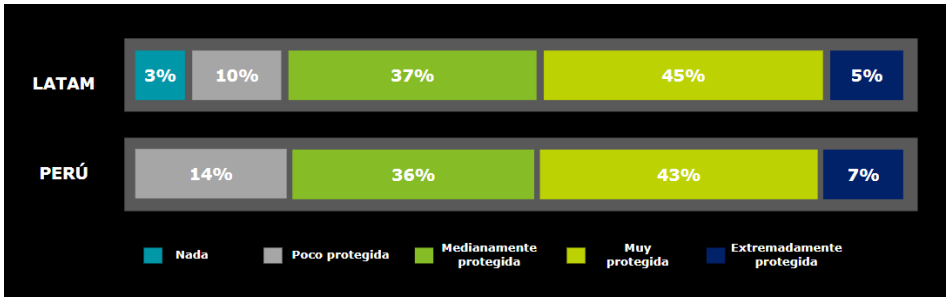


Figura 1.1 Nivel de protección de seguridad en las organizaciones

Fuente: (DELOITTE 2019)

Como se puede observar en la figura Nº 1.1, Prácticamente la mitad de las organizaciones se sienten muy protegidas con respecto a los riesgos de seguridad informática. En el Perú un 14 % se encuentra poco protegida la seguridad, es un porcentaje a tener muy en cuenta.

El Instituto de Educación Superior Tecnológica Privada "San Pedro", tiene como misión ser una comunidad de educación superior que imparte instrucción de alto nivel académico y constantemente actualizado para la realización de proyectos de formación, investigación tecnológica e interacción social que sirva al desarrollo integral, solidario y sostenible de las personas y de la sociedad, dentro de la región y la nación; y que contribuya a la consolidación de la paz social, la justicia y la democracia en la nación Peruana.

El Instituto de Educación Superior Tecnológica Privada San Pedro - Huancayo, cuenta con 224 estudiantes, 24 docentes, 8 de personal administrativo, nos ofrece 5 carreras profesionales tales son: Desarrollo de Sistemas, Construcción Civil, Gastronomía y Arte Culinario, Contabilidad y Secretariado Ejecutivo.

En el lugar elegido para la investigación se ha identificado los siguientes problemas:

- **Confidencialidad,** los usuarios tienen acceso constante a sus cuentas tanto institucionales como personales sin ningún tipo de administración, además no tienen ningún control de su identidad de las que hacen uso en la red, para realizar la medición se va utilizar el % de accesos no autorizados. (% de vulnerabilidad).

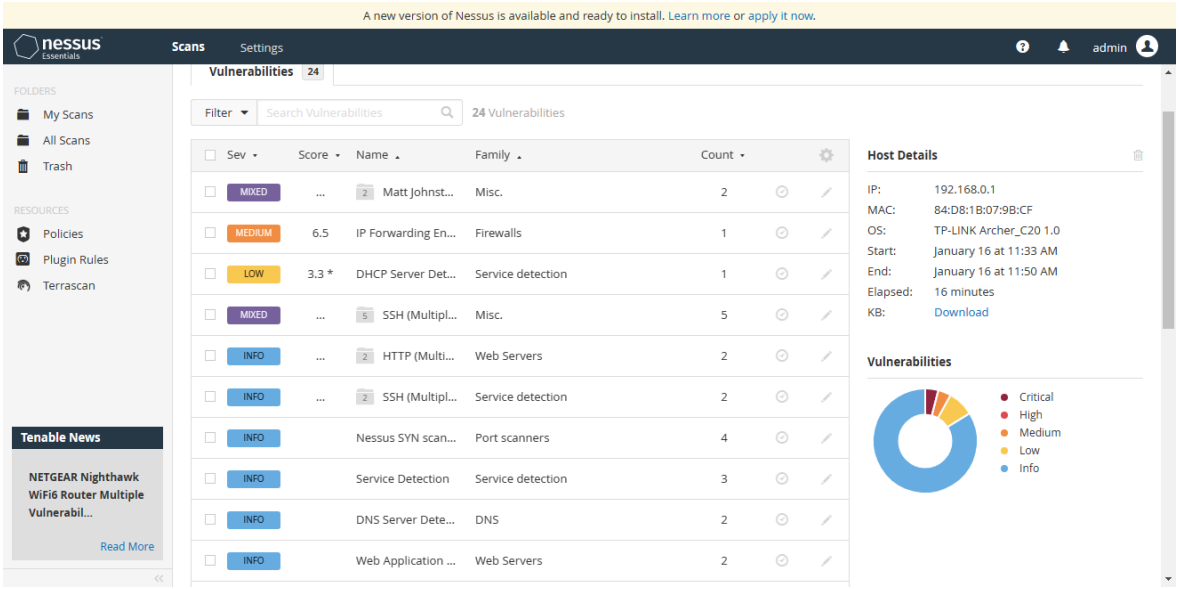


Figura 1.2 Scaneo de Vulnerabilidades con Nessus

En la figura N° 1.2, se puede apreciar el scaneo de las vulnerabilidades de la red, los dispositivos conectados a nuestra WLAN con ayuda del programa Nessus.

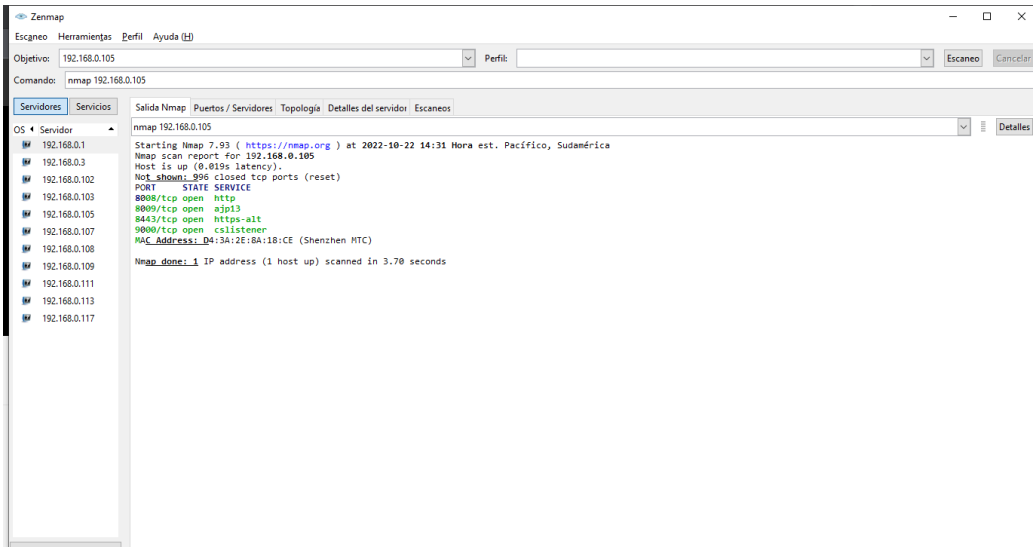


Figura 1.3 Scaneo de puertos abiertos

También en la Figura N° 1.3, se puede apreciar un scaneo a los puertos abiertos, con ayuda del programa NMap.

Tabla 1.1 % de accesos no autorizados

N° ESTADISTICO	MINIMO ESTADISTICO	MAXIMO ESTADISTICO	MEDIA ESTADISTICA %
154	47.60%	93.20%	70.97%

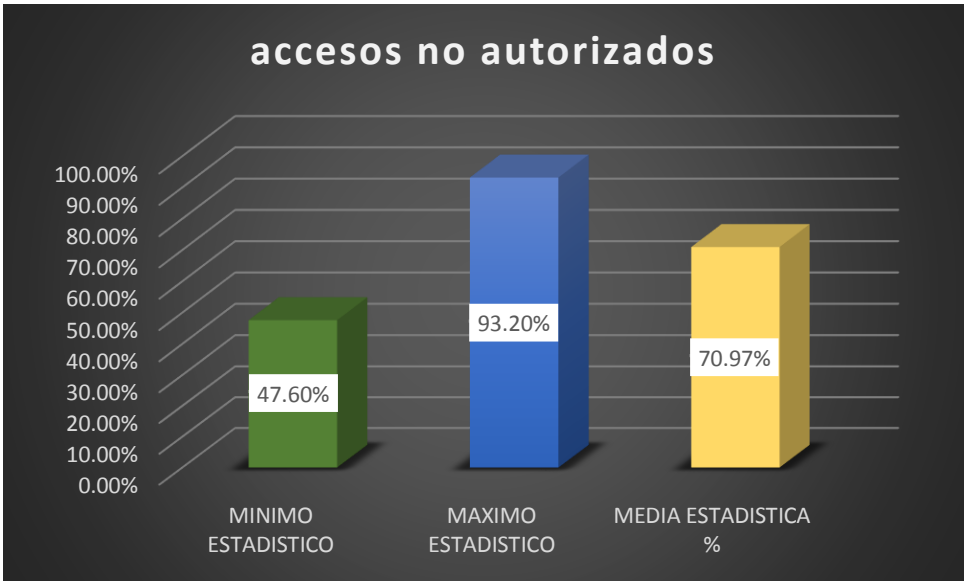


Figura 1.4 accesos no autorizados

En la tabla Nº 1.1 y figura Nº 1.4 se puede apreciar el porcentaje de accesos no autorizados, teniendo como media estadística un 70.97 % de accesos no autorizados.

- **Disponibilidad,** control de acceso a páginas web, los usuarios utilizan de forma inadecuada la navegación por internet, muchos de ellos dedican mucho tiempo al uso de redes sociales, juegos en línea, así como a la visualización de videos en línea, por consiguiente, saturaran el ancho de banda afectando su disponibilidad, para realizar la medición se va utilizar el tiempo promedio de respuesta en milisegundos (ms).

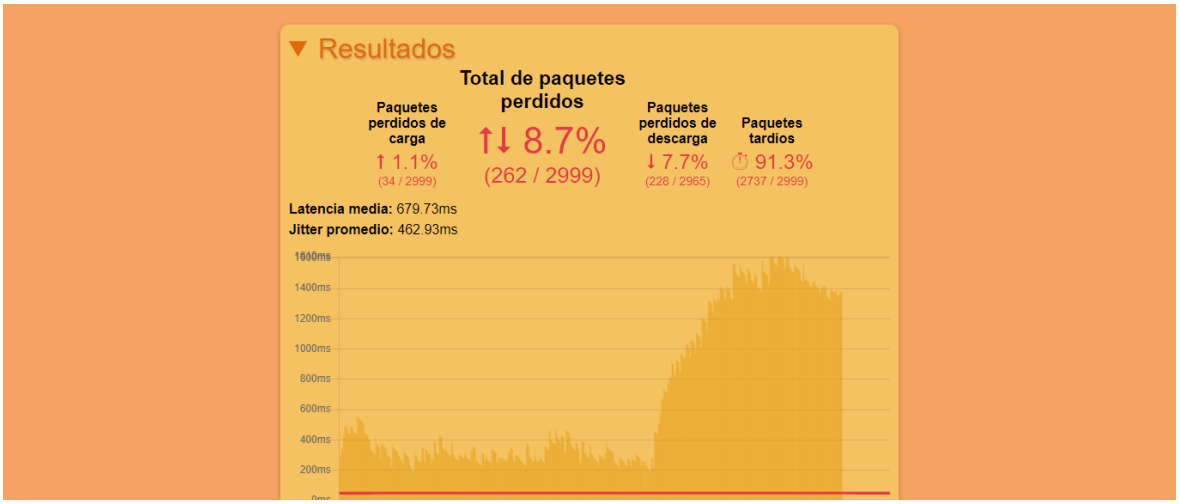


Figura 1.5 porcentaje de paquetes perdidos y la latencia promedio con la ayuda del Packet Loss Test

En la Figura N°1.5, podemos observar el porcentaje de paquetes perdidos y la latencia promedio con la ayuda del Packet Loss Test.

Tabla 1.2 Tiempo de respuesta promedio

N° ESTADISTICO	MINIMO ESTADISTICO	MAXIMO ESTADISTICO	MEDIA ESTADISTICA
154	90.00	130.00	111.37

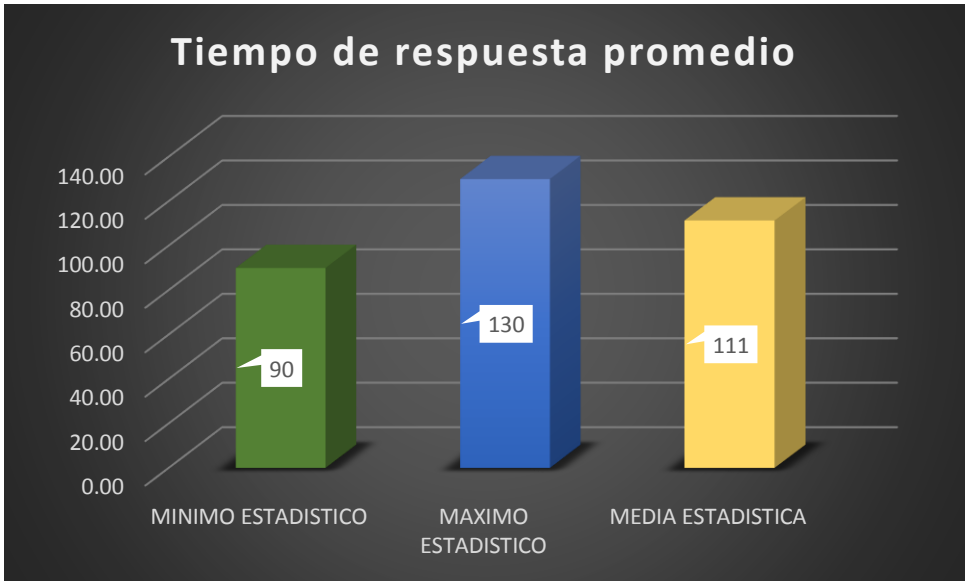


Figura 1.6 Tiempo de respuesta promedio

En la tabla Nº 1.2 y figura Nº 1.6 se puede apreciar el tiempo de respuesta promedio, teniendo como media estadística 111 ms.

- **Integridad,** no se está optimizando el uso de red priorizando el tráfico de acuerdo a lo establecido, existe una correlación entre perdida de datos y tiempos de latencia, si los tiempos de latencia son altos esto nos indicará que existirá perdidas de paquetes. Para medir la latencia o retardo se usa el ping se expresa en milisegundos (ms) y para medir la perdida de datos se tendrá en cuenta % perdida de paquetes.

Figura 1.7 Latencia en segundos
Fuente: (DELOITTE 2019)

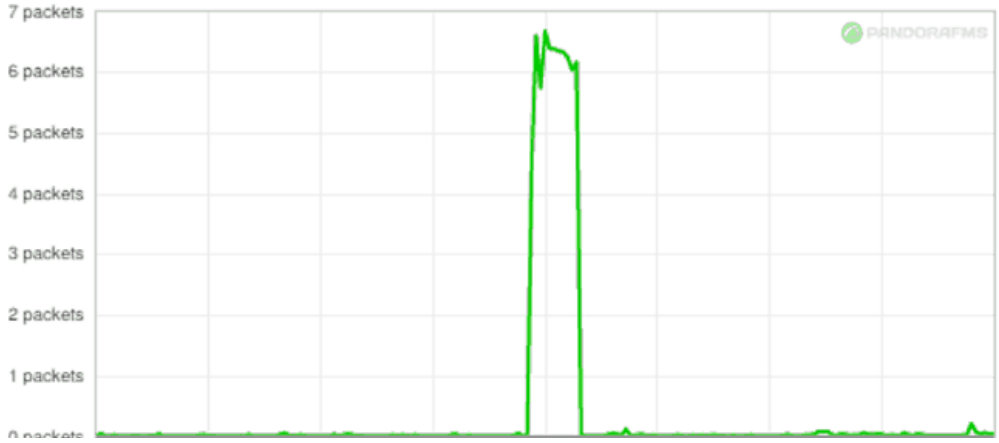


Figura 1.8 Perdida de paquetes
Fuente: (DELOITTE 2019)

En la Figura Nº 1.7 y 1.8, con la ayuda del programa Pandora FMS se puede observar la correlación existente entre segundos de latencia y pérdida de paquetes, es decir a mayor latencia, mayor la posibilidad de pérdida de paquetes, por tanto, la integridad se ve afectada.

Tabla 1.3 % de pérdida de paquetes

N° ESTADISTICO	N° PAQUETES ENVIADOS	MINIMO ESTADISTICO	MAXIMO ESTADISTICO	MEDIA ESTADISTICA	MEDIA ESTADISTICA %
154	1000	30	50	39	3.89%

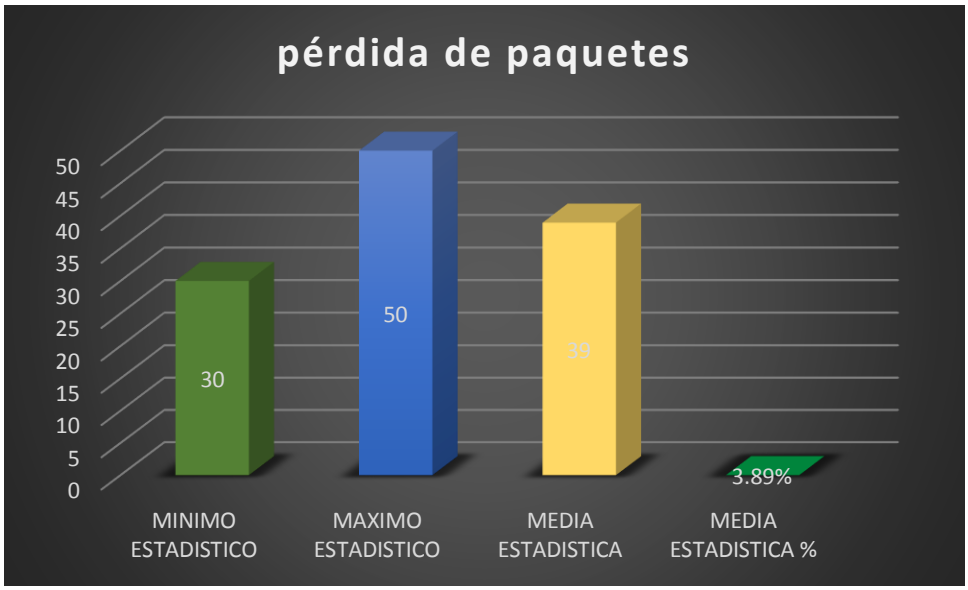


Figura 1.9 pérdida de paquetes

En la tabla Nº 1.3 y figura Nº 1.9 se puede apreciar el porcentaje de pérdida de paquetes, teniendo como media estadística 3.89 %.

Algunas causas que contribuyen al aumento de los problemas de seguridad informática en la red inalámbrica del IESP San Pedro son la falta de una administración de control de acceso (ACL) y políticas internas, la carencia de una administración de acceso a las páginas web, lo que lleva a un mayor uso de redes sociales, juegos en línea y visionado de videos en línea. También se ha detectado una correlación entre la pérdida de datos y la latencia en la transmisión de información, así como una priorización incorrecta del tráfico de datos.

Los efectos que los problemas de seguridad informática pueden traer son muy graves. Estos problemas pueden causar el robo de datos personales, información confidencial y/o credenciales, lo que afectaría la confidencialidad de los datos. Otra consecuencia de estos problemas es que la saturación de la banda de internet afectaría la disponibilidad de la

información. Finalmente, la perdida de datos y la latencia alta pueden generar una navegación inestable, lo que a su vez compromete la integridad de la información, causando frustración entre los usuarios.

Por lo antes mencionado se propone implementar un Portal Cautivo con la finalidad de que el administrador de la red pueda administrar y autorizar el acceso de los usuarios o grupos de usuarios, a los diferentes servicios ofrecidos por la red, en base a un registro de contabilidad de todas las acciones realizadas por los usuarios en la red; de igual modo, el administrador de la red podrá administrar el acceso a páginas web beneficiando el ancho de banda y por consiguiente la disponibilidad de datos y administrar la latencia a niveles óptimos de navegación y así evitar que la integridad de datos se vuelva perjudicial al momento de la navegación.

1.2. Delimitación del problema

1.2.1. Espacial

El trabajo de investigación se ejecutará en el IESTP SAN PEDRO de Huancayo.

1.2.2. Temporal

La investigación se desarrollará entre agosto de 2022 a diciembre de 2022.

1.2.3. Económica

El gasto ocasionado en el desarrollo de la investigación será asumido íntegramente por el tesista.

1.3. Formulación del problema

1.3.1. Problema General

¿De qué manera influye el Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO?

1.3.2. Problemas Específicos

¿De qué manera influye el Portal Cautivo para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO?

¿De qué manera influye el Portal Cautivo para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO?

¿De qué manera influye el Portal Cautivo para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO?

1.4. Justificación

1.4.1. Social

Los resultados de la investigación proporcionaran un gran beneficio para la institución ya que con esto se podrá mantener segura la información y lo más significativo impedir que terceras personas puedan vincularse a nuestra red ya que este es un servicio dedicado estrictamente a los estudiantes y a las diferentes oficinas con las que cuenta en el IESTP San Pedro con todo esto se podrá mejorar el acceso a la red.

1.4.2. Teórico

Esta investigación busca aportar conocimiento utilizando norma ISO/IEC 27002:2013 para la Seguridad de la Información.

Esta investigación se realiza con el propósito de aportar al conocimiento existente sobre el acceso a las redes inalámbricas mediante el uso de un Portal Cautivo, cuyos resultados de esta investigación podrá sistematizarse en una propuesta para ser incorporado en la red de información, ya que se estaría demostrando que el uso adecuado de un Portal Cautivo mejoraría el acceso a la red inalámbrica del IESTP "SAN PEDRO mediante los estudiantes de esta institución.

1.4.3. Metodológica

Esta investigación pretende contribuir en las investigaciones efectuadas hasta el momento, sobre la importancia de la implementación de un portal cautivo como elemento esencial para la seguridad de datos en una red inalámbrica, afectando en la confiabilidad, disponibilidad e integridad de la información.

El trabajo tiene utilidad metodológica en cuanto a la originalidad del instrumento, ya que fue diseñada considerando las características tanto de la población, así como el lugar de estudio. Gracias a esto se podrán realizar futuras investigaciones.

Pare el desarrollo de la presente, se basará en la metodología PPDIOO (Preparar, Planificar, Diseñar e Implementar).

Para los fines de esta investigación, se utilizará la metodología por su simplicidad, comunicación y realimentación dentro de todas las fases del proyecto. Esta metodología permite una mejor comprensión de los resultados obtenidos a través de un proceso de evaluación más sencillo y eficiente.

1.5. Objetivos

1.5.1. Objetivo General

Determinar de qué manera influye el Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO.

1.5.2. Objetivos Específicos

Identificar de qué manera influye el Portal Cautivo para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO.

Identificar de qué manera influye el Portal Cautivo para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO.

Identificar de qué manera influye el Portal Cautivo para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO.

CAPITULO II

MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Nacionales

Al revisar la tesis de (LINO LÓPEZ 2022), titulado "Diseño e Implementación de una red de seguridad informática para mejorar la administración de datos basado en la norma ISO/IEC 27002:2013, en la empresa A.C.E saco oliveros -sede Monterrico. lima 2021". Con el objetivo de Determinar de qué manera influye el diseño e implementación de una red de seguridad informática para mejorar la administración de datos en la empresa A.C.E Saco Oliveros -Sede Monterrico. Lima 2021 para lo cual utilizó la metodología de procesos, el ciclo de Deming más conocido como el ciclo PHVA (Planificar, Hacer, Verificar, Actuar). Finalmente se concluye que se maximizó la producción del personal administrativo, ejecutan políticas de seguridad y se minimizo el consumo de internet, garantizando estabilidad en los sistemas web administrativos.

Al revisar la tesis de (MORALES CHAPMAN, TORRES LEIVA 2021), titulado "Implementación de una Red Privada Virtual basada en la metodología PPDIOO para mejorar la seguridad informática en la red de Lima Traylers S.A.C.". Con el objetivo de principal es mejorar la seguridad informática en la red de Lima Traylers S.A.C para lo cual utilizó la metodología PPDIOO, Finalmente se concluye que, el uso de una VPN (Virtual Private Network) basado en la metodología PPDIOO, mejoró la seguridad informática en la red de Lima Traylers S.A.C.

Al revisar la tesis de (SÁNCHEZ REVOLLEDO, FERRER DULCE 2021), titulado "Implementación de un centro de operaciones de seguridad (COS) para mejorar la seguridad en la red informática de la Universidad Nacional del Santa". Con el objetivo de Mejorar la Seguridad en la Red Informática de la Universidad Nacional del Santa a través de la implementación de un Centro de Operaciones de Seguridad (COS) la cual utilizó la metodología experimental que consistirá en 7 fases Finalmente se concluye por los resultados de los tres indicadores de evaluación, se puede inducir y determinar que la implementación del Centro de Operaciones de Seguridad mejora la seguridad en la Red Informática de la Universidad Nacional del Santa.

Al revisar la tesis de (RIVEROS PARAGUAY 2019), titulado "Implementación de políticas de seguridad informática para mejorar el acceso y la seguridad lógica de la Red en la Oficina Departamental de Estadística e Informática de Junín". Con el objetivo de Implementar las políticas de seguridad informática para mejorar el acceso y seguridad lógica de la red en la Oficina Departamental de Estadística e Informática de Junín la cual utilizó la metodología Top Down, Finalmente se concluye La implementación de políticas de seguridad informática en la Oficina Departamental de Estadística e Informática de Junín mejoró el acceso a la red permitiendo al usuario tener un perfil privado y poder navegar sin problemas de lentitud ya que las quejas de los usuarios se redujeron en un 40%y la latencia disminuyo en 43%.

Al revisar la tesis de (POMALAYA MONTERO 2018), titulado "Rediseño de la red de datos para mejorar la seguridad informática de una Municipalidad". Con el objetivo de Determinar de qué manera el rediseño de la red de datos mejora la seguridad informática la cual utilizó la metodología Top Down Network Desing, Finalmente se concluye que, con el rediseño de la red de datos se mejoró significativamente la seguridad informática.

2.1.2. Internacionales

Al revisar la tesis de (LEÓN LÓPEZ 2021), titulado "Estudio de factibilidad para la implementación de un portal cautivo para mejorar la seguridad de transmisión de datos en la universidad estatal del sur de Manabí". Con el objetivo de Desarrollar el análisis de factibilidad para la implementación de un portal cautivo para mejorar la seguridad en la transmisión de datos la cual utilizó la metodología de tipo deductivo, analítico y

bibliográfico, Finalmente se concluye que es factible para los usuarios sirviendo nuevas funcionalidades y beneficiar al consumidor, el cual trabaja con la tecnología Unifiy es por aquello que es viable implementar un portal cautivo así teniendo aceptación por parte de los técnicos a cargo del mantenimiento de la red de datos.

Al revisar la tesis de (LAZO JAIME, SALTOS PONCE 2020), titulado "Implementación de una nueva infraestructura Wireless en la carrera de Ingeniería en Sistemas Computacionales, a través de un Portal Cautivo mediante la integración con Access Point de Cisco Meraki, teniendo una administración en la nube". Con el objetivo de Implementar un prototipo funcional de un Portal Cautivo integrado con Access Point de Cisco Meraki para el cambio de la infraestructura Wireless para lo cual utilizó la metodología cascada, Finalmente se concluye que se ha comprobado, que el 92% de usuarios indican que su red inalámbrica es insegura, convirtiéndose en lugares de encuentro de personas, debido a que disponen de dispositivos móviles con la capacidad de conectarse a sus redes Wi-Fi y un 8% de ellos, que sí poseen seguridad en su red inalámbrica.

Al revisar la tesis de (RUIZ ANDINO 2022), titulado "Evaluación del Firewall de Frontera Free Pfsense para proteger la confidencialidad, integridad y disponibilidad de la información de compañías de responsabilidad limitada en Riobamba año 2021". Con el objetivo de evaluar el firewall de frontera free PfSense para proteger la confidencialidad, integridad y disponibilidad de la información de Compañías De Responsabilidad Limitada en Riobamba año 2021, Finalmente se concluye que el uso del Firewall PfSense mejora la seguridad, integridad y confidencialidad de la información que tiene la compañía limita, se recomienda el uso de este software dentro de la red LAN de las Compañías de Responsabilidad Limitada de la Ciudad de Riobamba u otras entidades que necesiten fortalecer la seguridad informática.

Al revisar la tesis de (PIARPUEZÁN LÓPEZ, RIASCOS ORTIZ 2019), titulado "Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020". Con el objetivo de determinar agentes generadores de latencia en la red de datos inalámbrica (WLAN), basándose en la infraestructura tecnológica de la misma, identificando los principales factores que disminuyen la accesibilidad al contenido en la web a los estudiantes para lo cual utilizó la metodología de enfoque mixto, Finalmente

se concluye Se determinó que la latencia se genera por diferentes factores como lo son el uso de contenido HTTP que es un contenido sensible a fallos, equipos obsoletos o desactualizados, infraestructura que impide el paso de las ondas electromagnéticas, distribución de Access Pointsde forma rudimentaria y la ausencia de herramientas que controlen el consumo de ancho de banda.

Al revisar la tesis de (ANDRADE CAYAMBE 2019), titulado "Diseño y simulación de portal cautivo, que permita: autenticación, aplicación de herramientas, políticas de seguridad, QoS y sonda dered para el filtrado de contenido mediante equipo UTM en la CISC-CINT". Con el objetivo de diseñar una propuesta con ambiente controlado de herramientas administrativas y portal cautivo para el ingreso de la red inalámbrica en la carrera de Networking y Sistemas, para lo cual utilizó la metodología PPDIOO (Preparar, Planificar, Diseñar e Implementar), Finalmente se concluye que el software opensource solventa de manera eficaz las necesidades de la institución para administrarla red wireless, mejora la funcionabilidad y rendimiento de la red con medidas de seguridad y métodos de autenticación. Se obtendrá un control total de cada una de las herramientas tecnológicas y recursos de la institución. La red inalámbrica de la carrera de ingeniería de networking y sistemas será monitoreada constantemente y administrada de manera eficaz. Se restringe el acceso a usuarios no autorizados, se obtiene alertas y bloqueo a páginas web.

2.2. Bases Teóricas o Científicas

2.2.1. Definición de Red inalámbrica

Las redes inalámbricas son aquellas que permiten conectar dispositivos electrónicos a la red usando ondas electromagnéticas, sin necesidad de un cable, dentro de un área estimada (SALAZAR, 2016).

(LÓPEZ JURADO 2021), define que una red inalámbrica es un enlace que utiliza señales de radio o infrarrojo para comunicar dos o más terminales sin necesidad de cables. Esto permite que los dispositivos se conecten a la red a través de antenas y sin ningún cable, incluso a grandes distancias. Estas redes no requieren ninguna modificación de la infraestructura existente, a diferencia de las redes cableadas. Como se muestra en la figura 2.1

Figura 2.1 Representación de redes inalámbricas

Fuente: (LÓPEZ JURADO 2021)

a) Tipos de redes inalámbricas

Según (SALAZAR 2016), clasifica las redes inalámbricas según su alcance:

1. Red Inalámbrica de Área Personal (WPAN)

Las redes inalámbricas de área personal (WPAN) se rigen bajo la norma IEEE 802.15. Estas redes permiten la comunicación entre dispositivos a corta distancia, aproximadamente 10 metros. Estas redes no requieren conectividad directa o infraestructura externa al enlace establecido. Esto permite respuestas poco productivas con un gasto mínimo y un bajo consumo de energía. Estas redes dependen de avances tecnológicos como Bluetooth, IrDA, ZigBee o UWB, con una baja velocidad de transmisión que se mide en número de bits transferidos o recibidos por unidad de tiempo (bps o bit/s) (SALAZAR 2016).

2. Red Inalámbrica de Área Local (WLAN)

Las redes inalámbricas de área local (WLAN) proporcionan ingreso inalámbrico a usuarios dentro de un área determinada y según el estándar IEEE 802.11. Esta norma comprende una familia de diferentes estándares para redes inalámbricas de área local,

siendo el IEEE 802.11b su primer estándar reconocido y compatible con velocidades de hasta 11 Mbps en la banda de recurrencia sin licencia de 2,4 GHz. El IEEE 802.11g fue diseñado como el sustituto del IEEE 802.11b con una mayor velocidad de transmisión, y un punto de ingreso IEEE 802.11g puede soportar usuarios 802.11b y 802.11g (SALAZAR 2016).

3. Red Inalámbrica de Área Amplia (WWAN)

Las redes inalámbricas de área extensa abarcan grandes distancias de hasta 50 kilómetros y requieren frecuencias con licencia para su funcionamiento. Estas redes pueden cubrir una zona amplia, como, por ejemplo, localidades o territorios, usando sistemas de satélites o antenas controladas por un proveedor de servicios de Internet. Estas redes podrían usar dos tecnologías básicas: telefonía móvil o satélites (SALAZAR 2016). Como se muestra en la figura 2.2

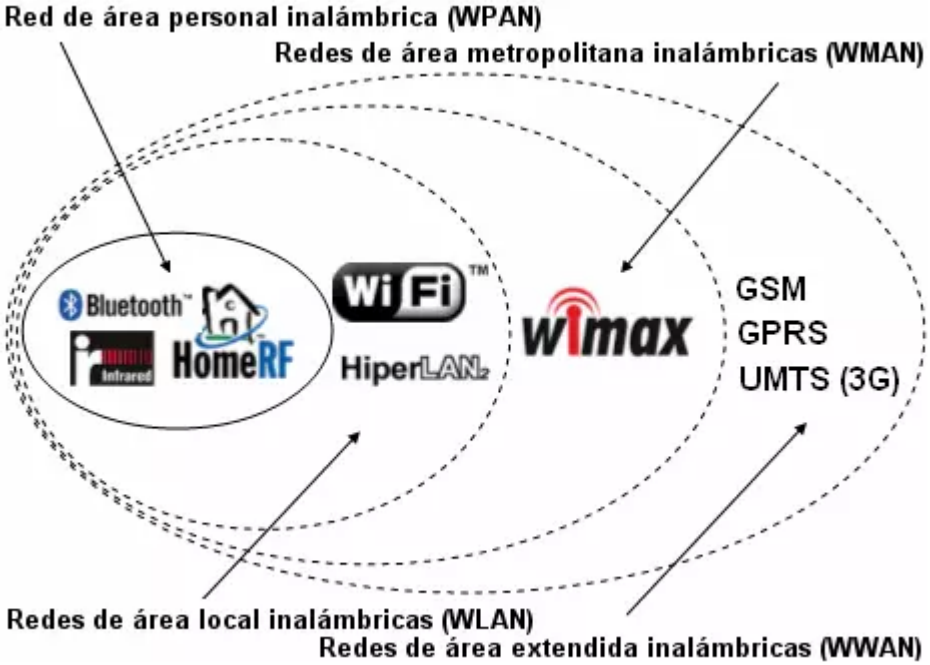


Figura 2.2 Redes WPAN, WLAN, WMAN, WWAN

fuente: (LÓPEZ JURADO 2021)

b) Ventajas y desventajas de las redes inalámbricas

(ANDREU 2011), deduce las siguientes ventajas que nos ofrece este medio:

- Rápida instalación de la red: Una instalación rápida sin la necesidad de cables o de solicitar permisos.

- Movilidad: La movilidad dentro del radio de alcance de la señal.
- Menos costos de mantenimiento: costos bajos de mantenimiento, debido a la ausencia de cableado.
- Accesibilidad: Todos los celulares. PDA y portátiles soportan o integran varias tecnologías inalámbricas.
- Productividad: mayor productividad.
- La posibilidad de cubrir zonas despobladas donde no llega el cableado.

(ANDREU 2011), así mismo define las siguientes desventajas insalvables e impredecibles:

- Cambios climáticos: la lluvia, el viento, entre otros factores.
- Interferencias externas: otros emisores de microondas.
- Falta de seguridad: al emitirse libremente por el aire para lograr ser interceptado por alguno, lo que necesita incrementar la seguridad y la encriptación.
- Aumento de errores por las interferencias.
- Aumento de costes iniciales: los dispositivos, antenas, entre otros tienden a ser más caros.
- La velocidad es más limitada.

Esto significa que la lluvia, el viento, otros emisores de microondas, o los dispositivos, antenas, entre otros, pueden interferir con la señal y limitar la velocidad de la red inalámbrica.

2.2.2. Hotspot

Según (RAMÍREZ SÁNCHEZ, VILLANUEVA LENDECHY 2008) Los hotspots son áreas donde hay cobertura Wi-Fi y donde los puntos de acceso ofrecen conexión a Internet por medio de un Proveedor de Servicios de Internet Inalámbrico (WISP). Estos lugares están en sitios públicos, como aeropuertos, bibliotecas, centros de convenciones, cafeterías y hoteles. Las personas pueden disfrutar de esta conexión en lugares públicos de forma gratuita o por una tarifa dependiendo del proveedor.

Los hotspots son redes inalámbricas que están compuestas de dos principales partes: puntos de acceso y tarjetas de computadora. Estos componentes se conectan entre sí mediante ondas de radio, lo que elimina la necesidad de cables para conectar la red.

2.2.3. Firewall y su función

Es la que autoriza o bloquea el tráfico de red al mismo tiempo.

Según (BACA URBINA 2016) Los firewalls tienen como función proteger computadoras personales o redes de computadora de ataques externos, ya sean maliciosos o no. Esto se hace mediante la configuración del firewall para bloquear información proveniente de ciertos sitios o aplicaciones, y al mismo tiempo permitiendo el paso de los datos esenciales para la organización.

2.2.4. Freeradius

Según (ANDRADE CAYAMBE 2019) El software es de código abierto, lo que permite autenticar a los usuarios mediante una base de datos hecha en FreeRADIUS o vinculada con un gestor de base de datos.

- El sistema acepta cualquier forma de autenticación EAP
- Se conecta a varios administradores de bases de datos como MySQL y PostgreSQL.
- Posee su propio certificado SSL/TLS.

2.2.5. Traffic Shaper

Según (Dávalos Castilla, Cabañas Victoria, Estrada 2013) Nos dice que, como herramienta administrativa, esto es útil para dar prioridad a determinado tipo de tráfico, ayudando así a los protocolos de red más importantes a tener una respuesta más rápida. De forma predeterminada, solo el tráfico HTTP y HTTPS tendrá prioridad.

Se utiliza políticas de gestión de tráfico para que el rendimiento de la red sea eficiente y veloz (Pfsense Traffic Shappe, 2019).

Sus Características

- El sistema ofrece configuraciones para dar un mayor peso y ancho de banda a ciertos paquetes (Pfsense Traffic Shapper, 2019).
- Limita el acceso por HTTPS.
- Establece límites de ancho de banda a IPs específicas.
- Permite crear limitadores para la subida y bajada de paquetes, y
- Tiene un asistente para generar colas y reglas automáticamente.

2.2.6. Herramientas Tecnológicas

- **PFSense**

Es una tecnología de código abierto con FreeBSD como sistema operativo. Todo el firewall/router se gestiona a través de una interfaz web para realizar configuraciones como DNS, DHCP, VPN, entre otros. Además, también ofrece funciones como monitoreo de red, control de ancho de banda, filtrado de contenido, etc. Lo cual demuestra que es un completo sistema para gestionar la red, brindando alta calidad en la conexión a Internet al usuario (PFSENSE, 2022).

- **Firewall**

Es aquella que autoriza o bloquea el tráfico de red al mismo tiempo.

Características:

- Ofrece filtrado de contenido,
- políticas de enrutamiento.
- Creación de alias para simplificar la configuración de IPs públicas, servidores, redes y puertos (FIREWALLHARDWARE 2021).
- Las reglas del firewall determinan si se permite o deniega el acceso de conexiones, especificando el tipo de red o los protocolos de comunicación entre otros (FIREWALLHARDWARE, 2021).

- **Ntopng**

Es aquella que sondea el tráfico de paquetes en tiempo real y presenta datos históricos (NTOP 2022)

Características:

- El sistema puede clasificar el tráfico de red según criterios como la dirección IP, puertos, sistemas autónomos y otros(NTOP 2022).
- El sistema muestra información en tiempo real.
- Así como un informe detallado sobre el rendimiento y latencias de la red (NTOP 2022).
- El sistema presenta información sobre protocolos de aplicación.
- Soporte para IPV4, IPV6, Capa 2, SNMP.
- informes detallados sobre hosts sospechosos y maliciosos, entre otros (NTOP 2022).

- **pfBlockerNG**

Es aquella que bloquea sitios no confiables de diferentes niveles por medio de descargas de listas y se establece en las reglas del firewall para prevenir ataques en la red(NETGATE 2022a).

Características:

- Utiliza la base de datos GEOIP
- Bloqueo de direcciones IP:
- Malware
- Spammers
- Entre otros ataques
- Bloqueo de sitios no seguros a nivel mundial

2.2.7. Método de autenticación

- **Protocolo de autenticación extensible (EAP)**

Es un protocolo de seguridad que se utiliza para autenticar usuarios a una red inalámbrica.

El Protocolo de Autenticación Extensible (EAP) es un diseño flexible que permite a las redes protegidas usar avanzados mecanismos de confirmación. Por ejemplo, el acceso inalámbrico basado en IEEE 802.1X. EAP no es una técnica de validación específica sino un sistema entre el cliente de entrada y el servidor de verificación. Esto permite a los especialistas de

red crear y enviar nuevas técnicas de verificación conocidas como Métodos EAP (MICROSOFT 2022).

Existen diferentes variantes del EAP:

- EAP-MD5: s una versión menos segura del protocolo EAP que usa nombres de usuario y contraseñas para autenticar. La función hash de MD5 de la contraseña se usa para realizar la verificación. Debido a que no verifica la identidad del servidor, es muy vulnerable a ataques como el Man-in-the-Middle (MICROSOFT 2022).
- EAP-LEAP: LEAP (Lightweight Extensible Authentication Protocol) es un sistema EAP propiedad de Cisco. Como en el caso de MD5, usa nombre de usuario y contraseña para autenticar. Utiliza un servidor RADIUS como servidor de autenticación. Está diseñado para prevenir ataques de tipo Man-in-the-Middle mediante autenticación mutua (MICROSOFT 2022).
- EAP-TLS: Usa certificados X.509 para tanto el usuario como para el servidor para la autenticación reciproca y cifrado de las comunicaciones. Esto ofrece un alto nivel de seguridad, pero requiere generar certificados para cada individuo, lo que puede ser un problema para organizaciones más pequeñas (MICROSOFT 2022).
- EAP-TTLS / PEAP: on dos ediciones en las que no se necesitan certificados para el usuario, como en el caso de EAP-TTLS. La identidad del servidor se establece con su certificado y la del usuario con un nombre de usuario y contraseña utilizando un servidor RADIUS (MICROSOFT, 2022).

2.2.8. Estándares inalámbricos 802.11

Es una tecnología inalámbrica que permite a los usuarios conectarse a la red local sin cables. Proporciona una solución de alto rendimiento y confiable para compartir datos, audio y vídeo entre equipos.

Estos estándares IEEE 802.11a/b/g/n se consideran identificadores de canales y frecuencias por donde se conectan los hosts a la WLAN.

- 802.11a: Opera en las bandas de frecuencia 5 GHz y 2,4 GHz, las cuales son comúnmente utilizadas en la región europea para Wi-Fi. Además, esta región también soporta el estándar 802.11h, el cual permite ajustar control dinámicamente el rango de frecuencias y potencias de transmisión para reducir al mínimo la interferencia con señales provenientes de satélites y sistemas de radar (CISCO 2022a).
- 802.11b y g: funciona exclusivamente en la banda de 2,4 GHz, provisto de 11 canales para Wi-Fi con los cuales se suelen usar el canal 1, 6 y 11. Esta banda opera a una frecuencia de 25 MHz como ancho de banda, con una velocidad de transmisión de 54 Mbps para el estándar "b" sin equipo OFDM establecido en la versión más reciente (CISCO 2022a).
- 802.11n: Comenzó a trabajar en 2008, aunque fue definido en 2004. Esta normativa ofrece una velocidad de transmisión máxima de 600 Mbps en conexiones de 3×3 (3 antenas). Además, es capaz de trabajar con las bandas de 2,4 GHz y 5 GHz de forma simultánea. La tecnología MIMO (Múltiple Input – Múltiple Output) también fue introducida por primera vez con este estándar, permitiendo usar varios canales al mismo tiempo para el envío y recepción de datos con hasta 3 antenas (CISCO, 2022a).
- 802.11ax: también conocido como Wi-Fi 6, se basa en los beneficios de los anteriores estándares de Wi-Fi y mejora su eficiencia, flexibilidad y escalabilidad. Ofrece velocidades de hasta 10 Gbps y alcanza aproximadamente 100 metros de distancia. También incluye un nuevo estándar llamado OFDMA (Acceso Múltiple por División de Frecuencias Ortogonales) para distribuir el ancho de banda subdividiendo los canales, permitiendo que los dispositivos se usen de forma eficiente para proporcionar aún mayor velocidad de transmisión de datos (CISCO 2022b).

2.2.9. Metodología PPDIOO (Preparar, Planear, Diseñar, Implementar, Operar, Optimizar).

Según (CISCO SYSTEM 2011) PPDIOO es una metodología creada por Cisco en el año 2008. Esta metodología consiste en seis fases: Preparar, Planear, Diseñar, Implementar,

Operar y Optimizar; las cuales describen el proceso completo de diseño e implementación de una red. La metodología PPDIOO como es conocida presenta una serie de beneficios y estos son:

- Aumenta la disponibilidad de la red.
- Reduce los costos en TI al validar los requisitos tecnológicos y los cambios en la infraestructura de red.
- Mejora el negocio estableciendo estrategias tecnológicas.
- Incrementa el acceso a las aplicaciones y servicios, y mejora el rendimiento, la seguridad, la fiabilidad y la escalabilidad de la red.

Fases de la Metodología PPDIOO

- **Fase I: Preparar.** Esta fase nos permite definir las características técnicas de la red, tales como aplicaciones a utilizar, cantidad de usuarios y demanda de cada una de las aplicaciones dentro de la red. Estos parámetros se utilizan para describir los puntos clave que definirán el uso de la red (CISCO SYSTEM 2011, pp. 11-25).
- **Fase II: Planear.** Esta fase se centra en los requerimientos de la red. Se analizan y obtienen todos los datos necesarios acerca de la misma, tales como patrones de tráfico, tipo de tráfico, direccionamiento y enrutamiento. A partir de los parámetros obtenidos en la fase de preparación, se propone una arquitectura de diseño que cumpla con todos los requisitos (CISCO SYSTEM 2011, pp. 11-25).
- **Fase III: Diseñar.** Esta fase se focaliza en la implementación de la arquitectura lógica y física de la red, poniendo a disposición los protocolos necesarios para su funcionamiento, además de los diferentes modelos de equipos y cableado estructurado, según los requisitos técnicos y empresariales obtenidos en fases previas (CISCO SYSTEM 2011, pp. 11-25).
- **Fase IV: Implementar.** Esta fase consiste en la creación de la red según las especificaciones obtenidas en etapas previas, proporcionando una descripción detallada de cada paso y del tiempo necesario para implementarla. Se realizan pruebas de campo para verificar la fiabilidad del diseño antes de su puesta en marcha (CISCO SYSTEM 2011, pp. 11-25).
- **Fase V: Operar.** Esta fase se dedica a asegurar el buen funcionamiento y el monitoreo de la red para verificar sus resultados, con el objetivo de prepararla para una posterior optimización (CISCO SYSTEM 2011, pp. 11-25).

- **Fase VI: Optimizar.** En esta fase se proponen cambios en el diseño de la red cuando se vea afectada su eficiencia o sean necesarias exigencias mayores. Esto se hace desde una administración proactiva, identificando y solucionando problemas antes de ver sus consecuencias reales (CISCO SYSTEM 2011, pp. 11-25).

Comparativa entre metodologías para el desarrollo de redes

Tabla 2.1 Tabla Comparativa entre metodología para el desarrollo de redes

Comparación de las metodologías de desarrollo de redes		
Metodología	**Ventajas**	**Desventajas**
Top-Down Network Desing (2004)	• Metodología destinada al diseño de redes enfocadas en el negocio. • Está centrada en los objetivos estratégicos que se desean alcanzar.	• Se necesitan un mayor compromiso y recursos para su ejecución. • Debido a que está orientada hacia un diseño de arriba hacia abajo, no es recomendable su uso cuando es necesario realizar una configuración de red.
PPDIOO (2008)	• Reduce los costos de implementación gracias a un examen de requerimientos previo. • Aumenta la velocidad de acceso para servicios y aplicaciones de manera segura. • Se puede aplicar en cualquier ámbito físico (negocios, industrias, casas, etc.)	• Es importante tener en cuenta que el diseño de la red debe ser un proceso estructurado y desarrollarse con precisión, ya que, si se cometen errores en algunas de las fases, el diseño e implementación no arrojarían los mejores resultados.

James Mccabe (1998)	• Se la puede utilizar como un análisis previo antes de establecer algo. • Dado que es una metodología teórica, se pueden realizar futuras modificaciones sin afectar la estructura de red.	• No está diseñado para redes corporativas. • s una metodología con objetivos experimentales. • Está descontinuada. • Se trata de un procedimiento secuencial.
Cormac Long	• Como es una metodología teórica, se pueden realizar futuras modificaciones sin dañar la arquitectura de la red.	• Es una metodología con objetivos experimentales. • Está descontinuada.

Fuente: (GUEVARA CAJAS, QUIZHPI LEÓN 2017)

En la tabla 2.1, se puede observar una comparativa entre cuatro metodologías para el desarrollo de redes, al final se decide utilizo la metodología PPDIOO, ya que nos ofrece más ventajas que el resto, es la que más de adapta a las necesidades de la institución. Para el desarrollo de la investigación se utilizó las siguientes fases (preparar, planificar, diseñar e implementar).

2.2.10. Nessus

Nessus es una herramienta de seguridad que ofrece versiones tanto gratuitas como de pago. Está diseñada para detectar vulnerabilidades en una variedad de sistemas operativos (TENABLE 2022). Consta de cuatro pasos:

- Escaneo de puertos, al igual que Nmap, Nessusd examina los dispositivos conectados a una red y los puertos abiertos para realizar su análisis
- Identificación de servicios.
- Identificación de vulnerabilidades.
- Un sondeo final para confirmar los resultados. Utiliza su extensa base de datos para detectar los fallos de seguridad en dispositivos conectados a una red (TENABLE 2022).

2.2.11. Packet Loss Test

"Utiliza technología WebRTC de punta para probar la pérdida de paquetes, la latencia y el jitter de latencia de su conexión a Internet en su navegador de forma gratuita" (MINER 2022).

"WebRTC es la tecnología de punta (a partir de 2019) que hace posible este sitio. Incluye varias API de JavaScript en WebIDL que proporcionan comunicación en tiempo real" (MINER 2022).

2.2.12. Vulnerabilidad

"Son errores en la seguridad del sistema que ponen en riesgo la información. El escaneo busca encontrar esos fallos para garantizar la protección de los datos" (TENABLE 2022).

2.2.13. Seguridad en Redes Inalámbricas

Según (ALFONSO, CABALLER MIGUEL 2005), explica que existen una variedad de protocolos y aplicaciones que se usan para transmitir datos. Muchas aplicaciones ya usan sus propios sistemas de cifrado, preparados para garantizar la seguridad al transmitir datos a través de redes públicas. El más común es el protocolo Secure Sockets Layer (SSL) utilizado en la web. El protocolo SSL encripta los documentos enviados a través de conexiones web.

El uso de estos protocolos impide que los datos transmitidos a través de la red sean interceptados, junto con otras medidas de seguridad adoptadas.

2.2.14. Políticas de seguridad

Según (ANDRADE CAYAMBE 2019) la administración de seguridad implica la implementación de políticas y privilegios para los usuarios, que son gestionados por el administrador de red. Estas políticas de seguridad se definen en función de las necesidades de la empresa u organización, y se apoyan en herramientas tecnológicas para la protección de la red.

2.2.15. Mecanismos de seguridad

- Prevención**.** – Establece la información cifrada, controla los accesos, y actúa como una protección ante ataques potenciales.

- Detección**.** – Puede detectar el comportamiento sospechoso que indicaría la presencia de un ataque y emitir una alerta para prevenir cualquier consecuencia negativa.
- Recuperación**.** – Detectar daños en la red y prevenir cualquier consecuencia negativa al restablecer la operación correctamente. (MIGUEL PÉREZ 2015).

a) Creación de Políticas de Seguridad

- **Almacenamiento de Contraseñas**

Los usuarios tienen asignado un usuario y contraseña, y cualquier uso indebido será reportado y notificado en nuestro sistema. (MIGUEL PÉREZ 2015).

- **Control de acceso**

✓ Acceso a la red.

Sólo los usuarios autorizados pueden acceder a la red mediante los mecanismos de autenticación establecidos. (MIGUEL PÉREZ 2015)

✓ Lista de usuarios.

La información de los usuarios autorizados se almacenará en la base de datos. (MIGUEL PÉREZ 2015)

✓ Registro de actividades.

Es capaz de detectar cualquier uso indebido o dañino que pueda afectar la red. (MIGUEL PÉREZ 2015).

✓ Acceso a Internet.

Solo las personas autorizadas tendrán acceso a navegar por Internet. (MIGUEL PÉREZ 2015).

✓ Restricción a sitios web.

Bloquea el acceso a sitios web no seguros con el fin de prevenir cualquier posible daño a la empresa. (MIGUEL PÉREZ 2015).

- **Control de tráfico**

✓ Ancho de banda

Es importante evitar la sobrecarga de la red por el uso inadecuado, ya sea por el acceso a sitios web o videos inapropiados, entre otros. Se debe priorizar el uso para aquellos fines relacionados con el estudio.

2.2.16. NORMA ISO/IEC 27001:2013

(ISO Central Secretariat 2022) Information Security Management Systems Requirements (Requisitos para los sistemas de Gestion de Seguridad de la Informacion), norma que permite certificar la implantación de un sistema de gestión de seguridad de la información en una organización. Es un estándar para la seguridad de la información. Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización.

La ISO 27001:2013 es la norma internacional de Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información. Esta revisión más reciente fue publicada en 2013, como una evolución de la anterior BS 7799-2, que se publicó en 2005.

ISO 27001 se centra en garantizar la confidencialidad, la integridad y la disponibilidad de la información de una empresa. Esto implica evaluar los posibles problemas que pudieran afectar dicha información, para luego definir las medidas necesarias para prevenir su ocurrencia. Ese proceso comprende desde el análisis de riesgos hasta la implementación de planes para su mitigación.

Importancia de la Norma ISO 27001

(WORLD ECONOMIC FORUM 2023) Según el informe anual del Foro Económico Mundial, los ciberataques vuelven a ser una de las principales amenazas a las que se enfrenta la humanidad en 2020. La pérdida de información sigue siendo un problema importante este año, especialmente con la nueva realidad del trabajo remoto. Esto está creando brechas de seguridad y múltiples riesgos para las empresas. De hecho, el ataque a Twitter tuvo lugar a través de la computadora de un colaborador que trabajaba desde su casa.

Entiendo que las organizaciones a nivel mundial dependen del procesamiento de información, lo cual los expone a amenazas. El desafío es encontrar el mejor punto de partida para proteger la información y garantizar su seguridad. Existen varios pasos que una organización puede tomar para comenzar a proteger sus datos, como proporcionar formación al personal, implementar tecnología de seguridad, monitorear constantemente el sistema, y mantener copias de seguridad.

2.3. Marco Conceptual (de las variables y dimensiones)

2.3.1. Portal Cautivo

(SIERRA CALLEJA 2015) nos dice, una página web de autenticación es una interfaz por la que un usuario de una red pública o privada debe pasar para garantizar el acceso a las funciones normales de la red. Estas páginas son ampliamente utilizadas en centros comerciales, aeropuertos, hoteles, cafeterías, cafés con Internet y otros proveedores de hotspot Wi-Fi para los usuarios de Internet.

Por otro lado, (IZASKUN PELLEJERO, LESTA 2006) Un sistema de autenticación puede implementarse con software o hardware para supervisar el tráfico de la red. Esto obliga a los usuarios a ingresar a través de una página HTML específica, para que puedan tener acceso web normal desde su dispositivo, ya sea en una red privada o pública. El usuario tendrá que autenticarse mediante un inicio de sesión para tener acceso a la web y navegar durante un tiempo limitado.

También, (CISCO 2022c) nos dice, el Portal cautivo de Cisco ofrece una forma conveniente, segura y rentable para ofrecer acceso inalámbrico a clientes y otros visitantes sin afectar la seguridad de su red interna.

También, (NETGATE 2022b) El portal captivo impide el acceso de personas que no están autorizadas a la red mediante una validación que se realiza desde un portal web al cual se reorienta al usuario cuando desee conectarse y utilizar los recursos de red.

a) ¿Para qué sirve un Portal Cautivo?

Según (SIERRA CALLEJA 2015) Un portal cautivo es muy útil a la hora de gestionar una red inalámbrica Wi-Fi, ya que podremos controlar a los usuarios que se conecten a la red, asignándoles un nombre y contraseña, ancho de banda y un tiempo limitado, con lo cual estamos brindándole el acceso a internet por el tiempo de forma que nosotros queramos. Por ejemplo, si tenemos un portal cautivo en un hotel, podremos asignar un usuario y contraseña a un huésped por el tiempo que dure su estancia.

Por otro lado (CISCO 2022c) nos dice, una red de invitados puede servir muchos propósitos empresariales importantes, como simplificar los negocios con los socios y proporcionar una mejor satisfacción del cliente y mejorar la productividad de los empleados.

b) Características

Según (ANDRADE CAYAMBE 2019) nos comenta que tiene las siguientes características:

- El sistema puede limitar el número de conexiones al mismo tiempo.
- Controlar el tiempo de conexión.
- Establecer una página web del portal cautivo con protocolo HTTPS.
- Redirigir a los usuarios a una página configurada por el administrador de red.
- proporcionar varios mecanismos de autenticación:
  - ✓ **Transparente. -** No se completa ningún dato
  - ✓ **Usuarios base de datos locales/remotos. –** Sí, en la base de datos se definen los usuarios permitidos para autenticarse.
  - ✓ **RADIUS. –** Usado para numerosos servidores RADIUS y sus capacidades son:
    - ✓ El sistema obliga a la re-autenticación.
    - ✓ **Actualiza** las cuentas de usuario.
    - ✓ Se autentica utilizando la dirección MAC, el nombre de usuario y contraseña.

c) Tipos de portal cautivo

(LEÓN LÓPEZ 2021), nos define que existen dos tipos de portales cautivos, estos son:

- **Portales cautivos por Software**

Son programas o paquetes que permiten implementar una puerta de enlace cautiva mediante la instalación en un sistema o servidor, algunos de estos programas son:

- ✓ PepperSpot
- ✓ NoCatAuuth
- ✓ Chillispot
- ✓ CoovaChilli
- ✓ AirMarshal
- ✓ ZeroShell
- ✓ Easy Captive
- ✓ PfSense
- ✓ OpenSplash
- ✓ Wicap
- ✓ Endian Firewall
- ✓ Clear OS 7

- **Portales Cautivos por Hardware**

Existe hardware que implementa el portal cautivo de forma nativa, algunos ejemplos de estos son:

- ✓ 3G/Wimax
- ✓ Aptilo Access Gateway
- ✓ Nomadix Gateway
- ✓ Antica PayBridge
- ✓ Cisco BBSM-Hotspo

En la figura 2.3 se puede apreciar una comparativa entre tres firewalls por software, en la cual se determina que el firewall PFSense es la que tiene mejores ventajas al resto, por tanto, para nuestra investigación se utilizó la implementación de dicho firewall. También comentar que se descartó los firewalls por hardware, debido a su costo que ronda los 800 a 1500 dólares americanos, como se muestra en la tabla Nº 2.2

Servicios	pfSense Community Edition (versión 2.5.2)	Endian Firewall Community (versión 3.3.2)	ClearOS 7 Community Edition (versión 7.2.0)
Servidor DNS	X	X	X
Servidor DHCP	X	X	X
VPN (IPsec y OpenVPN)	X	X	X
Balanceo de carga NAT	X	X	X
Tabla de estado	X	X	X
Proxy	X	X	X
Enrutamiento	X	X	
IP virtuales	X		
Portal cautivo	X		
Filtrado web	X	X	X
IPS	X	X	X
IDS	X	X	X
AntiSpam	X	X	X
Antivirus	X	X	X
Antiphishing			X
Servidor PPPoE	X		
Control de usuarios	X		X
Servidor SNMP		X	
Spyware	X		X

Figura 2.3 Comparativa entre Firewall por software

Fuente: (RUEDA CAMACHO, NUÑEZ AGURTO 2021)

Tabla 2.2 Diferencia de características entre Portal Cautivo Software y Portal Cautivo

PORTAL CAUTIVO						
MEDIANTE	**SOFTWARE**			**HARDWARE**		
Características	Bajo	Alto	Muy Alto	Bajo	Alto	Muy Alto
Precio	X				X	X
Dificultad Implementación		X			X	
Estabilidad		X				X
Hardware Adicional			X	X		

2.3.2. Seguridad de datos

Según (GÓMEZ VIEITES 2014) afirma que "La Seguridad Informática es la garantía de que los procesos realizados para tratar información se mantengan, en la medida de lo posible, libres de amenazas que puedan afectar su integridad, disponibilidad y fiabilidad" Para mantener un sistema informático seguro, se debe tener en cuenta los principios básicos de la seguridad informática, los cuales son:

- **Integridad:** es la garantía de que la información no puede ser alterada antes, durante ni después del proceso de transmisión.
- **Confidencialidad:** es garantizar que la información no puede ser conocida por personas no autorizadas para ello.
- **Disponibilidad:** asegurar que se puede tener acceso a la información cuando se requiera.

Por otro lado, (FRAYSSINET DELGADO 2014) La seguridad de la información es el conjunto de medidas preventivas y reactivas que las organizaciones toman para preservar y proteger la información, a fin de mantener sus dimensiones de confidencialidad, disponibilidad e integridad.

- **La confidencialidad** es la característica que evita el compartir información con personas o sistemas no autorizados.
- **La integridad** se refiere a mantener la precisión de la información generada originalmente, sin ser modificada por personas o procesos no autorizados.
- **La disponibilidad** se refiere a la habilidad de tener acceso a la información por parte de quienes la requieren, ya sea personal, procesos o aplicaciones.

También (ISO 27001 2022a), nos dice que la seguridad de la información cuenta con tres dimensiones que son: confidencialidad, integridad y disponibilidad de la información.

CAPITULO III

HIPÓTESIS

3.1. Hipótesis General

El Portal Cautivo influye significativamente para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO

3.2. Hipótesis Especificas

El Portal Cautivo influye significativamente para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO

El Portal Cautivo influye significativamente para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO

El Portal Cautivo influye significativamente para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO

3.3. Variables

3.3.1. Definición conceptual de las variables

- **Variable Independiente (X)**

✓ **Portal Cautivo**

Es una aplicación responsable de controlar y supervisar la entrada de clientes a organizaciones públicas y privadas de forma informatizada.

Es una página web con la que un usuario de una organización tanto pública como privada debe comunicarse antes de que se les conceda el acceso a las capacidades estándar de la organización.

- **Variable Dependiente (Y)**

✓ **Seguridad de datos**

Se encarga de evitar y encontrar el abuso de un sistema informático con la finalidad de resguardar la integridad y privacidad de los datos guardados.

Es la garantía de que los ciclos realizados para el tratamiento de los datos se mantienen desvinculados, más allá de lo que muchos considerarían posible, de los peligros que podrían influir en la integridad, disponibilidad y confiabilidad de los datos.

3.3.2. Definición operacional de las variables

- **Variable Independiente (X)**

✓ **Portal Cautivo**

Es una página web, que al estar conectadas a una red aparecen para solicitarnos datos adicionales antes de permitirnos acceder a Internet.

Una función clave del Portal cautivo es fortalecer la seguridad de la red al controlar mejor quién tiene acceso al requerir autenticación.

- **Variable Dependiente (Y)**

✓ **Seguridad de datos**

La seguridad de datos es la protección de la información digital contra accesos no autorizados, daños o robos, brindado mayor integridad de información en la transmisión de paquetes, confidencialidad y disponibilidad de la red.

3.3.3. Operacionalización de las variables

La operacionalización de variables se encuentra en el ANEXO 2.

CAPITULO IV

METODOLOGÍA

4.1. Método de la Investigación

4.1.1. Método General

El Método de Investigación Científica es una metodología usada para producir nuevos conocimientos con el respaldo de la comunidad científica. Se basa en la observación sistemática de los resultados, su implementación, análisis y ajuste de hipótesis para generar conocimientos válidos. Está caracterizado por su falsabilidad, reproducibilidad y repetición, que se comprueban mediante pruebas (HERNÁNDEZ SAMPIERI, MENDOZA TORRES 2018, p. 9).

4.1.2. Método Especifico

El Método Deductivo se usa en el razonamiento formal, donde la conclusión se obtiene a partir del juicio desde el que se parte. Implica un proceso de inferencia de arriba hacia abajo y deducción necesaria (ANDRADE NARANJO et al., 2018, p. 17).

4.2. Tipo de Investigación

Esta investigación es aplicada, ya que usa un pre-test y un post-test para hacer una comparación. Está destinada a responder a preguntas sobre lo que diferencia directamente a una cooperativa dentro de un ciclo de cooperación. Se recopilan datos de varias fuentes,

tanto esenciales como opcionales. Esto otorga importancia social, ya que su propósito no es generar nuevas informaciones teóricas, sino ofrecer resultados relacionados con los marcos directivos de las cooperativas. Su objetivo es beneficiar a los trabajadores y los individuos involucrados (HERNÁNDEZ SAMPIERI, MENDOZA TORRES 2018, p. 142).

4.3. Nivel de Investigación

El nivel de investigación es explicativo. En este contexto, se distinguen las causas y los efectos, el resultado final de una peculiaridad dada, y se planifican nuevas estrategias para entender las razones, los efectos finales, así como para intentar darnos cuenta de los retrasos y cómo podemos cambiarlos mediante la nueva programación de datos.

Se puede decir también que es explicativa, ya que trata de dar sentido a la justificación de por qué suceden las realidades a partir de la relación causa-efecto (HERNÁNDEZ SAMPIERI, MENDOZA TORRES 2018, p. 91).

4.4. Diseño de la Investigación

El diseño para esta investigación es pre experimental, lo que significa que se realiza un pre-test para evaluar la información y luego se lleva a cabo un post-test posterior. No tiene control sobre la variable que está revisando, sino que solo la mide. Es transversal ya que implica una instantánea única de tiempo para su giro de eventos. También es científica, ya que los profesionales entienden y aprenden cómo abordar el tema mediante la investigación de casos similares en varios campos. Para este caso, la mejora del desarrollo de software se trata generalmente y se aplica a esta unidad de análisis elegida (HERNÁNDEZ SAMPIERI, MENDOZA TORRES 2018, p. 15).

4.5. Población y Muestra

4.1.3. Población

La población está conformada por 256 usuarios, todos se conectan a la red inalámbrica del IESTP SAN PEDRO.

4.1.4. Muestra

La muestra es, generalmente, un subconjunto de la población total. Estos subconjuntos tienen un lugar definido en el conjunto que llamamos población y generalmente es imposible medir a toda la población, por lo que

se obtiene o elige una muestra que se espera que sea representativa de la población en su conjunto. Para verificar los ejemplos y establecer una metodología cuantitativa, los términos aleatorios y aleatorios sirven para describir una técnica mecánica relacionada con la probabilidad para determinar componentes o unidades individuales, aunque no explican el tipo de prueba o la técnica de examen que se utiliza (HERNÁNDEZ SAMPIERI, FERNÁNDEZ COLLADO, BAPTISTA LUCIO 2014, p. 175). Se muestra en la figura 4.1.

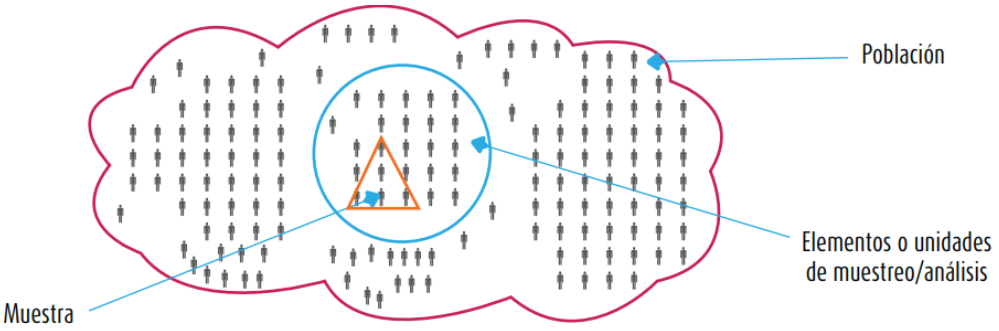


Figura 4.1 Población y muestra

fuente: (HERNÁNDEZ SAMPIERI, FERNÁNDEZ COLLADO, BAPTISTA LUCIO 2014).

La muestra se calcula por la fórmula para cálculo de la muestra de poblaciones finitas, el cual es la siguiente:

a.

$$n = \frac{(N)(Z)^2(p)(q)}{(d)^2(N-1)+(p)(q)(Z)^2}$$

Donde:

d = Precisión de la investigación = 0,05

Z = Nivel de seguridad = 95% = 1,96

p = Probabilidad de éxito = 0,5

q = Probabilidad de error = 0,5

N = Total de Población = 256

$$n = \frac{(256)(1.96)^2(0.5)(0.5)}{(0.05)^2(265-1)+(0.5)(0.5)(1.96)^2}$$

n= 154

4.6. Técnicas e Instrumentos de recolección de datos

La recolección de datos implica el desarrollo de un plan detallado de procedimientos para recopilar datos con un objetivo concreto. Se deben considerar los mecanismos para obtener información, los tipos de datos requeridos, las preguntas que hay que hacer y cómo procesar los datos (HERNÁNDEZ SAMPIERI, FERNÁNDEZ COLLADO, BAPTISTA LUCIO 2014, p. 198).

4.1.5. Técnica

Para esta investigación denominada Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO y los objetivos planteados. La técnica de recolección de datos que se utilizo es la observación, utilizamos esta técnica para identificar y analizar los datos que nos proporcionan.

4.1.6. Instrumento

Para el desarrollo del trabajo se utilizó la observación directa como instrumento. Esta técnica permite al investigador observar y recopilar datos por su propia experiencia, de acuerdo a las definiciones de Tamayo. Por lo tanto, con la observación directa, se pueden obtener datos directos a partir de la vivencia del investigador (TAMAYO Y TAMAYO 2004, p. 122).

También se utilizó el software Nessus, nos sirve para medir las vulnerabilidades de la red inalámbrica.

Por otro lado, se utilizó el Packet Loss Test, nos sirve para medir la perdida de paquetes y latencia.

4.7. Técnicas de procesamiento y análisis de datos

4.1.7. Técnicas de procesamiento de datos

Para el procesamiento de la información se utilizó el programa SPSS, que nos ayudó a manejar y constatar la información con el objeto de validar las hipótesis y su diferencia.

4.1.8. Técnicas de análisis de datos

Para realizar la técnica de análisis de datos se evaluó el Pre-Test mediante una cuantificación y su resultado se comparó con los datos del Post-Test. El análisis de los datos es de carácter cuantitativo y se empleó para realizar una prueba de hipótesis que se basa en mediciones numéricas, gráficos y análisis estadísticos.

4.8. Aspectos éticos de la investigación

Este estudio se apegará a lo señalado en el código de ética para la investigación científica en la Universidad Peruana los Andes con Resolución N°: 1750-2019-CU-Vrinv. Se protegerá la confidencialidad de la información y se recabará consentimiento informado, el documento de consentimiento informado se visualiza en el ANEXO 11.

CAPITULO V

RESULTADOS

5.1. Descripción del diseño tecnológico

El desarrollo del portal cautivo se describe en el ANEXO 12.

5.2. Descripción de resultados

5.2.1. Metodología de desarrollo del producto.

5.2.2. Validez del instrumento.

En esta investigación se utilizó una ficha de observación como instrumento para recopilar datos, la cual fue validada por tres expertos. Se visualiza dicha validación en el ANEXO 7,8 Y 9.

5.2.3. Presentación de la recolección de datos.

En esta investigación, se obtuvieron resultados que se realizó en el Instituto de Educación Superior Tecnológico Privado San Pedro, mediante la observación del antes y después de implementar el portal cautivo, con el objeto de evaluar la seguridad de datos en la red inalámbrica del instituto, para esta evaluación se aplicó un Pre Test con el objeto de conocer la condición inicial de los indicadores de la variable dependiente, donde se realizó la estadística descriptiva donde especificamos la media, el valor mínimo, máximo y grafico de barras; luego se implementó el portal cautivo y se realizó el Post Test, aplicando una nueva evaluación para comprobar las hipótesis planteadas en esta investigación. Se muestra a continuación las variables con sus indicadores respectivo procesados:

- **Variable Independiente:**
  - **Indicador: Tiempo promedio de respuesta de conexión en la red inalámbrica**

    Pre Test

    Los resultados obtenidos del indicador tiempo promedio de respuesta de conexión en la red inalámbrica, esta evaluación se realizó mediante el uso del Packet Loss Test, se midió el tiempo promedio de respuesta de conexión antes de la implementación del portal cautivo.

Tabla 5.1 Tiempo promedio de respuesta de conexión en la red inalámbrica pre test

ITEM	Identificación del equipo (usuario)	Fecha de verificación	Tiempo utilizado (ms)	observaciones
1	pc1	3/10/2022	111	
2	pc2	3/10/2022	99	
3	pc3	3/10/2022	95	
4	pc4	3/10/2022	105	
5	pc5	3/10/2022	96	
6	pc6	3/10/2022	109	
7	pc7	3/10/2022	116	
8	pc8	3/10/2022	124	
9	pc9	3/10/2022	127	
10	pc10	3/10/2022	128	
11	pc11	3/10/2022	140	
12	pc12	3/10/2022	119	
13	pc13	3/10/2022	126	
14	pc14	3/10/2022	95	
15	pc15	3/10/2022	99	
16	pc16	3/10/2022	133	
17	pc17	3/10/2022	96	
18	pc18	3/10/2022	90	
19	pc19	3/10/2022	129	
-				
-				
154	pc154	7/10/2022	97	

En la tabla N° 5.1, se puede observar promedio de respuesta de conexión en la red inalámbrica, estos datos se obtuvieron antes de la implementación del portal cautivo.

Post Test

Los resultados obtenidos del indicador tiempo promedio de respuesta de conexión en la red inalámbrica, esta evaluación se realizó mediante el uso del Packet Loss Test, se midió el tiempo promedio de respuesta de conexión después de la implementación del portal cautivo.

Tabla 5.2 Tiempo promedio de respuesta de conexión en la red inalámbrica post test

ITEM	Identificación del equipo (usuario)	Fecha de verificación	Tiempo utilizado (ms)	observaciones
1	jmuñoz	26/12/2022	74	
2	yespinoza	26/12/2022	67	
3	fquiñones	26/12/2022	66	
4	mtorres	26/12/2022	69	
5	gnoa	26/12/2022	49	
6	oarauco	26/12/2022	79	
7	lolivera	26/12/2022	82	
8	fflores	26/12/2022	68	
9	euribe	26/12/2022	51	
10	nmeza	26/12/2022	82	
11	mmendez	26/12/2022	75	
12	dpantoja	26/12/2022	56	
13	asinche	26/12/2022	88	
14	dquispe	26/12/2022	83	
15	rnoriega	26/12/2022	62	
16	hortiz	26/12/2022	72	
17	rmedina	26/12/2022	87	
-				
-				
154	dgonzales	30/12/2022	67	

En la tabla N° 5.2, se puede observar promedio de respuesta de conexión en la red inalámbrica, estos datos se obtuvieron después de la implementación del portal cautivo.

Los resultados estadísticos, tanto en el pre test como en el post test del Tiempo de respuesta de conexión se muestran en la tabla Nº 5.3

Tabla 5.3 Datos estadísticos del Tiempo de respuesta de conexión

Estadísticos

		PRE	POST
N	Válido	154	154
	Perdidos	0	0
Media		113,0000	70,2987
Desv. Desviación		14,90405	12,25339
Mínimo		90,00	49,00
Máximo		140,00	90,00

En la tabla Nº 5.3, se muestra el resultado estadístico del indicador tiempo de respuesta de conexión, en la cual se puede observar que en la evaluación pre test de la muestra se obtuvo un valor de 113,00 de media, mientras que el post test se obtuvo un valor de 70,30 de media. Lo cual explica que existe una diferencia entre el antes y después de la implementación del portal cautivo.

Manejando la información de la tabla Nº 5.3, se elabora la figura Nº 5.1, mostrando la diferencia que existe cuando se implementa el portal cautivo.

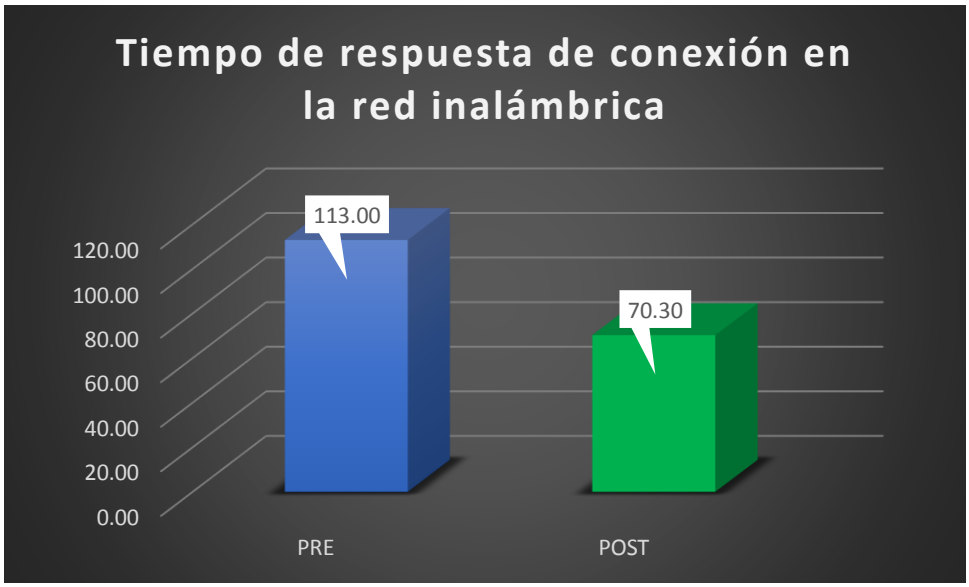


Figura 5.1 Tiempo de respuesta de conexión en la red inalámbrica

- **Variable Dependiente:**
  - **Dimensión de Confiabilidad: Indicador 1 Porcentaje de accesos a servicios no autorizados**

Pre Test

Los resultados obtenidos del indicador porcentaje de accesos a servicios no autorizados en el pre test, esta evaluación se realizó mediante el uso del software Nessus, se midió el porcentaje de vulneraciones antes de la implementación del portal cautivo.

Datos obtenidos del Pre Test: Porcentaje de accesos a servicios no autorizados

FICHA DE OBSERVACIÓN PRE-TEST

DIMENSION N° 01 Confidencialidad
INDICADOR N° 01 Porcentaje de accesos a servicios no autorizados

Tabla 5.4 Ficha de Observación Porcentaje de accesos a servicios no autorizados pre test

ITEM	Identificación del equipo (usuario)	Fecha de verificación	% de vuln.	observaciones
1	pc1	17/10/2022	61.20%	
2	pc2	17/10/2022	75.60%	
3	pc3	17/10/2022	77.60%	
4	pc4	17/10/2022	86.40%	
5	pc5	17/10/2022	64.00%	
6	pc6	17/10/2022	78.00%	
7	pc7	17/10/2022	73.20%	
8	pc8	17/10/2022	47.60%	
9	pc9	17/10/2022	57.60%	
10	pc10	17/10/2022	81.60%	
11	pc11	17/10/2022	72.00%	
12	pc12	17/10/2022	62.80%	
13	pc13	17/10/2022	71.60%	
14	pc14	17/10/2022	55.60%	
15	pc15	17/10/2022	70.00%	
16	pc16	17/10/2022	58.00%	
17	pc17	17/10/2022	83.60%	
18	pc18	17/10/2022	52.80%	
19	pc19	17/10/2022	78.80%	
-				
-				

154	pc154	17/10/2022	63.20%	

En la tabla N° 5.4, se puede observar el porcentaje de vulneraciones, estos datos se obtuvieron antes de la implementación del portal cautivo.

Post Test

Los resultados obtenidos del indicador porcentaje de accesos a servicios no autorizados en el post test, esta evaluación se realizó mediante el uso del software Nessus, se midió el porcentaje de vulneraciones con el portal cautivo implementado.

FICHA DE OBSERVACIÓN POST-TEST

DIMENSION N° 01 Confidencialidad
INDICADOR N° 01 Porcentaje de accesos a servicios no autorizados

Tabla 5.5 Ficha de Observación Porcentaje de accesos a servicios no autorizados post test

ITEM	Identificación del equipo (usuario)	Fecha de verificación	% de vuln.	observaciones
1	jmuñoz	26/12/2022	3.20%	
2	yespinoza	26/12/2022	3.60%	
3	fquiñones	26/12/2022	2.40%	
4	mtorres	26/12/2022	2.80%	
5	gnoa	26/12/2022	4.80%	
6	oarauco	26/12/2022	6.00%	
7	lolivera	26/12/2022	6.00%	
8	fflores	26/12/2022	4.40%	
9	euribe	26/12/2022	4.00%	
10	nmeza	26/12/2022	4.80%	
11	mmendez	26/12/2022	4.00%	
12	dpantoja	26/12/2022	4.40%	
13	asinche	26/12/2022	2.80%	
14	dquispe	26/12/2022	6.00%	
15	rnoriega	26/12/2022	4.40%	
16	hortiz	26/12/2022	3.60%	
17	rmedina	26/12/2022	3.60%	
18	wpumachahua	26/12/2022	6.00%	
19	mrafael	26/12/2022	5.60%	
-				
-				
154	dgonzales	30/12/2022	2.40%	

En la tabla N° 5.5, se puede observar el porcentaje de vulneraciones, estos datos se obtuvieron después de la implementación del portal cautivo.

Los resultados estadísticos, tanto en el pre test como en el post test del porcentaje de vulneraciones se muestran en la tabla Nº 5.6.

Tabla 5.6 Datos estadísticos del porcentaje de vulneraciones

Estadísticos

		PRE	POST
N	Válido	154	154
	Perdidos	0	0
Media		70,9688	3,9948
Desv. Desviación		9,86209	1,16506
Mínimo		47,60	2,00
Máximo		93,20	6,00

En la tabla Nº 5.6, se muestra el resultado estadístico del indicador porcentaje de accesos a servicios no autorizados, en la cual se puede observar que en la evaluación pre test de la muestra se obtuvo un valor de 70,97 de media, mientras que el post test se obtuvo un valor de 3,99 de media. Lo cual explica que existe una diferencia entre el antes y después de la implementación del portal cautivo.

Manejando la información de la tabla Nº 5.6, se elabora la figura Nº 5.2, mostrando la diferencia que existe cuando se implementa el portal cautivo.

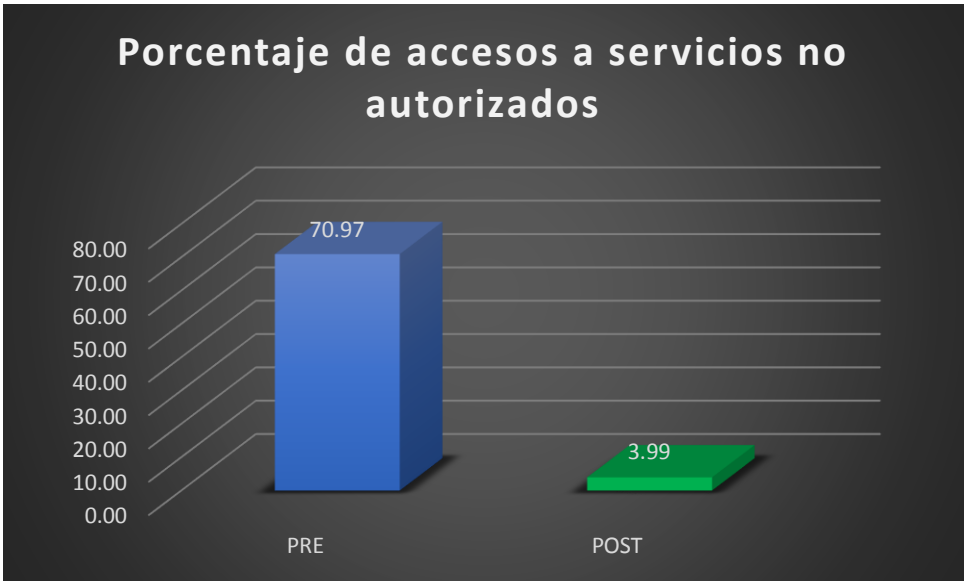


Figura 5.2 Porcentaje de accesos a servicios no autorizados

- **Dimensión de disponibilidad: Indicador 2, Tiempo promedio de respuesta de navegación WLAN y WAN**

Pre Test

Los resultados obtenidos del indicador tiempo promedio de respuesta de navegación WLAN y WAN en el pre test, esta evaluación se realizó mediante el uso del comando "ping", se midió el tiempo de respuesta en la navegación tanto interno como externo antes de la implementación del portal cautivo.

Datos obtenidos del Pre Test: Tiempo promedio de respuesta de navegación WLAN y WAN

FICHA DE OBSERVACIÓN PRE-TEST

DIMENSION N° 02 Disponibilidad
INDICADOR N° 02 Tiempo promedio de respuesta de navegación WLAN y WAN

Tabla 5.7 Ficha de Observación Tiempo promedio de respuesta de navegación WLAN y WAN pre test

ITEM	Nombre de la Web ó intranet	Identificación del equipo (usuario)	Fecha de verificación	Tiempo utilizado (ms)	observaciones
1	PAGINA WEB	pc1	3/10/2022	108	

2	PAGINA WEB	pc2	3/10/2022	104	
3	PAGINA WEB	pc3	3/10/2022	95	
4	PAGINA WEB	pc4	3/10/2022	121	
5	PAGINA WEB	pc5	3/10/2022	108	
6	PAGINA WEB	pc6	3/10/2022	130	
7	PAGINA WEB	pc7	3/10/2022	122	
8	PAGINA WEB	pc8	3/10/2022	99	
9	PAGINA WEB	pc9	3/10/2022	128	
10	PAGINA WEB	pc10	3/10/2022	124	
11	PAGINA WEB	pc11	3/10/2022	103	
12	PAGINA WEB	pc12	3/10/2022	91	
13	PAGINA WEB	pc13	3/10/2022	126	
14	PAGINA WEB	pc14	3/10/2022	128	
15	PAGINA WEB	pc15	3/10/2022	100	
16	PAGINA WEB	pc16	3/10/2022	112	
17	PAGINA WEB	pc17	3/10/2022	100	
18	PAGINA WEB	pc18	3/10/2022	101	
19	PAGINA WEB	pc19	3/10/2022	124	
-					
-					
154	ENTRE HOST	pc154	7/10/2022	130	

En la tabla N° 5.7, se puede observar el tiempo promedio de respuesta de navegación, estos datos se obtuvieron antes de la implementación del portal cautivo.

Post Test

Los resultados obtenidos del indicador tiempo promedio de respuesta de navegación WLAN y WAN en el pre test, esta evaluación se realizó mediante el uso del comando “ping”, se midió el tiempo de respuesta en la navegación tanto interno como externo después de la implementación del portal cautivo.

FICHA DE OBSERVACIÓN POST-TEST

DIMENSION N° 02 Disponibilidad
INDICADOR N° 02 Tiempo promedio de respuesta de navegación WLAN y WAN

Tabla 5.8 Ficha de Observación Tiempo promedio de respuesta de navegación WLAN y WAN post test

ITEM	Nombre de la Web ó intranet	Identificación del equipo (usuario)	Fecha de verificación	Tiempo utilizado (ms)	observaciones
1	PAGINA WEB	jmuñoz	26/12/2022	88	
2	PAGINA WEB	yespinoza	26/12/2022	66	
3	PAGINA WEB	fquiñones	26/12/2022	52	
4	PAGINA WEB	mtorres	26/12/2022	80	
5	PAGINA WEB	gnoa	26/12/2022	80	
6	PAGINA WEB	oarauco	26/12/2022	90	
7	PAGINA WEB	lolivera	26/12/2022	80	
8	PAGINA WEB	fflores	26/12/2022	52	
9	PAGINA WEB	euribe	26/12/2022	55	
10	PAGINA WEB	nmeza	26/12/2022	54	
11	PAGINA WEB	mmendez	26/12/2022	61	
12	PAGINA WEB	dpantoja	26/12/2022	50	
13	PAGINA WEB	asinche	26/12/2022	89	
14	PAGINA WEB	dquispe	26/12/2022	88	
15	PAGINA WEB	rnoriega	26/12/2022	82	
16	PAGINA WEB	hortiz	26/12/2022	72	
17	PAGINA WEB	rmedina	26/12/2022	56	
18	PAGINA WEB	wpumachahua	26/12/2022	50	
19	PAGINA WEB	mrafael	26/12/2022	56	
-					
-					
154	ENTRE HOST	dgonzales	30/12/2022	72	

En la tabla N° 5.8, se puede observar el tiempo promedio de respuesta de navegación, estos datos se obtuvieron después de la implementación del portal cautivo.

Los resultados estadísticos, tanto en el pre test como en el post test del tiempo promedio de respuesta de navegación se muestran en la tabla Nº 5.9.

Tabla 5.9 resultados estadísticos

Estadísticos

		PRE	POST
N	Válido	154	154
	Perdidos	0	0
Media		111,3701	68,4545
Desv. Desviación		12,49154	12,51670
Mínimo		90,00	49,00
Máximo		130,00	90,00

En la tabla Nº 5.9, se muestra el resultado estadístico del indicador Tiempo promedio de respuesta de navegación WLAN y WAN, en la cual se puede observar que en la evaluación pre test de la muestra se obtuvo un valor de 111.37 de media, mientras que el post test se obtuvo un valor de 68.45 de media. Lo cual explica que existe una diferencia entre el antes y después de la implementación del portal cautivo.

Manejando la información de la tabla Nº 5.9, se elabora la figura Nº 5.3, mostrando la diferencia que existe cuando se implementa el portal cautivo.

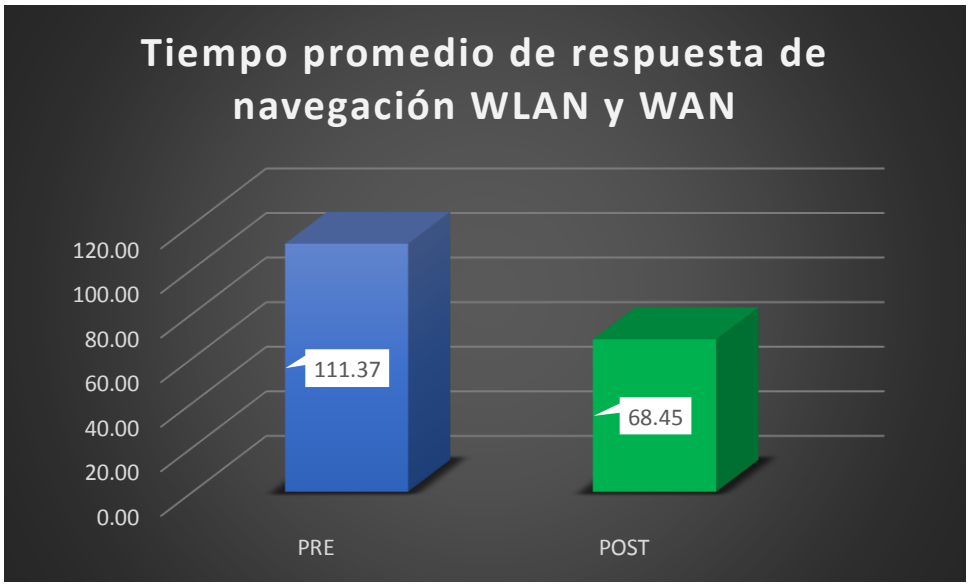


Figura 5.3 Tiempo promedio de respuesta de navegación WLAN y WAN

- **Dimensión de integridad: Indicador 3, Porcentaje de pérdida de paquetes de transmisión de datos**

Pre Test

Los resultados obtenidos del indicador porcentaje de pérdida de paquetes de transmisión de datos en el pre test, esta evaluación se realizó mediante el uso del Packet Loss Test, se midió porcentaje de pérdida de paquetes antes de la implementación del portal cautivo.

Datos obtenidos del Pre Test: Porcentaje de pérdida de paquetes de transmisión de datos

FICHA DE OBSERVACIÓN PRE-TEST

DIMENSION N° 03 Integridad
INDICADOR N° 03 Porcentaje de pérdida de paquetes de transmisión de datos

Tabla 5.10 Ficha de Observación Porcentaje de pérdida de paquetes de transmisión de datos pre test

ITEM	N° Paq. Enviados	Identificación del equipo (usuario)	Fecha de verificación	N° Paq. Perdidos	% Paq. Perdidos
1	1000	pc1	3/10/2022	37	3.70%
2	1000	pc2	3/10/2022	40	4.00%
3	1000	pc3	3/10/2022	50	5.00%
4	1000	pc4	3/10/2022	44	4.40%
5	1000	pc5	3/10/2022	33	3.30%
6	1000	pc6	3/10/2022	34	3.40%
7	1000	pc7	3/10/2022	31	3.10%
8	1000	pc8	3/10/2022	45	4.50%
9	1000	pc9	3/10/2022	40	4.00%
10	1000	pc10	3/10/2022	45	4.50%
11	1000	pc11	3/10/2022	47	4.70%
12	1000	pc12	3/10/2022	36	3.60%
13	1000	pc13	3/10/2022	35	3.50%
14	1000	pc14	3/10/2022	30	3.00%
15	1000	pc15	3/10/2022	40	4.00%
16	1000	pc16	3/10/2022	30	3.00%

17	1000	pc17	3/10/2022	34	3.40%
18	1000	pc18	3/10/2022	49	4.90%
19	1000	pc19	3/10/2022	31	3.10%
-					
-					
154	1000	pc154	7/10/2022	40	4.00%

En la tabla N° 5.10, se puede observar el porcentaje de pérdida de paquetes de transmisión de datos, estos datos se obtuvieron antes de la implementación del portal cautivo.

Post Test

Los resultados obtenidos del indicador porcentaje de pérdida de paquetes de transmisión de datos en el pre test, esta evaluación se realizó mediante el uso del Packet Loss Test, se midió porcentaje de pérdida de paquetes después de la implementación del portal cautivo.

FICHA DE OBSERVACIÓN POST-TEST

DIMENSION N° 03 Integridad
INDICADOR N° 03 Porcentaje de pérdida de paquetes de transmisión de datos

Tabla 5.11 Ficha de Observación Porcentaje de pérdida de paquetes de transmisión de datos post test

ITEM	N° Paq. Enviados	Identificación del equipo (usuario)	Fecha de verificación	N° Paq. Perdidos	% Paq. Perdidos
1	1000	jmuñoz	26/12/2022	4	0.40%
2	1000	yespinoza	26/12/2022	5	0.50%
3	1000	fquiñones	26/12/2022	3	0.30%
4	1000	mtorres	26/12/2022	2	0.20%
5	1000	gnoa	26/12/2022	6	0.60%
6	1000	oarauco	26/12/2022	2	0.20%
7	1000	lolivera	26/12/2022	7	0.70%
8	1000	fflores	26/12/2022	5	0.50%
9	1000	euribe	26/12/2022	1	0.10%
10	1000	nmeza	26/12/2022	1	0.10%
11	1000	mmendez	26/12/2022	7	0.70%

12	1000	dpantoja	26/12/2022	0	0.00%
13	1000	asinche	26/12/2022	5	0.50%
14	1000	dquispe	26/12/2022	8	0.80%
15	1000	rnoriega	26/12/2022	6	0.60%
16	1000	hortiz	26/12/2022	6	0.60%
17	1000	rmedina	26/12/2022	4	0.40%
18	1000	wpumachahua	26/12/2022	1	0.10%
19	1000	mrafael	26/12/2022	4	0.40%
-					
-					
154	1000	dgonzales	30/12/2022	7	0.70%

En la tabla N° 5.11, se puede observar el porcentaje de pérdida de paquetes de transmisión de datos, estos datos se obtuvieron después de la implementación del portal cautivo.

Los resultados estadísticos, tanto en el pre test como en el post test del porcentaje de pérdida de paquetes de transmisión de datos se muestran en la tabla Nº 5.12.

Tabla 5.12 Datos estadísticos de pérdida de paquetes de transmisión de datos

Estadísticos

		INTPRE	INTPOST
N	Válido	154	154
	Perdidos	0	0
Media		38,9481	4,6364
Desv. Desviación		5,66354	3,01373
Mínimo		30,00	,00
Máximo		50,00	10,00

En la tabla Nº 5.12, se muestra el resultado estadístico del indicador porcentaje de pérdida de paquetes de transmisión de datos, en la cual se puede observar que en la evaluación pre test de la muestra se obtuvo un valor de 38.95 de media, mientras que el post test se obtuvo un valor de 4.64 de media. Lo cual explica que existe una diferencia entre el antes y después de la implementación del portal cautivo.

Manejando la información de la tabla Nº 5.12, se elabora la figura Nº 5.4, mostrando la diferencia que existe cuando se implementa el portal cautivo.

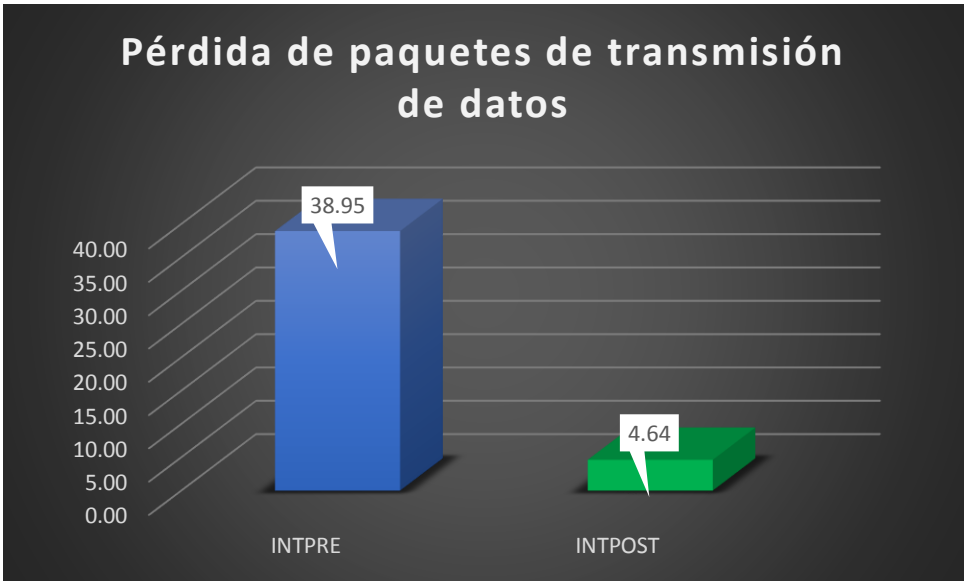


Figura 5.4 Pérdida de paquetes de transmisión de datos

5.3. Contrastación de hipótesis

5.3.1. Hipótesis General

1. Planteamiento de la Hipótesis Nula y Alterna

$\mathbf{H_0}$ = Hipótesis Nula

$\mathbf{H_1}$ = Hipótesis Alterna

Hipótesis $\mathbf{H_0}$: El Portal Cautivo NO influye significativamente para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO

Hipótesis $\mathbf{H_1}$: El Portal Cautivo influye significativamente para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO

2. Nivel de significancia o riesgo

Confianza = 95 %

Alfa = 5 %

3. Prueba de normalidad

Para muestras grandes (>50 individuos), se utiliza la prueba de normalidad mediante Kolmogorov-Smirnov (TAPIA, CEVALLOS 2021).

Criterio para determinar la Normalidad:

P-valor > = x

Aceptar H_0 = Los datos provienen de una distribución normal.

P-valor < x

Aceptar H_1 = Los datos NO provienen de una distribución normal.

Tabla 5.13 Kolmogorov-Smirnova

	Kolmogorov-Smirnov		
	Estadístico	gl	Sig.
PRE	,079	154	,021
POST	,199	154	,000

P-Valor (antes) = 0, 021 < x = 0.05

P-Valor (después) = 0,000 < x= 0.05

Los datos del Pre Test y Post Test provienen de una distribución NO normal, por consiguiente, se aplicó la prueba de Wilconxon. Como se puede verificar en la tabla 5.13.

4. Prueba estadística

Se utiliza la prueba de Wilconxon.

Tabla 5.14 Resumen de contrastes de hipótesis

Resumen de contrastes de hipótesis

	Hipótesis nula	Prueba	ig.	Decisión
	La mediana de diferencias entre PRE y POST es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	000	Rechace la hipótesis nula.

En la tabla 5.14 se puede observar que se rechaza la hipótesis nula.

5. Conclusiones Estadísticas

Se puede observar en la tabla Nº 11, el valor de la insignificancia es 0,000 este valor es menor que 0.05, por consiguiente, podemos afirmar que existen diferencias estadísticas significativas entre las muestras (Pre Test y Post Test). Entonces se rechaza la hipótesis nula, aceptando la hipótesis alterna con un 95 % de confianza.

Por lo tanto, se concluye que la implementación del Portal Cautivo SI influye significativamente para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO

5.3.2. Hipótesis Especifica 01

1. Planteamiento de la Hipótesis Nula y Alterna

$\mathbf{H_0}$ = Hipótesis Nula

$\mathbf{H_1}$ = Hipótesis Alterna

Hipótesis $\mathbf{H_0}$: El Portal Cautivo NO influye significativamente para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO

Hipótesis $\mathbf{H_1}$: El Portal Cautivo influye significativamente para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO

2. Nivel de significancia o riesgo

Confianza = 95 %

Alfa = 5 %

3. Prueba de normalidad

Para muestras grandes (>50 individuos), se utiliza la prueba de normalidad mediante Kolmogorov-Smirnov.

Criterio para determinar la Normalidad:

P-valor > = x

Aceptar $\mathbf{H_0}$ = Los datos provienen de una distribución normal.

P-valor < x

Aceptar $\mathbf{H_1}$ = Los datos NO provienen de una distribución normal.

Tabla 5.15 Kolmogorov-Smirnov

	Kolmogorov-Smirnov		
	Estadístico	gl	Sig.
PRE	,079	154	,021
POST	,199	154	,000

P-Valor (antes) = 0, 021 < x = 0.05

P-Valor (después) = 0,000 < x= 0.05

Los datos del Pre Test y Post Test provienen de una distribución NO normal, por consiguiente, se aplicó la prueba de Wilconxon. Como se puede verificar en la tabla 5.15.

4. Prueba estadística

Se utiliza la prueba de Wilconxon

Tabla 5.16 Resumen de contrastes de hipótesis

Resumen de contrastes de hipótesis

Hipótesis nula	Prueba	ig.	Decisión
La mediana de diferencias entre PRE y POST es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	000	Rechace la hipótesis nula.

En la tabla 5.16 se puede observar que se rechaza la hipótesis nula.

5. Conclusiones Estadísticas

Se puede observar en la tabla Nº 5.16, el valor de la insignificancia es 0,000 este valor es menor que 0.05, por consiguiente, podemos afirmar que existen diferencias estadísticas significativas entre las muestras (Pre Test y Post Test). Entonces se rechaza la hipótesis nula, aceptando la hipótesis alterna con un 95 % de confianza.

Por lo tanto, se concluye que la implementación del Portal Cautivo SI influye significativamente para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO

5.3.3. Hipótesis Especifica 02

1. Planteamiento de la Hipótesis Nula y Alterna

Hipótesis H_0 : El Portal Cautivo NO influye significativamente para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO

Hipótesis H_1 : El Portal Cautivo influye significativamente para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO

2. Nivel de significancia o riesgo

Confianza = 95 %

Alfa = 5 %

3. Prueba de normalidad

Para muestras grandes (>50 individuos), se utiliza la prueba de normalidad mediante Kolmogorov-Smirnov.

Criterio para determinar la Normalidad:

P-valor > = x

Aceptar H_0 = Los datos provienen de una distribución normal.

P-valor < x

Aceptar H_1 = Los datos NO provienen de una distribución normal.

Tabla 5.17 Kolmogorov-Smirnov

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
PRE	,099	154	,001
POST	,093	154	,002

P-Valor (antes) = 0, 001 < x = 0.05

P-Valor (después) = 0,002 < x= 0.05

Los datos del Pre Test y Post Test provienen de una distribución NO normal, por consiguiente, se aplicó la prueba de Wilconxon. Como se puede verificar en la tabla 5.17.

4. Prueba estadística

Se utiliza la prueba de Wilconxon

Tabla 5.18 Resumen de contrastes de hipótesis

Resumen de contrastes de hipótesis

	Hipótesis nula	Prueba	Sig.	Decisión
	La mediana de diferencias entre DISPPRE y DISPPOST es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechace la hipótesis nula.

En la tabla 5.18 se puede observar que se rechaza la hipótesis nula.

5. Conclusiones Estadísticas

Se puede observar en la tabla Nº 5.15, el valor de la insignificancia es 0,000 este valor es menor que 0.05, por consiguiente, podemos afirmar que existen diferencias estadísticas significativas entre las muestras (Pre Test y Post Test). Entonces se rechaza la hipótesis nula, aceptando la hipótesis alterna con un 95 % de confianza.

Por lo tanto, se concluye que la implementación del Portal Cautivo SI influye significativamente para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO

5.3.4. Hipótesis Especifica 03

1. Planteamiento de la Hipótesis Nula y Alterna

Hipótesis H_0 : El Portal Cautivo NO influye significativamente para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO

Hipótesis H_1 : El Portal Cautivo influye significativamente para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO

2. Nivel de significancia o riesgo

Confianza = 95 %

Alfa = 5 %

3. Prueba de normalidad

Para muestras grandes (>50 individuos), se utiliza la prueba de normalidad mediante Kolmogorov-Smirnov.

Criterio para determinar la Normalidad:

P-valor > = x

Aceptar H_0 = Los datos provienen de una distribución normal.

P-valor < x

Aceptar H_1 = Los datos NO provienen de una distribución normal.

Tabla 5.19 Kolmogorov-Smirnov

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
PRE	,088	154	,005
POST	,134	154	,000

P-Valor (antes)	=	0, 005	<	x = 0.05
P-Valor (después)	=	0,000	<	x= 0.05

Los datos del Pre Test y Post Test provienen de una distribución NO normal, por consiguiente, se aplicó la prueba de Wilconxon. Como se puede verificar en la tabla 5.19.

4. Prueba estadística

Se utiliza la prueba de Wilconxon

Tabla 5.20 Resumen de contrastes de hipótesis

Resumen de contrastes de hipótesis

	Hipótesis nula	Prueba	Sig.[a,b]	Decisión
	La mediana de diferencias entre INTPRE y INTPOST es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechace la hipótesis nula.

En la tabla 5.20 se puede observar que se rechaza la hipótesis nula.

5. Conclusiones Estadísticas

Se puede observar en la tabla Nº 20, el valor de la insignificancia es 0,000 este valor es menor que 0.05, por consiguiente, podemos afirmar que existen diferencias estadísticas significativas entre las muestras (Pre Test y Post Test). Entonces se rechaza la hipótesis nula, aceptando la hipótesis alterna con un 95 % de confianza.

Por lo tanto, se concluye que la implementación del Portal Cautivo SI influye significativamente para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO**.**

CAPITULO VI

ANÁLISIS Y DISCUSIÓN DE RESULTADOS

6.1. Discusión de resultados

En base a los resultados de la presente investigación se analiza una comparativa de un antes y un después sobre los datos obtenidos en las dimensiones de confiabilidad, disponibilidad e integridad con sus respectivos indicadores de porcentaje de accesos a servicios no autorizados, tiempo promedio de respuesta de navegación WLAN y WAN y porcentaje de pérdida de paquetes de transmisión de datos con la finalidad de determinar la influencia del portal cautivo para administrar la seguridad de datos de la red inalámbrica del IESTP San Pedro.

1. La intención de identificar de qué manera influye el Portal Cautivo para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO motivo del presente trabajo, el cual demostró que, en la dimensión de confiabilidad, el porcentaje de accesos a servicios no autorizados, se reduce el porcentaje promedio de 70.97 % (Pre Test) a 3.99 % de accesos no autorizados (Post Test), la disminución es de 66.98 % de accesos a servicios no autorizados.

   Estos hallazgos guardan similitud con la tesis titulada "Rediseño de la red de datos para mejorar la seguridad informática de una Municipalidad" de (POMALAYA MONTERO 2018), donde menciona como conclusión: Se concluye que el tiempo promedio de porcentaje de accesos a servicios no autorizados con la red actual (Pre Test) viene hacer de 94.4% y el porcentaje de accesos a servicios no autorizados con el diseño propuesto (Post Test). es de 1.6%, dando como resultado una disminución

de 92.8% de accesos a los servicios no autorizados, determinando una mejora significativa de la confidencialidad de la información en la Municipalidad de Huamancaca Chico.

En esta investigación los resultados indican una disminución del 66.98 % de accesos a servicios no autorizados en la red inalámbrica del IESTP San Pedro.

(ISO 27001 2022b) La información o los datos confidenciales deben divulgarse únicamente a usuarios autorizados, con la finalidad de garantizar la confidencialidad y salvaguardar los datos de intrusos no deseados o que van a causar daño.

2. La intención de identificar de qué manera influye el Portal Cautivo para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO, motivo del presente trabajo, el cual demostró que, en la dimensión de disponibilidad, el tiempo promedio de respuesta de navegación WLAN y WAN, se reduce el tiempo de respuesta de navegación de 111.37 ms (Pre Test) a 68.45 ms (Post test), la disminución es de 42.92 ms para el tiempo promedio de respuesta de navegación.

   Estos hallazgos guardan similitud con la tesis titulada "Rediseño de la red de datos para mejorar la seguridad informática de una Municipalidad" de (POMALAYA MONTERO 2018), donde menciona como conclusión: Con la red de datos existente el tiempo de respuesta de las aplicaciones informáticas a nivel Lan es de 190ms (Pre Test) y 40.5 Obtenido con el diseño de red de datos propuesto (Post Test). y a nivel Wan de 256.5 obtenido con la red actual (Pre Test) y 44.33 obtenido con el diseño de red de datos propuesto (Post Test).

   En esta investigación los resultados indican una disminución del 42.92 ms del tiempo promedio de respuesta de navegación WLAN y WAN en la red inalámbrica del IESTP San Pedro.

   (ISO 27001 2022b) Cuando un sistema no funciona regularmente, la disponibilidad de la información se ve afectada y afecta significativamente a los usuarios. Otro factor que afecta la disponibilidad es el tiempo. Si un sistema informático no puede entregar información de manera eficiente, la disponibilidad se ve comprometida.

3. La intención de identificar de qué manera influye el Portal Cautivo para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO, motivo del presente trabajo, el cual demostró que, en la dimensión de integridad, el porcentaje de pérdida de paquetes de transmisión de datos, se reduce el porcentaje de perdida de

paquetes de 38.95 % (Pre Test) a 4.64 % (Post Test), la disminución es de 34.31 % de perdida de paquetes.

Estos hallazgos guardan similitud con la tesis titulada "Rediseño de la red de datos para mejorar la seguridad informática de una Municipalidad" de (POMALAYA MONTERO 2018), donde menciona como conclusión: Se concluye también que el porcentaje de pérdida de paquetes de transmisión en la red obtenido con la red actual (Pre Test) es de 8.15% y 0.62% Obtenido con el diseño de red de datos propuesto (Post Test). Mostrando una disminución de un porcentaje valorativo de 7.53%, Determinando una mejora significativa de la Integridad de la información en la Municipalidad de Huamancaca Chico.

En esta investigación los resultados indican una disminución del 34.31 % de pérdida de paquetes de transmisión de datos en la red inalámbrica del IESTP San Pedro.

(ISO 27001 2022b) La integridad de la información se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios.

4. La intención de determinar de qué manera influye el Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO motivo del presente trabajo, el cual demostró que, de acuerdo a los resultados de indicadores de estudio, se puede determinar que la implementación del portal cautivo mejora significativamente la administración de la seguridad de datos de la red inalámbrica del IESTP San Pedro.

   Estos hallazgos guardan similitud con la tesis titulada "Rediseño de la red de datos para mejorar la seguridad informática de una Municipalidad" de (POMALAYA MONTERO 2018), donde menciona como conclusión: Finalmente después de haber obtenido resultados satisfactorios de los indicadores de estudio, se concluye que el rediseño de la red de datos mejora la seguridad informática en la Municipalidad de Huamancaca Chico. Por ende, se determina que es viable. Del mismo modo que la tesis titulada "Evaluación del Firewall de Frontera Free Pfsense para proteger la confidencialidad, integridad y disponibilidad de la información de compañías de responsabilidad limitada en Riobamba año 2021" de (RUIZ ANDINO 2022), donde concluye: De acuerdo con los resultados obtenidos, implementar el Firewall PfSense

reduce significativamente la Probabilidad de Amenaza y Magnitud del Daño, se concluye que, el uso del Firewall PfSense mejora la seguridad, integridad y confidencialidad de la información que tiene la compañía limita, se recomienda el uso de este software dentro de la red LAN de las Compañías de Responsabilidad Limitada de la Ciudad de Riobamba u otras entidades que necesiten fortalecer la seguridad informática.

(ISO 27001 2022b) La seguridad de la información tiene por objetivo la protección de la confidencialidad, integridad y disponibilidad de los datos de los sistemas de información de cualquier amenaza y de cualquiera que tenga intenciones maliciosas.

CONCLUSIONES

A manera de colofón se expresa lo siguiente:

1. Se concluye en la presente investigación que, después de la implementación del portal cautivo, el porcentaje de accesos a servicios no autorizados disminuye de 70.97 % (Pre Test) a 3.99 % de accesos no autorizados (Post Test), la disminución es de 66.98 % de accesos a servicios no autorizados, por lo tanto, se identifica una mejora significativa para administrar la confidencialidad de datos en la red inalámbrica del IESTP SAN PEDRO.
2. Se concluye en la presente investigación que, después de la implementación del portal cautivo, el tiempo de respuesta de navegación disminuye de 111.37 ms (Pre Test) a 68.45 ms (Post test), la disminución es de 42.92 ms para el tiempo promedio de respuesta de navegación, por lo tanto, se identifica una mejora significativa para administrar la disponibilidad de datos en la red inalámbrica del IESTP SAN PEDRO.
3. Se concluye en la presente investigación que, después de la implementación del portal cautivo, el porcentaje de perdida de paquetes disminuye de 38.95 % (Pre Test) a 4.64 % (Post Test), la disminución es de 34.31 % de perdida de paquetes, por lo tanto, se identifica una mejora significativa para administrar la integridad de datos en la red inalámbrica del IESTP SAN PEDRO.
4. Finalmente, después de obtener resultados satisfactorios de los indicadores de estudio, se concluye que la implementación del portal cautivo mejora significativamente la administración de la seguridad de datos de la red inalámbrica del IESTP SAN PEDRO.

RECOMENDACIONES

1. Se recomienda a los administradores de redes, implementar un firewall como PFSense con un portal cautivo para administrar la confidencialidad de datos en una red inalámbrica, teniendo en cuenta que es de uso libre. Se puede aplicar a otras instituciones o empresas, mejorando de forma significativa la administración de la confidencialidad de datos.
2. Se recomienda a los administradores de redes, implementar un firewall como PFSense con un portal cautivo para administrar la disponibilidad de datos en una red inalámbrica, teniendo en cuenta que es de uso libre. Se puede aplicar a otras instituciones o empresas, mejorando de forma significativa la administración de la disponibilidad de datos.
3. Se recomienda a los administradores de redes, implementar un firewall como PFSense con un portal cautivo para administrar la integridad de datos en una red inalámbrica, teniendo en cuenta que es de uso libre. Se puede aplicar a otras instituciones o empresas, mejorando de forma significativa la administración de la integridad de datos.
4. Se recomienda a los directivos de los centros de educación, implementar un firewall como PFSense con un portal cautivo para administrar la seguridad de datos en una red inalámbrica, teniendo en cuenta que es de uso libre. Se puede aplicar a otras instituciones o empresas, mejorando de forma significativa la administración de la seguridad de datos.

REFERENCIAS BIBLIOGRÁFICAS

ALFONSO, C. d. y CABALLER MIGUEL, H. v., 2005. *Seguridad en Redes Inalámbricas*. Valencia.

ANDRADE CAYAMBE, Linda Inés, 2019. Diseño y simulación de portal cautivo, que permita: autenticación, aplicación de herramientas, políticas de seguridad, QoS y sonda de red para el filtrado de contenido mediante equipo UTM en la CISC-CINT. . 2019.

ANDRADE NARANJO, Diego Santiago, CABEZAS MEJÍA, Edison Damián y TORRES SANTAMARÍA, Johana Belén, 2018. Introducción a la Metodología de la Investigación Científica | ISBN 978-9942-765-44-4 - Libro. en línea. 2018. [Accedido 29 octubre 2022]. Recuperado a partir de: https://isbn.cloud/9789942765444/introduccion-a-la-metodologia-de-la-investigacion-cientifica/

ANDREU, Joaquín, 2011. Redes inalámbricas (Servicios en red) - Joaquín Andreu - Google Libros. en línea. 2011. [Accedido 14 octubre 2022]. Recuperado a partir de: https://books.google.com.pe/books/about/Redes_inal%C3%A1mbricas_Servicios_en_red.html?id=98_TAwAAQBAJ&redir_esc=y

BACA URBINA, Gabriel, 2016. *Introducción a la Seguridad Informática* en línea. [Accedido 17 octubre 2022]. Recuperado a partir de: https://books.google.es/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=firewall+seguridad&ots=0XQA2EAdHv&sig=X-uK-J8jXb1caRkM35IlEaA_ggI#v=onepage&q=firewall%20seguridad&f=false

CISCO SYSTEM, 2011. CCDA 640-864 Official Cert Guide, 4th Edition. en línea. 2011. pp. 699. [Accedido 23 enero 2023]. Recuperado a partir de: https://www.ciscopress.com/store/ccda-640-864-official-cert-guide-9781587142574

CISCO, 2022a. Estándares Inalámbricos - Cisco Community. en línea. 2022. [Accedido 24 enero 2023]. Recuperado a partir de: https://community.cisco.com/t5/blogs-wireless-mobility/est%C3%A1ndares-inal%C3%A1mbricos/ba-p/3365301

CISCO, 2022b. ¿Qué es Wi-Fi 6? Tecnología Wi-Fi de última generación - Cisco. en línea. 2022. [Accedido 24 enero 2023]. Recuperado a partir de: https://www.cisco.com/c/es_mx/products/wireless/what-is-wi-fi-6.html

CISCO, 2022c. Enable a Captive Portal on your Cisco Wireless Network - Cisco. en línea. 2022. [Accedido 31 enero 2023]. Recuperado a partir de: https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-300-series-wireless-access-points/smb4937-enable-a-captive-portal-on-your-cisco-wireless-network.html

DÁVALOS CASTILLA, Laura, CABAÑAS VICTORIA, Vladimir y ESTRADA, Melissa Blanqueto, 2013. ADMINISTRACIÓN Y CONTROL DE LOS RECURSOS DE UNA RED DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE UN GATEWAY DE DISTRIBUCIÓN LIBRE. . 2013.

DELOITTE, 2019. *Ciber Riesgos y Seguridad de la Información en América Latina & Caribe Tendencias 2019* en línea. [Accedido 22 octubre 2022]. Recuperado a partir de: https://www2.deloitte.com/pe/es/pages/risk/articles/ciber-riesgos-y-seguridad-de-la-info-en-america-latina-y-caribe.html

ECN, 2018. Ataques tipo sobre redes WiFi. en línea. 2018. [Accedido 22 octubre 2022]. Recuperado a partir de: https://www.e-channelnews.com/top-5-most-dangerous-public-wifi-attacks/

FIREWALLHARDWARE, 2021. Firewall Hardware Sizing Guide. en línea. 2021. [Accedido 23 enero 2023]. Recuperado a partir de: https://www.firewallhardware.it/en/firewall-hardware-sizing-guide/

FRAYSSINET DELGADO, Maurice, 2014. *Taller de Implementación de la norma ISO 27001* en línea. Recuperado a partir de: www.ongei.gob.pe

GÓMEZ VIEITES, Álvaro, 2014. Enciclopedia de la Seguridad Informática. 2ª edición - Álvaro Gómez Vieites - Google Libros. en línea. 2014. [Accedido 14 octubre 2022]. Recuperado a partir de: https://books.google.com.mx/books?id=Bq8-DwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

GUEVARA CAJAS, Julián Fernando y QUIZHPI LEÓN, David Andrés, 2017. *DISEÑO DE LARED DE CAMPUS DE LA EMPRESA "EQUIPOS Y SUMINISTROS DE TELECOMUNICACIONES EQUYSUM" DE LA CIUDAD DE QUITO*.

HERNÁNDEZ SAMPIERI, Roberto, FERNÁNDEZ COLLADO, Carlos y BAPTISTA LUCIO, María del Pilar, 2014. *METODOLOGÍA de la investigación* en línea. Recuperado a partir de: www.FreeLibros.com

HERNÁNDEZ SAMPIERI, Roberto y MENDOZA TORRES, Paulina, 2018. Metodología de la investigación. en línea. 2018. pp. 752. [Accedido 21 octubre 2022]. Recuperado a partir de: https://books.google.com/books/about/METODOLOG%C3%8DA_DE_LA_INVESTIGACI%C3%93N.html?hl=es&id=jly9vQEACAAJ

ISO 27001, 2022a. NORMA ISO 27001:2013. en línea. 2022. [Accedido 11 febrero 2023]. Recuperado a partir de: https://normaiso27001.es/#

ISO 27001, 2022b. REFERENCIAS NORMATIVAS ISO 27000 - Glosario de términos ISO 27001. en línea. 2022. [Accedido 12 febrero 2023]. Recuperado a partir de: https://normaiso27001.es/referencias-normativas-iso-27000/#def310

ISO CENTRAL SECRETARIAT, 2022. ISO - ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements. en línea. 2022. [Accedido 19 febrero 2023]. Recuperado a partir de: https://www.iso.org/standard/54534.html

IZASKUN PELLEJERO, Fernando Andreu y LESTA, Amaia, 2006. Fundamentos y Aplicaciones de Seguridad en Redes WLAN: Fundamentos y ... - Fernando Andreu, Izaskun Pellejero, Amaia Lesta - Google Libros. en línea. 2006. [Accedido 14 octubre 2022]. Recuperado a partir de: https://books.google.com.ec/books?id=k3JuVG2D9lMC&pg=PA160&lpg=PA160&dq=fundamentos+de+seguridad+en+redes+fernando+andreu+pdf&source=bl&ots=8Eug2qjXcO&sig=dySXtIpX2JgIMUHDkANwHpjfu9Q&hl=es&sa=X&ved=0ahUKEwif97XPuNbSAhUmqFQKHSBzCfMQ6AEIIzAC#v=onepage&q=fun&f=false

KASPERSKY, 2022. MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky. en línea. 2022. [Accedido 28 enero 2023]. Recuperado a partir de: https://cybermap.kaspersky.com/es

LAZO JAIME, Guillermo Bismarck y SALTOS PONCE, Mayra Lorena, 2020. *Implementación de una nueva infraestructura Wireless en la carrera de Ingeniería en Sistemas Computacionales, a través de un Portal Cautivo mediante la integración con Access Point de Cisco Meraki, teniendo una administración en la nube.*

LEÓN LÓPEZ, Diego Enrique, 2021. *ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE UN PORTAL CAUTIVO PARA MEJORAR LA SEGURIDAD DE TRANSMISIÓN DE DATOS EN LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ.*

LINO LÓPEZ, Juan Jesús, 2022. "DISEÑO E IMPLEMENTACIÓN DE UNA RED DE SEGURIDAD INFORMÁTIC A PARA MEJORAR LA ADMINISTRACIÓN DE DATOS BASADO EN LA NORMA ISO/IEC 27002:2013, EN LA EMPRESA A.C.E SACO OLIVEROS -SEDE MONTERRICO. LIMA 2021" 2022.

LÓPEZ JURADO, Carlos, 2021. ¿Qué es una red inalámbrica y qué tipos existen? - CCM. en línea. 2021. [Accedido 14 octubre 2022]. Recuperado a partir de: https://es.ccm.net/contents/818-redes-inalambricas

MICROSOFT, 2022. Protocolo de autenticación extensible (EAP) para el acceso a la red | Microsoft Learn. en línea. 2022. [Accedido 23 enero 2023]. Recuperado a partir de: https://learn.microsoft.com/es-es/windows-server/networking/technologies/extensible-authentication-protocol/network-access

MIGUEL PÉREZ, Julio César, 2015. Protección de Datos y Seguridad de la Información - Julio César Miguel Pérez - Google Libros. en línea. 2015. [Accedido 14 octubre 2022]. Recuperado a partir de: https://books.google.com.pe/books/about/Protecci%C3%B3n_de_Datos_y_Seguridad_de_la_I.html?id=To6fDwAAQBAJ&redir_esc=y

MINER, Matthew, 2022. Packet Loss Test – Prueba la calidad de tu conexión. en línea. 2022. [Accedido 27 enero 2023]. Recuperado a partir de: https://es.packetlosstest.com/

MORALES CHAPMAN, Julio Armando y TORRES LEIVA, Neyser, 2021. *Implementación de una Red Privada Virtual basada enla metodología PPDIOO paramejorar la seguridad informática en la red de Lima Traylers S.A.C.*

NETGATE, 2019. Pfsense Traffic Shappe. en línea. 2019. [Accedido 17 octubre 2022]. Recuperado a partir de: https://docs.netgate.com/pfsense/en/latest/trafficshaper/index.html

NETGATE, 2022a. Paquetes — Paquete pfBlocker-NG | Documentación de pfSense. en línea. 2022. [Accedido 23 enero 2023]. Recuperado a partir de: https://docs.netgate.com/pfsense/en/latest/packages/pfblocker.html

NETGATE, 2022b. Captive Portal on pfSense. en línea. 2022. [Accedido 1 febrero 2023]. Recuperado a partir de: https://www.netgate.com/pfsense-plus-software/resources/videos-captive-portal-onpfsense

NTOP, 2022. ntop – High Performance Network Monitoring Solutions based on Open Source and Commodity Hardware. en línea. 2022. [Accedido 23 enero 2023]. Recuperado a partir de: https://www.ntop.org/

PFSENSE, 2022. pfSense Community Edition. en línea. 2022. [Accedido 30 noviembre 2022]. Recuperado a partir de: https://www.pfsense.org

PIARPUEZÁN LÓPEZ, Jefferson Alexander y RIASCOS ORTIZ, Dany Alexander, 2019. *Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020*.

POMALAYA MONTERO, Karol Pamela, 2018. *REDISEÑO DE LA RED DE DATOS PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE UNA MUNICIPALIDAD*.

RAMÍREZ SÁNCHEZ, Jesús y VILLANUEVA LENDECHY, Héctor Manuel, 2008. *LAS REDES INALÁMBRICAS EN LAS ORGANIZACIONES* en línea. Recuperado a partir de: http://www.itu.int/ITU-R/study-groups/was/index-es

RIVEROS PARAGUAY, Jhon Kenedy, 2019. Implementación de políticas de seguridad informática para mejorar el acceso y la seguridad lógica de la Red en la Oficina Departamental de Estadística e Informática de Junín. 2019.

RUEDA CAMACHO, Carlos Steveen y NUÑEZ AGURTO, Alberto Daniel, 2021. ANÁLISIS COMPARATIVO DE UN UNIFIED THREAT MANAGEMENT (UTM) OPEN-SOURCE PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LAS PYMES. *Revista de Ciencias de Seguridad y Defensa*. en línea. 31 diciembre 2021. Vol. 6, no. 4, pp. 14. [Accedido 23 enero 2023]. DOI 10.24133/RCSD.VOL06.N04.2021.05.

RUIZ ANDINO, Edison Fernando, 2022. *Evaluación del Firewall de Frontera Free Pfsense para proteger la confidencialidad, integridad y disponibilidad de la información de compañías de responsabilidad limitada en Riobamba año 2021*.

SALAZAR, Jordi, 2016. *REDES INALÁMBRICAS* en línea. Recuperado a partir de: http://www.techpedia.eu

SÁNCHEZ REVOLLEDO, Jimmy Gustavo y FERRER DULCE, Sixto Moisés, 2021. *"IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD(COS) PARA MEJORAR LA SEGURIDAD EN LA RED INFORMÁTICA DE LAUNIVERSIDADNACIONALDELSANTA"*.

SIERRA CALLEJA, Emmanuel, 2015. Portal Cautivo | PDF | Red de computadoras | Wifi. en línea. 2015. [Accedido 14 octubre 2022]. Recuperado a partir de: https://es.scribd.com/doc/266485604/Portal-Cautivo

TAMAYO Y TAMAYO, Mario, 2004. El proceso de la investigación científica. en línea. 2004. [Accedido 28 octubre 2022]. Recuperado a partir de: https://books.google.com.mx/books?id=BhymmEqkkJwC&printsec=frontcover&hl=es#v=onepage&q&f=false

TAPIA, Carlos Ernesto Flores y CEVALLOS, Karla Lissette Flores, 2021. PRUEBAS PARA COMPROBAR LA NORMALIDAD DE DATOS EN PROCESOS PRODUCTIVOS: ANDERSON-DARLING, RYAN-JOINER, SHAPIRO-WILK Y KOLMOGÓROV-SMIRNOV. *Societas*. en línea. julio 2021. [Accedido 8 febrero 2023]. Recuperado a partir de: https://revistas.up.ac.pa/index.php/societas/article/view/2302/2137

TENABLE, 2022. Descargue la Evaluación de vulnerabilidades | Nessus® | Tenable®. en línea. 2022. [Accedido 27 enero 2023]. Recuperado a partir de: https://es-la.tenable.com/products/nessus

WORLD ECONOMIC FORUM, 2023. El Foro Económico Mundial. en línea. 2023. [Accedido 25 febrero 2023]. Recuperado a partir de: https://es.weforum.org/

ANEXOS

Anexo 1: Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	METODOLOGÍA
Problema general	**Objetivo general:**	**Hipótesis general**	**VARIABLE 1:** Independiente Portal Cautivo **DIMENSIONES**: Rendimiento **VARIABLE 2:** Dependiente Seguridad de datos **DIMENSIONES:** Confidencialidad Disponibilidad Integridad	**MÉTODO DE INVESTIGACIÓN:** **Método General:** Método Científico **Método Especifico:** Hipotético Deductivo **TIPO DE INVESTIGACIÓN:** Aplicada **ALCANCE DE LA INVESTIGACIÓN**: Nivel explicativo **DISEÑO DE LA INVESTIGACIÓN:** Diseño pre experimental **POBLACIÓN**: 256 **MUESTRA**: 154 **TÉCNICAS Y/O INSTRUMENTOS DE RECOLECCIÓN DE DATOS:** Ficha de observación Nessus Packet Loss Test **PROCESAMIENTO DE LA INFORMACIÓN:** Ficha de observación SPSS
¿De qué manera influye el Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO?	Determinar de qué manera influye el Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO	El Portal Cautivo influye significativamente para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO		
Problema específico	**Objetivos específicos**	**Hipótesis específicas**		
¿De qué manera influye el Portal Cautivo para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO?	Identificar de qué manera influye el Portal Cautivo para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO	El Portal Cautivo influye significativamente para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO		
¿De qué manera influye el Portal Cautivo para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO?	Identificar de qué manera influye el Portal Cautivo para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO	El Portal Cautivo influye significativamente para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO		
¿De qué manera influye el Portal Cautivo para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO?	Identificar de qué manera influye el Portal Cautivo para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO	El Portal Cautivo influye significativamente para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO		

Anexo 2: Matriz de operacionalización de variables

Variables		Definición	Dimensiones	Indicadores	Instrumento
Independiente	**Portal Cautivo**	Es una página web, que al estar conectadas a una red aparecen para solicitarnos datos adicionales antes de permitirnos acceder a Internet. Una función clave del Portal cautivo es fortalecer la seguridad de la red al controlar mejor quién tiene acceso al requerir autenticación.	Rendimiento	Tiempo promedio de respuesta de conexión en la red inalámbrica	Ficha de Observación/ Nessus/Packet Loss Test
Dependiente	Seguridad de datos	La seguridad de datos es la protección de la información digital contra accesos no autorizados, daños o robos, brindado mayor integridad de información en la transmisión de paquetes, confidencialidad y disponibilidad de la red.	Confidencialidad	Porcentaje de accesos a servicios no autorizados	Ficha de Observación/ Nessus/Packet Loss Test
			Disponibilidad	Tiempo promedio de respuesta de navegación WLAN y WAN.	Ficha de Observación/ Nessus/Packet Loss Test
			Integridad	Porcentaje de pérdida de paquetes de transmisión de datos	Ficha de Observación/ Nessus/Packet Loss Test

Anexo 3: Matriz de operacionalización del instrumento

VARIABLE	SUB VARIABLE O DIMENSIONES	INDICADORES	ÍTEM O REACTIVOS	ESCALA VALORATIVA	INSTRUMENTO
Seguridad de datos	Confidencialidad	Porcentaje de accesos a servicios no autorizados	Porcentaje de accesos no autorizados, se mide en %	% de accesos no autorizados (vulnerabilidad)	Ficha de Observación Nessus Packet Loss Test
	Disponibilidad	Tiempo promedio de respuesta de navegación WLAN y WAN.	Tiempo promedio de dar respuesta entre host y a páginas web, se mide en ms	Milisegundos (ms)	Ficha de Observación Nessus Packet Loss Test
	Integridad	Porcentaje de pérdida de paquetes de transmisión de datos	Porcentaje de perdida de paquetes en una transmisión de datos, se mide en %	% de perdida de paquetes	Ficha de Observación Nessus Packet Loss Test

Anexo 4: Instrumento de investigación del indicador Nº 1

INSTRUMENTO DE MEDICION N° 01

"PORTAL CAUTIVO PARA ADMINISTRAR LA SEGURIDAD DE DATOS DE LA RED INALÁMBRICA DEL IESTP SAN PEDRO"

DIMENSION N° 01	Confidencialidad
INDICADOR N° 01	Porcentaje de accesos a servicios no autorizados

FICHA DE OBSERVACIÓN

INTRUCCIONES:

- La presente ficha se utiliza para medir el porcentaje de accesos a servicios no autorizados, se mide el % de vulnerabilidad.

Fecha de inicio de la observación:

Item	Identificación del equipo (usuario)	Fecha de verificación	% de vuln.	observaciones

Fecha de fin de la observación:

Observaciones:

_____

_____

_____

Observador

Anexo 5: Instrumento de investigación del indicador Nº 2

INSTRUMENTO DE MEDICION N° 02

"PORTAL CAUTIVO PARA ADMINISTRAR LA SEGURIDAD DE DATOS DE LA RED INALÁMBRICA DEL IESTP SAN PEDRO"

DIMENSION N° 02	Disponibilidad
INDICADOR N° 02	Tiempo promedio de respuesta de navegación WLAN y WAN

FICHA DE OBSERVACIÓN

INTRUCCIONES:

- La presente ficha se utiliza para medir el tiempo que se tarda en acceder a las páginas web y la intranet. En la casilla tiempo utilizado, se ingresará el tiempo transcurrido en milisegundos y luego se obtendrá un promedio.

Fecha de inicio de la observación:

Item	Nombre de la Web ó intranet	Identificación del equipo	Fecha de verificación	Tiempo utilizado (ms)	observaciones

Fecha de fin de la observación:

Observaciones:

_____

_____

_____

Observador

Anexo 6: Instrumento de investigación del indicador Nº 3

INSTRUMENTO DE MEDICION N° 03

"PORTAL CAUTIVO PARA ADMINISTRAR LA SEGURIDAD DE DATOS DE LA RED INALÁMBRICA DEL IESTP SAN PEDRO"

DIMENSION N° 03	Integridad
INDICADOR N° 03	Porcentaje de pérdida de paquetes de transmisión de datos

FICHA DE OBSERVACIÓN

INTRUCCIONES:

- La presente ficha se utiliza para medir el porcentaje de pérdida de paquetes de transmisión de datos, se mide el % de perdida de paquetes.

Fecha de inicio de la observación:

Item	N° Paq. Enviados	Identificación del equipo (usuario)	Fecha de verificación	N° Paq. Perdidos	% Paq. Perdidos

Fecha de fin de la observación:

Observaciones:

Observador

Anexo 7: Confiabilidad y validez del instrumento por el experto 1

UPLA

FICHA DE VALIDACIÓN POR CRITERIO DE EXPERTO

Tesista	Bach. Christian Ayala Bendezú
Título de tesis	PORTAL CAUTIVO PARA ADMINISTRAR LA SEGURIDAD DE DATOS DE LA RED INALÁMBRICA DEL IESTP SAN PEDRO
Objetivo general de la Tesis	Determinar en qué influye el Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO.
Variables	**Variable Independiente:** Portal Cautivo **Variable Dependiente:** Seguridad de datos
Instrucciones	Estimada(o) especialista se le pide su colaboración para que luego de analizar y cotejar el presente instrumento de investigación, en base a su criterio y experiencia profesional, valide dicho instrumento para su aplicación en el trabajo e investigación descrito
Nota	Para cada criterio considere la Escala de Likert del 1 al 5 1= Nunca | 2=Casi Nunca | 3=A veces | 4= Casi Siempre | 5= Siempre
Lugar y Fecha	Huancayo, 07 de noviembre del 2022

ASPECTOS DE VALIDACIÓN

Items	Indicadores	1	2	3	4	5	Observaciones / Sugerencias
01	¿El instrumento de medición cumple con el diseño adecuado?				X		
02	¿El instrumento de recolección de datos tiene relación con la medición?					X	
03	¿El instrumento re recolección de datos facilitará el logro del objetivo de la investigación?				X		
04	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de los datos?					X	
05	¿El instrumento de medición será accesible a la población sujeto de estudio?				X		
06	¿El instrumento de medición es claro, conciso y sencillo para su registro y asi obtener el dato requerido?					X	
07	¿El instrumento de recolección de datos se relaciona con las variables de estudio?					X	
08	¿El instrumento de recolección de datos facilitará la información de la investigación?					X	
Puntaje Total					3	5	

De 0 a 10: No Válido, Reformular	
De 11 a 20: No Válido, Reformular	
De 21 a 30: Válido, Mejorar	
De 21 a 30: Válido, Aplicar	X

Apellidos y Nombres	Huayta Meza, Freddy Toribio
Grado Académico	Doctor en Ing. de Sistemas.
Firma	Freddy Toribio Huayta Meza Dr. Ingeniería de Sistemas CIP N° 91638

Anexo 8: Confiabilidad y validez del instrumento por el experto 2

UPLA

FICHA DE VALIDACIÓN POR CRITERIO DE EXPERTO

Tesista	Bach. Christian Ayala Bendezú
Título de tesis	PORTAL CAUTIVO PARA ADMINISTRAR LA SEGURIDAD DE DATOS DE LA RED INALÁMBRICA DEL IESTP SAN PEDRO
Objetivo general de la Tesis	Determinar en qué influye el Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO.
Variables	**Variable Independiente:** Portal Cautivo **Variable Dependiente:** Seguridad de datos
Instrucciones	Estimada(o) especialista se le pide su colaboración para que luego de analizar y cotejar el presente instrumento de investigación, en base a su criterio y experiencia profesional, valide dicho instrumento para su aplicación en el trabajo e investigación descrito
Nota	Para cada criterio considere la Escala de Likert del 1 al 5 1= Nunca | 2=Casi Nunca | 3=A veces | 4= Casi Siempre | 5= Siempre
Lugar y Fecha	Huancayo, 07 de noviembre del 2022

ASPECTOS DE VALIDACIÓN

Items	Indicadores	1	2	3	4	5	Observaciones / Sugerencias
01	¿El instrumento de medición cumple con el diseño adecuado?					X	
02	¿El instrumento de recolección de datos tiene relación con la medición?				X		
03	¿El instrumento re recolección de datos facilitará el logro del objetivo de la investigación?					X	
04	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de los datos?				X		
05	¿El instrumento de medición será accesible a la población sujeto de estudio?				X		
06	¿El instrumento de medición es claro, conciso y sencillo para su registro y asi obtener el dato requerido?					X	
07	¿El instrumento de recolección de datos se relaciona con las variables de estudio?					X	
08	¿El instrumento de recolección de datos facilitará la información de la investigación?					X	
Puntaje Total					3	5	

De 0 a 10: No Válido, Reformular	
De 11 a 20: No Válido, Reformular	
De 21 a 30: Válido, Mejorar	
De 21 a 30: Válido, Aplicar	X

Apellidos y Nombres	Yapias Rojas Alfredo
Grado Académico	Maestro
Firma	COLEGIO DE INGENIEROS DEL PERU CONSEJO DEPARTAMENTAL DE JUNIN Ing. Alfredo H. Yapias Rojas SISTEMAS Y COMPUTACION CIP 111374

Anexo 9: Confiabilidad y validez del instrumento por el experto 3

UPLA

FICHA DE VALIDACIÓN POR CRITERIO DE EXPERTO

Tesista	Bach. Christian Ayala Bendezú
Título de tesis	PORTAL CAUTIVO PARA ADMINISTRAR LA SEGURIDAD DE DATOS DE LA RED INALÁMBRICA DEL IESTP SAN PEDRO
Objetivo general de la Tesis	Determinar en qué influye el Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO.
Variables	**Variable Independiente:** Portal Cautivo **Variable Dependiente:** Seguridad de datos
Instrucciones	Estimada(o) especialista se le pide su colaboración para que luego de analizar y cotejar el presente instrumento de investigación, en base a su criterio y experiencia profesional, valide dicho instrumento para su aplicación en el trabajo e investigación descrito
Nota	Para cada criterio considere la Escala de Likert del 1 al 5 1= Nunca | 2=Casi Nunca | 3=A veces | 4= Casi Siempre | 5= Siempre
Lugar y Fecha	Huancayo, 07 de noviembre del 2022

ASPECTOS DE VALIDACIÓN

Items	Indicadores	1	2	3	4	5	Observaciones / Sugerencias
01	¿El instrumento de medición cumple con el diseño adecuado?					X	
02	¿El instrumento de recolección de datos tiene relación con la medición?				X		
03	¿El instrumento re recolección de datos facilitará el logro del objetivo de la investigación?					X	
04	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de los datos?				X		
05	¿El instrumento de medición será accesible a la población sujeto de estudio?					X	
06	¿El instrumento de medición es claro, conciso y sencillo para su registro y asi obtener el dato requerido?					X	
07	¿El instrumento de recolección de datos se relaciona con las variables de estudio?				X		
08	¿El instrumento de recolección de datos facilitará la información de la investigación?					X	
Puntaje Total					3	5	

De 0 a 10: No Válido, Reformular	
De 11 a 20: No Válido, Reformular	
De 21 a 30: Válido, Mejorar	
De 21 a 30: Válido, Aplicar	X

Apellidos y Nombres	Maldonado Chumbe Herly Heaz
Grado Académico	Maestro
Firma	Mg. Herly H. Maldonado Chumbe DNI 41500949

Anexo 10: La data del procesamiento de datos

PORTAL CAUTIVO PARA ADMINISTRAR LA SEGURIDAD DE DATOS DE LA RED INALÁMBRICA DEL IESTP SAN PEDRO						
VARIABLE DEPENDIENTE	Seguridad de datos					
HIPOTESIS GENERAL:	El Portal Cautivo influye para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO					
HIPOTESIS ESPECIFICAS:	El Portal Cautivo influye para administrar la confidencialidad de datos en la Red Inalámbrica del IESTP SAN PEDRO		El Portal Cautivo influye para administrar la disponibilidad de datos en la Red Inalámbrica del IESTP SAN PEDRO		El Portal Cautivo influye para administrar la integridad de datos en la Red Inalámbrica del IESTP SAN PEDRO	
DIMENSION:	Confidencialidad		Disponibilidad		Integridad	
INDICADOR:	Porcentaje de accesos a servicios no autorizados		Tiempo promedio de respuesta de navegación WLAN y WAN		Porcentaje de pérdida de paquetes de transmisión de datos	
ASPECTOS A OBSERVAR:						
OBJETIVO DEL INSTRUMENTO:	Determinar el porcentaje de accesos a servicios no autorizados		Determinar el tiempo promedio de respuesta de navegación WLAN y WAN		Determinar el Porcentaje de pérdida de paquetes de transmisión de datos	
OBSERVADOR:	Bach. Christian Ayala Bendezú					
ACCION DEL OBSERVADOR:	Uso del programa Nessus, para medir el porcentaje de accesos a servicios no autorizados		Uso del Packet Loss Test, para medir el tiempo promedio de respuesta de navegación WLAN y WAN		Uso del Packet Loss Test, para medir el porcentaje de pérdida de paquetes de transmisión de datos	
PERIODO DE OBSERVACIÓN:	**01/09/2022-31/10/2022**	**15/11/2022-31/12/2022**	**01/09/2022-31/10/2022**	**15/11/2022-31/12/2022**	**01/09/2022-31/10/2022**	**15/11/2022-31/12/2022**
ITEM	**PRE**	**POST**	**PRE**	**POST**	**PRE**	**POST**
1	61.20%	3.20%	108	88	3.70%	0.40%
2	75.60%	3.60%	104	66	4.00%	0.50%
3	77.60%	2.40%	95	52	5.00%	0.30%
4	86.40%	2.80%	121	80	4.40%	0.20%
5	64.00%	4.80%	108	80	3.30%	0.60%
6	78.00%	6.00%	130	90	3.40%	0.20%
7	73.20%	6.00%	122	80	3.10%	0.70%
8	47.60%	4.40%	99	52	4.50%	0.50%
9	57.60%	4.00%	128	55	4.00%	0.10%
10	81.60%	4.80%	124	54	4.50%	0.10%
11	72.00%	4.00%	103	61	4.70%	0.70%
12	62.80%	4.40%	91	50	3.60%	0.00%
13	71.60%	2.80%	126	89	3.50%	0.50%
14	55.60%	6.00%	128	88	3.00%	0.80%
15	70.00%	4.40%	100	82	4.00%	0.60%
16	58.00%	3.60%	112	72	3.00%	0.60%
17	83.60%	3.60%	100	56	3.40%	0.40%
18	52.80%	6.00%	101	50	4.90%	0.10%
19	78.80%	5.60%	124	56	3.10%	0.40%
20	84.40%	6.00%	130	58	3.80%	0.50%
21	56.80%	6.00%	97	82	3.30%	0.70%
22	64.00%	3.60%	102	86	3.80%	0.50%
23	78.40%	3.20%	110	79	3.10%	0.90%
24	77.20%	5.60%	120	74	3.30%	0.10%
25	87.20%	4.00%	108	76	4.30%	0.30%
26	88.00%	3.60%	113	58	4.60%	0.60%

27	86.80%	3.20%	103	73	3.70%	0.20%
28	86.40%	4.00%	99	89	4.10%	0.20%
29	93.20%	3.20%	92	49	3.10%	0.30%
30	69.60%	4.00%	114	74	4.90%	0.00%
31	82.40%	6.00%	125	76	4.10%	0.30%
32	65.20%	4.40%	115	55	5.00%	0.90%
33	74.00%	4.80%	93	90	3.00%	0.60%
34	66.00%	2.00%	120	63	3.90%	0.40%
35	82.80%	5.20%	129	87	4.30%	0.40%
36	65.20%	2.00%	130	63	3.70%	0.10%
37	61.20%	5.20%	102	67	4.20%	1.00%
38	77.20%	4.80%	95	56	4.10%	0.70%
39	55.60%	3.20%	94	64	3.40%	0.60%
40	81.20%	3.20%	106	74	4.30%	0.60%
41	64.00%	2.40%	127	83	4.60%	0.50%
42	59.20%	2.80%	96	53	4.90%	0.40%
43	70.40%	2.00%	123	69	4.70%	0.80%
44	75.60%	4.00%	107	72	4.60%	0.10%
45	69.20%	3.60%	101	81	3.80%	0.20%
46	68.80%	5.20%	119	55	4.00%	1.00%
47	75.60%	3.20%	90	78	4.30%	0.20%
48	63.60%	3.60%	103	81	4.80%	0.90%
49	60.00%	3.20%	95	85	3.20%	0.60%
50	70.40%	2.40%	93	66	3.60%	0.10%
51	69.60%	4.00%	112	50	3.90%	0.50%
52	92.40%	2.00%	124	52	3.10%	0.20%
53	71.60%	3.20%	104	71	3.20%	1.00%
54	68.00%	2.00%	102	76	4.60%	0.50%
55	69.60%	4.00%	108	67	3.40%	0.60%
56	89.60%	2.80%	93	84	3.30%	0.60%
57	78.80%	4.00%	128	70	3.60%	0.20%
58	71.20%	3.20%	118	58	3.50%	0.50%
59	63.60%	3.60%	119	61	4.20%	0.10%
60	78.40%	4.40%	107	73	3.70%	0.60%
61	82.80%	2.80%	126	55	4.00%	0.10%
62	78.80%	4.40%	126	79	4.20%	0.30%
63	76.80%	6.00%	109	53	3.20%	0.40%
64	77.20%	4.80%	106	67	3.80%	0.00%
65	76.40%	4.00%	104	83	3.00%	0.90%
66	81.20%	2.00%	121	62	4.40%	0.10%
67	71.20%	2.00%	101	72	3.40%	0.80%
68	64.80%	4.80%	118	50	4.20%	0.50%
69	74.00%	5.20%	122	63	4.40%	0.10%
70	77.60%	4.00%	123	63	4.00%	0.10%
71	65.60%	4.80%	115	90	3.20%	0.60%
72	69.60%	5.20%	128	60	4.50%	0.20%
73	75.60%	4.80%	123	62	4.00%	0.70%
74	64.80%	6.00%	125	77	4.60%	0.70%
75	54.80%	4.00%	118	52	4.50%	0.30%
76	53.20%	4.40%	108	82	4.20%	0.40%
77	55.20%	2.80%	120	56	4.40%	0.20%
78	92.40%	5.60%	112	53	4.60%	0.20%
79	84.80%	2.80%	90	52	3.00%	0.20%
80	69.20%	3.60%	130	74	4.70%	0.40%
81	66.00%	2.40%	109	86	4.20%	0.10%
82	76.80%	4.00%	119	64	4.30%	0.60%
83	80.40%	4.00%	109	72	3.00%	0.80%
84	70.80%	3.60%	100	55	4.00%	0.70%
85	73.20%	6.00%	108	64	4.20%	0.40%
86	64.40%	2.00%	103	70	3.20%	0.90%
87	76.40%	3.60%	126	59	3.50%	0.00%
88	76.40%	5.60%	130	50	3.50%	0.80%
89	75.20%	2.80%	129	86	3.30%	0.50%
90	64.00%	2.80%	121	69	4.40%	0.30%

91	73.20%	4.80%	94	52	4.00%	0.00%
92	62.80%	4.40%	114	88	4.60%	0.50%
93	50.00%	6.00%	94	64	3.20%	0.10%
94	70.40%	4.00%	99	66	3.50%	0.20%
95	76.80%	3.20%	91	89	4.10%	0.50%
96	76.40%	4.80%	125	77	3.80%	0.40%
97	67.60%	5.20%	96	53	3.30%	0.50%
98	54.40%	3.60%	110	86	3.80%	0.60%
99	74.80%	5.60%	119	54	4.00%	1.00%
100	72.80%	4.00%	107	56	3.70%	0.60%
101	82.40%	4.40%	122	54	3.60%	0.90%
102	51.60%	5.60%	110	68	3.70%	0.90%
103	84.40%	5.20%	103	90	3.40%	0.10%
104	78.80%	6.00%	114	83	4.40%	0.10%
105	72.40%	2.00%	126	52	3.50%	0.40%
106	61.60%	4.40%	128	66	4.00%	0.00%
107	55.20%	5.20%	94	51	4.90%	0.90%
108	54.40%	3.60%	101	70	3.40%	1.00%
109	58.40%	3.20%	109	49	3.20%	0.80%
110	52.40%	4.80%	91	90	4.70%	1.00%
111	76.00%	3.20%	130	54	3.90%	0.20%
112	87.20%	4.40%	126	64	4.60%	0.20%
113	78.00%	3.20%	115	66	3.10%	0.00%
114	67.60%	4.40%	91	69	3.90%	0.10%
115	50.80%	4.00%	109	75	3.70%	0.20%
116	75.20%	4.80%	90	84	4.60%	0.60%
117	78.00%	2.00%	125	78	3.70%	0.30%
118	61.60%	3.60%	119	66	3.20%	0.60%
119	63.60%	3.60%	128	84	3.30%	1.00%
120	77.60%	3.20%	97	50	3.50%	0.00%
121	73.60%	4.00%	99	76	4.20%	0.50%
122	64.00%	5.60%	97	65	3.70%	0.00%
123	63.20%	2.00%	111	64	3.10%	0.90%
124	60.40%	5.20%	91	74	3.90%	0.20%
125	70.80%	3.60%	93	62	3.10%	0.40%
126	59.60%	6.00%	130	75	3.60%	0.70%
127	67.20%	3.60%	111	59	3.10%	0.20%
128	72.80%	2.40%	112	59	3.70%	0.70%
129	78.40%	5.60%	111	71	3.70%	0.10%
130	66.00%	4.80%	99	87	4.10%	0.50%
131	74.00%	4.80%	126	64	3.20%	0.30%
132	80.40%	4.00%	102	49	3.20%	0.60%
133	76.40%	6.00%	110	54	4.10%	1.00%
134	68.80%	4.00%	127	61	3.30%	0.80%
135	80.40%	3.20%	127	53	4.40%	1.00%
136	86.40%	3.20%	117	90	3.20%	0.80%
137	71.60%	4.40%	91	70	4.60%	0.10%
138	68.00%	2.80%	119	50	5.00%	0.30%
139	67.20%	4.00%	117	80	3.50%	0.90%
140	64.00%	4.00%	122	68	3.00%	1.00%
141	66.40%	4.00%	116	64	4.20%	0.70%
142	76.80%	4.40%	124	75	3.40%	0.80%
143	71.60%	4.00%	127	61	4.40%	0.20%
144	82.80%	2.80%	128	49	4.20%	1.00%
145	78.80%	4.00%	125	85	4.40%	0.00%
146	61.20%	2.00%	98	72	4.60%	0.30%
147	82.00%	6.00%	96	74	5.00%	0.70%
148	57.20%	2.00%	118	74	4.20%	0.20%
149	72.80%	2.80%	90	90	3.60%	0.70%
150	64.40%	2.80%	120	61	4.00%	0.00%
151	55.60%	3.60%	114	65	4.70%	0.50%
152	78.80%	3.20%	116	86	4.80%	0.70%
153	68.00%	5.60%	95	70	4.30%	0.70%
154	63.20%	2.40%	126	78	4.00%	0.70%

Anexo 11: Consentimiento informado

CONSENTIMIENTO INFORMADO

Yo, Juan Carlos Llanco Ricse, Gerente General del **Instituto de Educación Superior Tecnológico Privado "San Pedro"** de Huancayo, declaro que he sido informado por el Sr. Christian Ayala Bendezú con DNI: 20079145 sobre el estudio de investigación "Portal Cautivo para administrar la seguridad de datos de la Red Inalámbrica del IESTP SAN PEDRO" a realizarse en la institución. Este es un proyecto de investigación científica que cuenta con el respaldo y apoyo del **Instituto de Educación Superior Tecnológico Privado "San Pedro"**

Se expide la presente la los fines que estime pertinente.

Anexo 12: Desarrollo de la Metodología

DESARROLLO DE LA SOLUCIÓN CON LA METODOLOGIA PPDIOO

INFORMACION DE LA INSTITUCION

1. DEFINICION DE LA INSTITUCION

1.1. DENOMINACION OFICIAL

Instituto de Educación Superior Tecnológico Privado San Pedro

1.2. DOCUMENTO LEGAL DE CREACION

Resolución Ministerial Nº 0811-94-ED

1.3. DOCUMENTO DE REVALIDACION

Resolución Directoral Nº 246-2005-ed

1.4. UBICACIÓN GEOGRAFICA

Tabla 5.1 Datos de la Ubicación Geográfica de la Institución

REGIÓN	Junín
PROVINCIA	Huancayo
DISTRITO	El Tambo
DIRECCIÓN	Pje. Los Andes Nº 390
TELÉFONO	975759081
PAGINA WEB	https://www.istsanpedro.edu.pe/
FACEBOOK	https://www.facebook.com/istsanpedro?mibextid=ZbWKwL
GESTIÓN	Privada
LOCAL	Propio

1.5. NIVEL

Profesional Técnico

1.6. CARRERAS PROFESIONALES

Desarrollo de Sistemas

Construcción Civil

Gastronomía y Arte Culinario

Contabilidad

Secretariado Ejecutivo

1.7. VISION

Al 2018 Ser la institución líder de la educación superior tecnológica de alta excelencia con visión futurista, como líder en la formación integral de ciudadanos, profesionales y dirigentes. Con espíritu emprendedor, comprometidos con su propio desarrollo y el de la nación peruana.

1.8. MISION

El Instituto de Educación Superior Tecnológica Privada "San Pedro", tiene como misión ser una comunidad de educación superior que imparte instrucción de alto nivel académico y constantemente actualizado para la realización de proyectos de formación, investigación tecnológica e interacción social que sirva al desarrollo integral, solidario y sostenible de las personas y de la sociedad, dentro de la región y la nación; y que contribuya a la consolidación de la paz social, la justicia y la democracia en la nación Peruana.

1.9. VALORES INSTITUCIONALES

Respeto

Honestidad

Solidaridad

Responsabilidad

1.10. MODALIDAD

Presencial

Semi – Presencial

2. APLICACIÓN DE LA METODOLOGIA

Según la revisión realizada, se determina utilizar la metodología PPDIOO (Preparar, Planificar, Diseñar e Implementar), para la presente investigación se tomará en cuenta las cuatro primeras fases, se utilizó dicha metodología para instalar PfSense con sus diferentes funcionalidades para administrar la seguridad de la red inalámbrica.

2.1. Fase 1. Preparar

Para desarrollar esta fase se ha utilizado la técnica de observación a la infraestructura de la institución.

Del resultado obtenido se ha determinado lo siguiente:

2.1.1. Seguridad de datos: la institución actualmente no cuenta con políticas de seguridad de datos, de tal manera esto afecta a la privacidad de los usuarios al momento de conectarse a la red inalámbrica de la institución.

2.1.2. Objetivos y limitaciones de la institución: la institución espera estar a la vanguardia en las tecnologías de información, para tal fin se requiere que se administre la seguridad de datos de forma óptima en la comunicación inalámbrica de la institución.

Cabe mencionar que una de las limitaciones que tiene la institución para brindar una adecuada administración de seguridad de datos, es que precisamente no cuenta con ningún tipo de gestor para brindar una administración de seguridad de datos.

Otra de las limitaciones encontradas es el factor económico, por tal motivo se plantea un presupuesto a coste cero, ya que para implementar un portal cautivo se utilizará software gratis, además el tesista asumirá cualquier gasto que ocasione esta investigación.

2.1.3. Direccionamiento IP

La cantidad de dispositivos que se conectan a la red inalámbrica es un total de 256 usuarios, asignándoles una IP dinámica en la red 192.168.1.0; por lo tanto, si se llegaran a conectar todos los usuarios a la vez, faltaría un total de dos direcciones de host.

2.1.4. Topología actual de la red inalámbrica

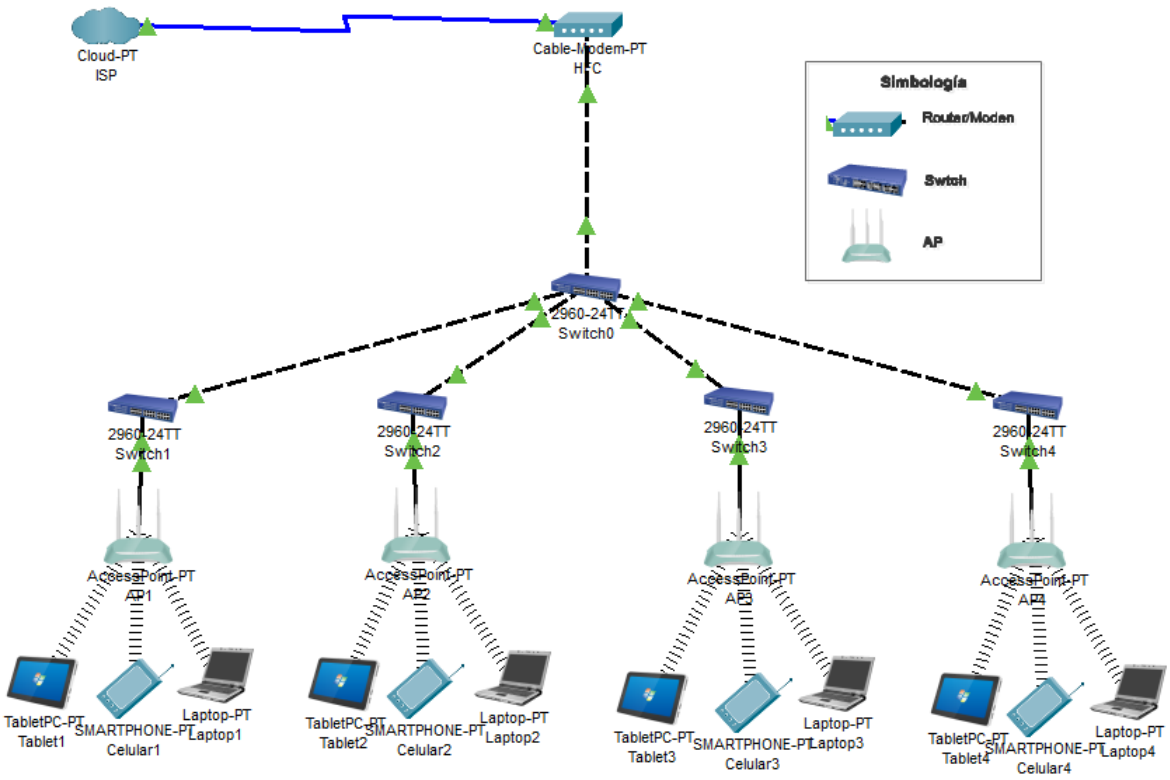


Figura 5.1 Topología actual de la red inalámbrica de la institución

2.1.5. Dispositivos y conexión a internet

DISPOSITIVOS

Tabla 5.2 Características del ordenador

Cantidad	Dispositivo	Características
1	Router/Modem	Askey TCG220-46
4	Swicth	TP-LINK TL – SG1024 • 24 puertos RJ45 a 10/100 Mbps • IEEE 802.3ab, IEEE 802.3u, IEEE 802.3x • 100 - 240V, 50/60Hz
10	Access Point	TL-WA801ND • Un puerto Ethernet 10/100 Mbps (RJ45) Soporte para PoE pasivo

		• 9VDC / 0.85ª • Potencia de Transmisión: 20dBm • Estándares Inalámbricos: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b

CONEXIÓN A INTERNET

La conexión a internet es mediante la tecnología HFC (Hybrid Fiber-Coaxial), fibra coaxial híbrida. Sólo permite que la fibra llegue a un nodo, y desde allí, mediante un cable coaxial, llega la conexión a la casa.

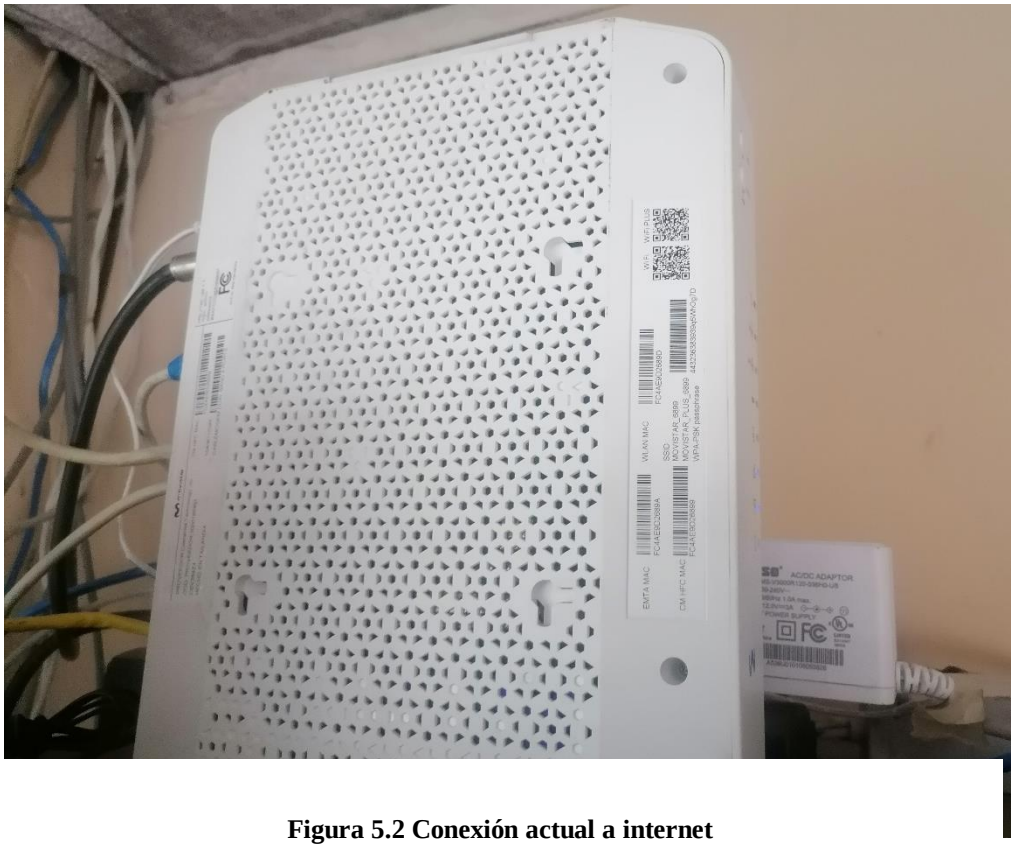


Figura 5.2 Conexión actual a internet

En la figura Nº 5.2, muestra la conexión actual a internet, que se da mediante la tecnología HFC, el proveedor es la compañía Movistar, con una velocidad contratada de 300 Mbps

2.2. Fase 2. Planear

La institución cuenta con personal administrativo, profesores y alumnos, que se conectan a la red inalámbrica de manera diaria, al no tener una administración de seguridad de datos, los usuarios se conectan tanto a sus cuentas institucionales como a sus cuentas personales, tampoco cuentan con algún tipo de control de identidad, afectando a la confidencialidad (% de vulnerabilidad); por otro lado los usuarios no tienen control en la navegación en páginas web, utilizando de forma inadecuada la navegación, dedican mucho tiempo en las páginas de redes sociales, juegos en línea, visualización de videos en línea, todo lo mencionado afecta a la disponibilidad de los datos, por tanto el promedio de respuesta se eleva considerablemente en milisegundos (ms); también no se está optimizando el tráfico de red, a mayor latencia existe perdida de paquetes, por lo tanto afectara a la integridad de los datos (% de perdida de paquetes).

2.2.1. Análisis y requerimientos de servicio de comunicación

Después de haber recopilado la información en la fase de preparación, se requieren cambios para rediseñar la red y mejorar la seguridad de la información. Esto se logra a través de los requerimientos funcionales y no funcionales, que se muestran a continuación.

Para los requerimientos de red, se obtuvo la información mediante fichas de observación con el fin de obtener una información real respecto al servicio de la red inalámbrica teniendo en cuenta la confidencialidad, disponibilidad e integridad de datos.

Requerimientos funcionales:

.

Tabla 5.3 Requerimientos Funcionales

ID	Requerimientos	Descripción
RF1	Identificación y autenticación de usuarios	La identificación y autenticación de usuarios es una parte fundamental de la seguridad de una red inalámbrica. Esto implica verificar la identidad de los usuarios antes de permitirles acceder a la

		red. Esto se hace mediante credenciales como nombres de usuario y contraseñas.
RF2	Segregación de redes mediante segmentación	La segregación de redes mediante segmentación es una técnica para aislar la red interna en subredes lógicas. Esto ofrece diversas ventajas, como la mejora del rendimiento, la seguridad y la simplicidad de administración. Esto se logra colocando los dispositivos dentro de diferentes segmentos de red, reduciendo de esta forma la cantidad de tráfico que pasa por ellos. Esto también facilita el monitoreo de la red y la detección de intrusiones
RF3	Detección de intrusiones	La detección de intrusiones es una técnica usada para identificar actividades sospechosas en la red. Esto se logra mediante el monitoreo de patrones de tráfico, los protocolos de comunicación, los registros de inicio de sesión y los archivos de configuración. Si la herramienta de detección detecta una actividad sospechosa, se puede tomar acción inmediata para detener la amenaza antes de que dañe la red.
RF4	Servidor DHCP	Un servidor DHCP es un servidor que administra y distribuye direcciones IP a los dispositivos de la red. Esto es crucial para permitir la comunicación entre dispositivos de la misma red, ya que permite a los dispositivos conocer la ubicación de otros dispositivos en la misma red. Esto también simplifica la configuración de los dispositivos, ya que no se requiere configurar manualmente las direcciones IP.

		El servidor DHCP puede ayudar al sistema a detectar y prevenir intrusiones.

Requerimientos no funcionales:

Tabla 5.4 Requerimientos No Funcionales

ID	Requerimientos	Descripción
RNF1	Disponibilidad para los usuarios	También es importante garantizar el acceso a la información en tiempo real para que los usuarios puedan obtenerla cuando lo necesiten.
RNF2	Tiempo de respuesta	Para mejorar el rendimiento de la comunicación, debemos acelerar el tiempo de carga de los sistemas informáticos y navegación web para que éstos funcionen de manera óptima.
RNF3	Integridad en la información	Garantizar la integridad de la información, manteniéndola correcta y sin cambios o manipulaciones realizadas por personas ajenas durante su transmisión.
RNF4	Priorización de tráfico	Priorizar el tráfico y garantizar un ancho de banda mínimo, priorizando paquetes en función de las colas de prioridad.
RNF5	Seguridad en la información	Proteger el acceso a las redes de datos para salvaguardar la información que es el activo más valioso de la institución.
RNF6	Conexiones estables	Para mejorar la comunicación de red, necesitamos asegurar que los paquetes de información se envíen y reciban sin retrasos ni pérdidas.

Requerimientos de infraestructura:

La infraestructura de una red debe ser escalable, permitiendo la adición de nuevos componentes de forma continua, que trabajen a la misma velocidad y con un hardware redundante, rápido y según los estándares internacionales; todo esto para estar disponible y completamente activo cuando lo necesitemos. Se muestra en la tabla 5.4

Tabla 5.5 Requerimientos de infraestructura

ID	Requerimientos	Descripción
RF1	Flexibilidad	Permitir el crecimiento en forma modular y adaptarse a la nueva dinámica tecnológica, brindando la posibilidad de implementar nuevas aplicaciones cuando las organizaciones lo necesiten.
RF2	Administrable	Unificar los servicios en la red, controlar el uso de recursos de cada equipo, bloquear o restringir el uso de equipos problemáticos, optimizar el tráfico y mejorar la seguridad.
RF3	Confiable	Soportar aplicaciones robustas, funcionar a través de diferentes tipos de conexión y dispositivos para formar la infraestructura física.

Tabla 5.6 Lista de equipos y accesorios para la implementación

Nombre	Características
Servidor PFSense	AMD Athlon 64 X2 3800+, 2009.91 MHz
Router/Modem	Askey TCG220-46
Swicth	TP-LINK TL – SG1024 • 24 puertos RJ45 a 10/100 Mbps • IEEE 802.3ab, IEEE 802.3u, IEEE 802.3x

	100 - 240V, 50/60Hz
Access Point	TL-WA801ND • Un puerto Ethernet 10/100 Mbps (RJ45) Soporte para PoE pasivo • 9VDC / 0.85ª • Potencia de Transmisión: 20dBm Estándares Inalámbricos: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b

2.2.2. Recurso humano designado para la implementación

Para el desarrollo de cada una de las fases de la metodología se hace cargo el Bach. Christian Ayala Bendezú.

2.2.3. Presupuesto del proyecto

Tabla 5.7 Presupuesto

DESCRIPCION	CANTIDAD	VALOR U.	TOTAL	FINANCIADOR
Movilización		S/. 100	S/. 100	Recursos propios
Acceso a Internet	5	S/. 90	S/. 450	Recursos propios
Papel A4	600	S/. 0.05	S/. 30	Recursos propios
Copias		S/. 100	S/. 100	Recursos propios
Impresión de documentos		S/. 250	S/. 250	Recursos propios
Anillados		S/. 20	S/. 20	Recursos propios
Empastados		S/. 60	S/. 60	Recursos propios
USB		S/. 30	S/. 30	Recursos propios
Imprevistos		S/. 100	S/. 100	Recursos propios
TOTAL			**S/. 1110**	

2.2.4. Cronograma de actividades

Tabla 5.8 Cronograma de actividades

ÍTEM	ACTIVIDADES	2022				
		AGO	SEP	OCT	NOV	DIC
1	Fase de Preparación	X	X			
2	Fase de Planificación			X		
3	Fase de Diseño				X	
4	Fase de Implementación					X

2.3. Fase 3. Diseñar

2.3.1. Planeamiento IP

Para mejorar el ordenamiento y seguridad en la red se tomó el siguiente direccionamiento IP de Sub-Red.

Tabla 5.9 Direccionamiento IP

Total, Host	Red	Mascara	1ra IP utilizable	Ultima IP utilizable
510	172.16.0.0	255.255.254	172.16.0.1	172.16.1.254

2.3.2. Rediseño de la red inalámbrica

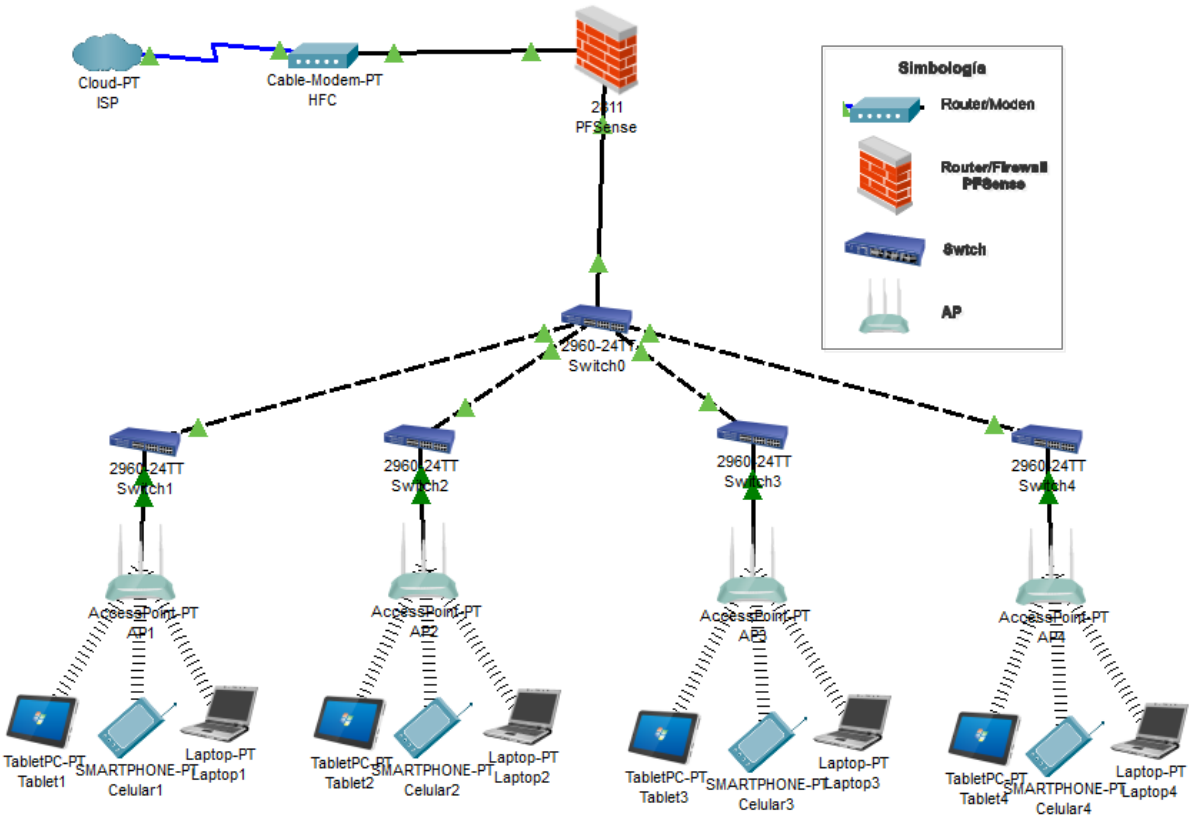


Figura 5.3 Rediseño de la implementación del pfsense

Los AP (Access point) será ubicado en puntos estratégicos de difusión al momento de realizar la implementación en el primer piso se ubican 5 APs, en el segundo piso 3 APs y en el tercer piso 2 APs, para la distribución de las APs se tiene en cuenta las estructuras, pero con dicha distribución abastecen toda la

cobertura, estos equipos tienen un rango de 100 metros y su potencia de transmisión es de 20dBm; dicha distribución se muestra en la figura Nº 5.4 y Nº 5.5.

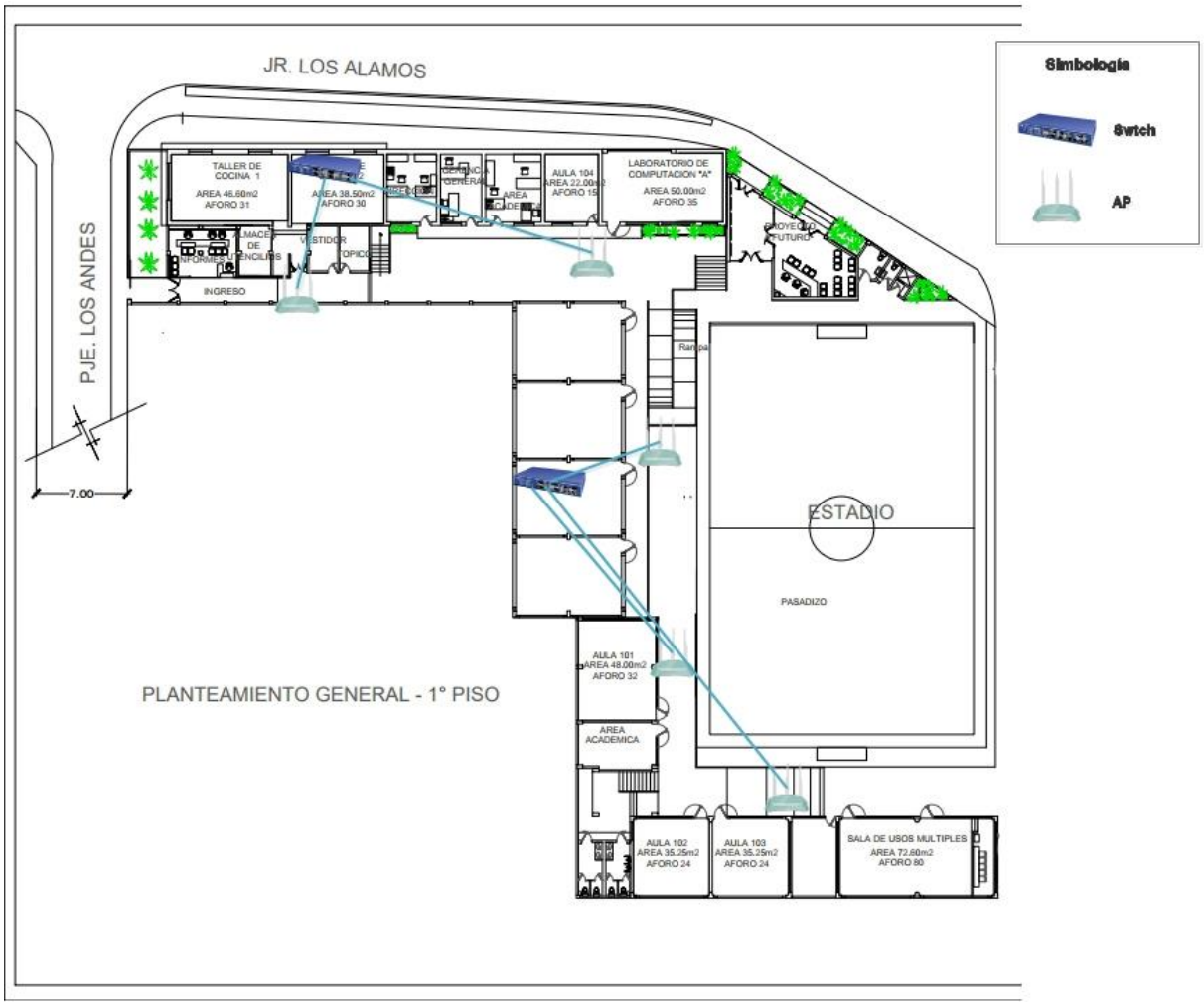


Figura 5.4 Conexiones de APS en el primer piso

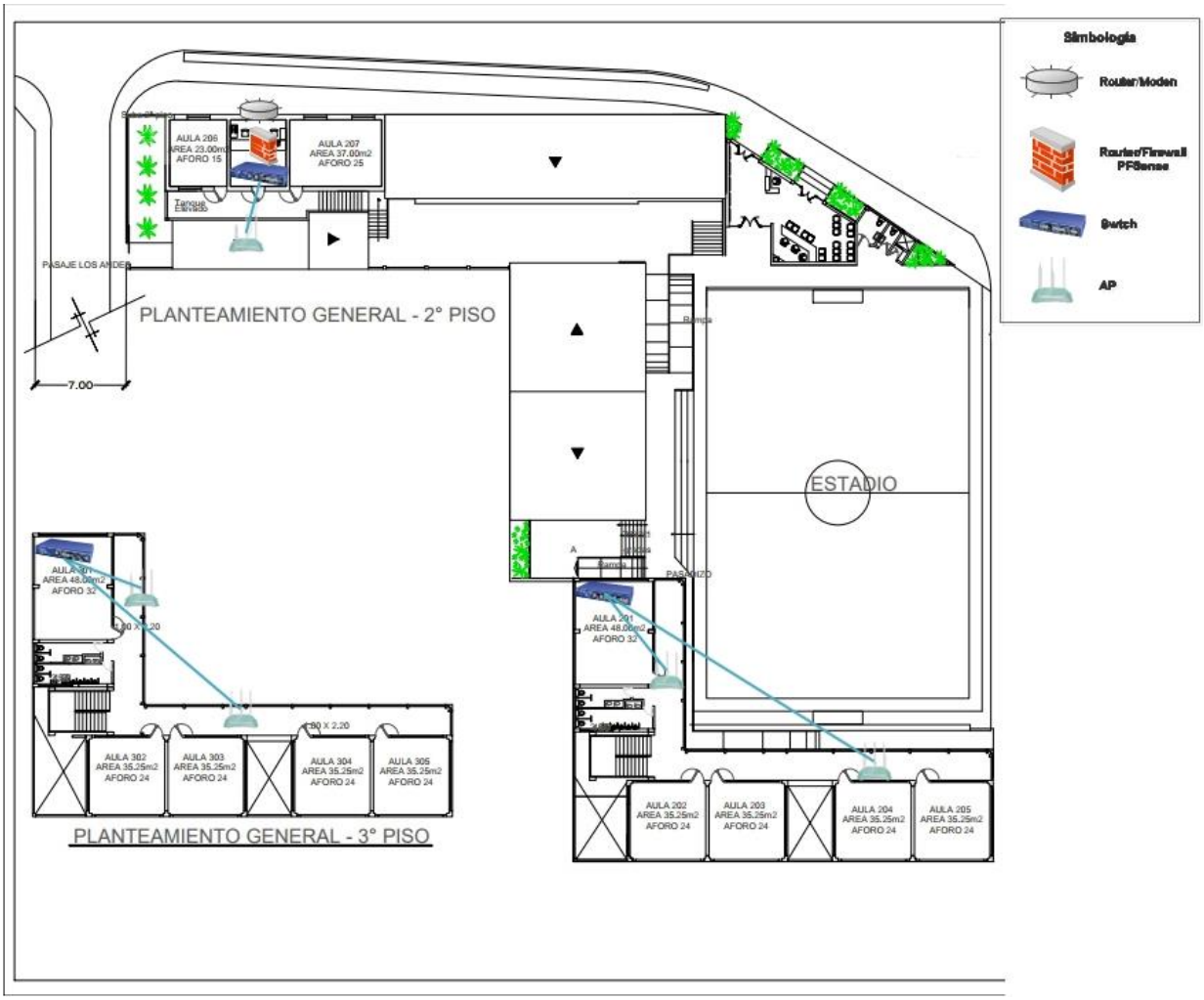


Figura 5.5 Figura Nº 5. Conexiones de APS en el segundo y tercer piso

2.4. Fase 4. Implementar

Para implementar el software PFSense se ha utilizado un equipo de PC que se encontraba en el almacén de la institución, con la finalidad de no ocasionar gastos adicionales. Tomando en cuenta las características que nos recomienda la comunidad NetGate, se muestra en la tabla Nº 5.9

Tabla 5.10 Requerimientos PFSense

EQUIPO	CARACTERISTICAS	CANTIDAD
Procesador	AMD Athlon 64 X2 3800+, 2009.91 MHz	1
Placa Base	ASUSTeK Computer INC. M2N4-SLI	1
Memoria RAM	4 Gb	2
Disco Duro	160 GB	1
Tarjeta de Video	NVIDIA GeForce 8400GS	1
Monitor	18.5” LG LED 1366X768	1
Teclado/Mouse	KIT GENIUS MULTIMEDIA USB	1
Tarjeta de Red	Integrado NVIDIA nForce D-Link DFE-520TX PCI	2

Paso siguiente es crear una WLAN cuyo nombre se le asigna WIFI_SP, dicha configuración se realiza en el moden/router de la compañía Movistar, como se muestra la figura Nº 5.6

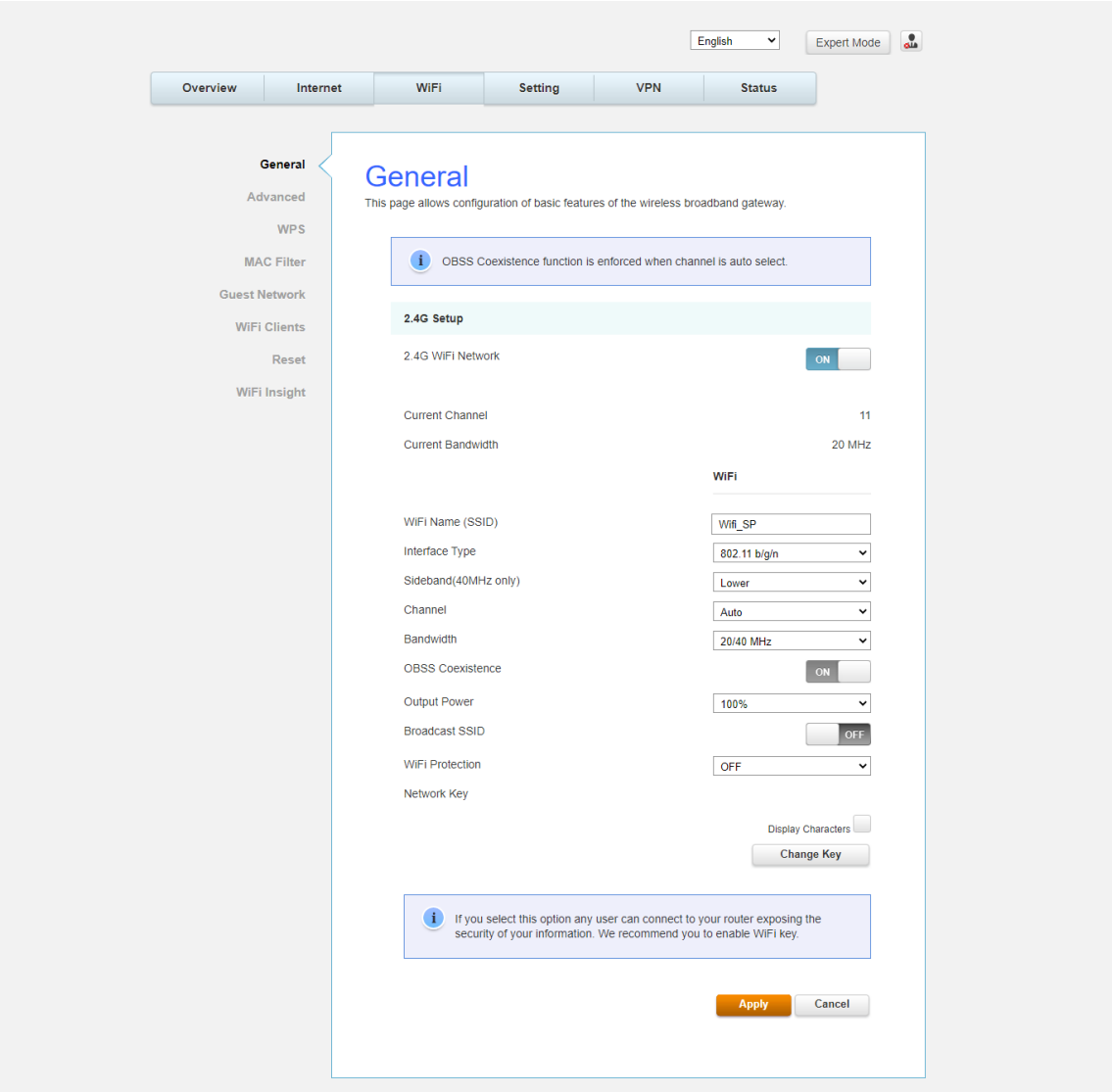


Figura 5.6 Configuración de la WLAN: WIFI_SP

Luego se verifica la WLAN creada anteriormente, como muestra la figura Nº 5.7

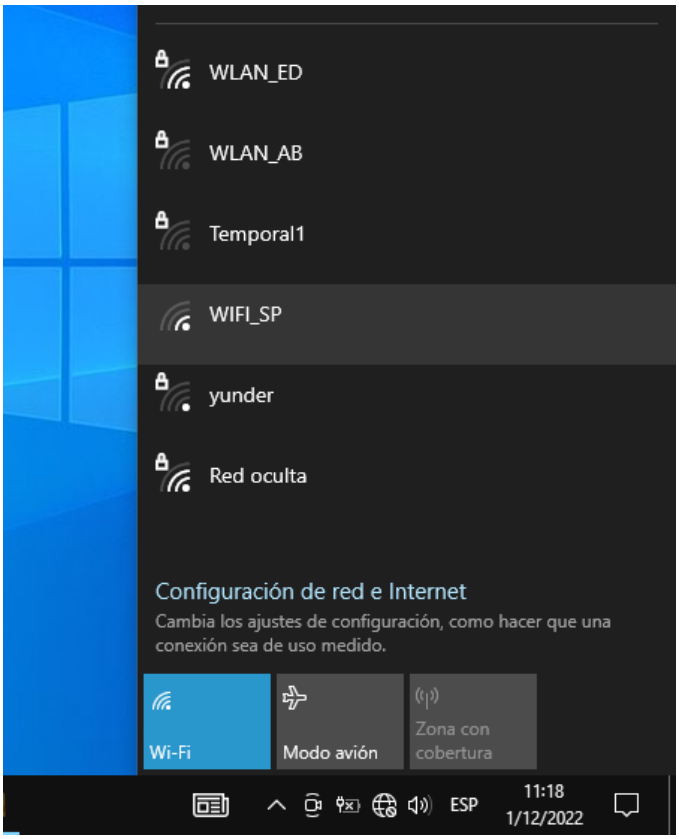


Figura 5.7 Verificación WLAN creada

Continuando con el paso el paso anterior, pasamos a la instalación del software Pfsense, para luego configurar el portal cautivo que se mostrara en la red inalámbrica de la institución.

Implementación del Pfsense

Lo primero que se realiza es descargar la imagen ISO desde la página oficial de Pfsense: https://www.pfsense.org/download/, como muestra la figura Nº 5, luego se configura el equipo en el arranque para que inicie desde la unidad creada con la imagen ISO.

Cuando inicia el equipo por medio de la USB de instalación se muestra como la figura Nº 5.8

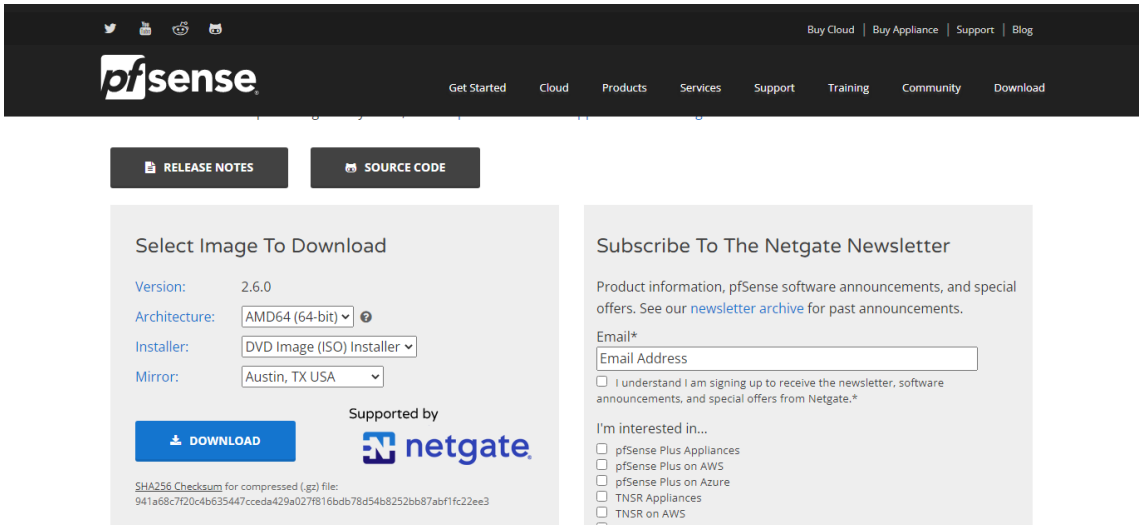


Figura 5.8 Página oficial Pfsense

Fuente: (PFSENSE 2022)

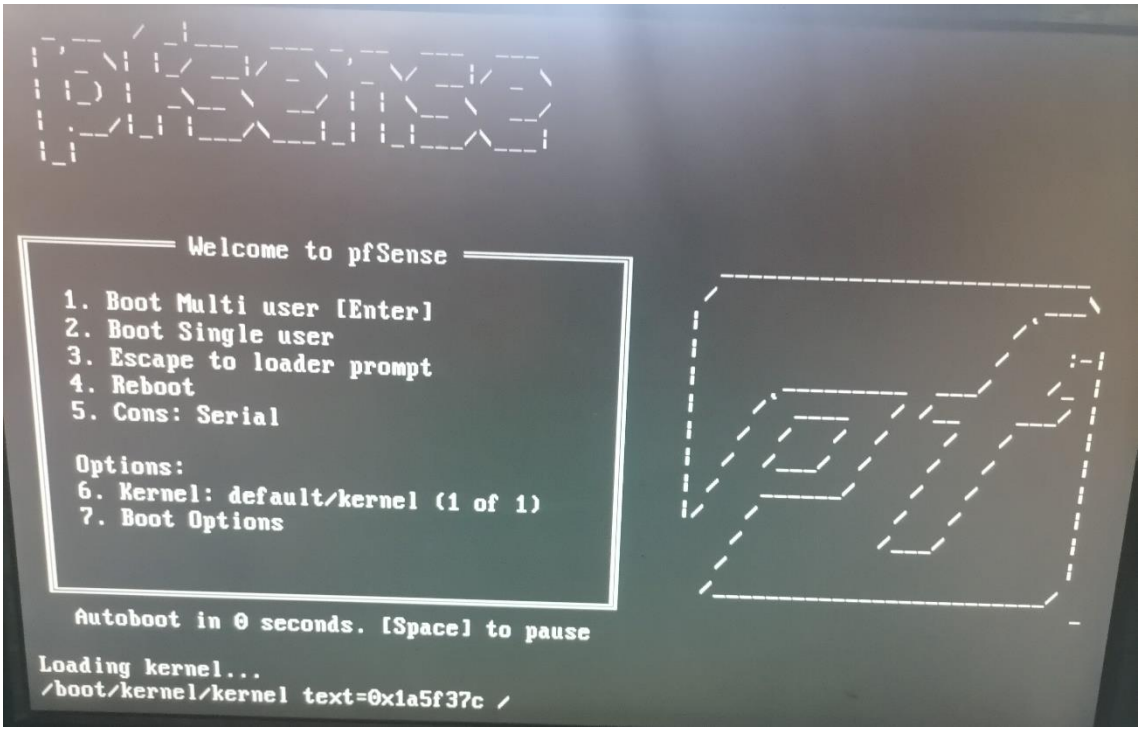


Figura 5.9 Arranque de instalación de Pfsense

Para iniciar la instalación se elige la opción 1.

Una vez culminado la instalación, se visualiza lo que muestra la figura Nº 9, confirmándonos su correcta instalación.

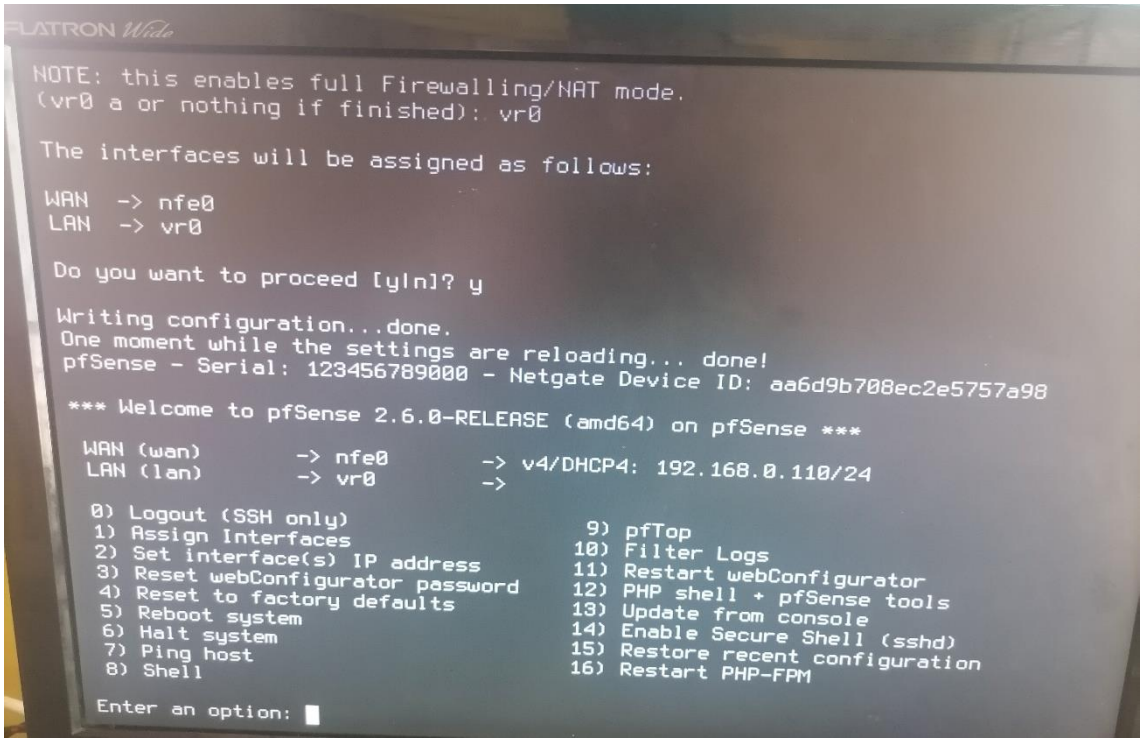


Figura 5.10 Menú de configuración Pfsense

Luego cambiamos la IP de la LAN para evitar conflictos con nuestra red, para ello elegimos la opción 2, asignamos la nueva dirección IP: 172.16.0.1 con mascara de red: 255.255.254.0 /23, como muestra la figura Nº 5.10

Para poder ingresar a Pfsense a la configuración web, colocamos una IP estatica en las propiedades de red de nuestra PC como muestra la figura Nº 5.11, desde la cual vamos a configurar el portal cautivo, mediante esta dirección IP accedemos a nuestro navegador web para realizar la configuración correspondiente como se muestra en la figura Nº 5.11, en este caso colocamos la IP: 172.16.0.1

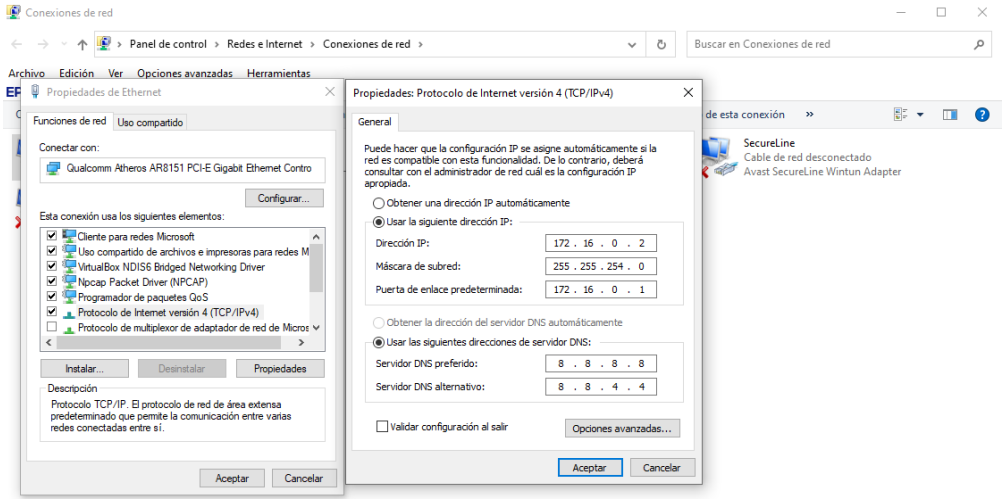


Figura 5.11 introducción IP estática

Ingresamos a la IP de nuestro Pfsense que es el 172.16.0.1, nos pide que ingresemos nuestras credenciales: User: admin, password: pfsense (por defecto), como se muestra en la figura Nº 5.12

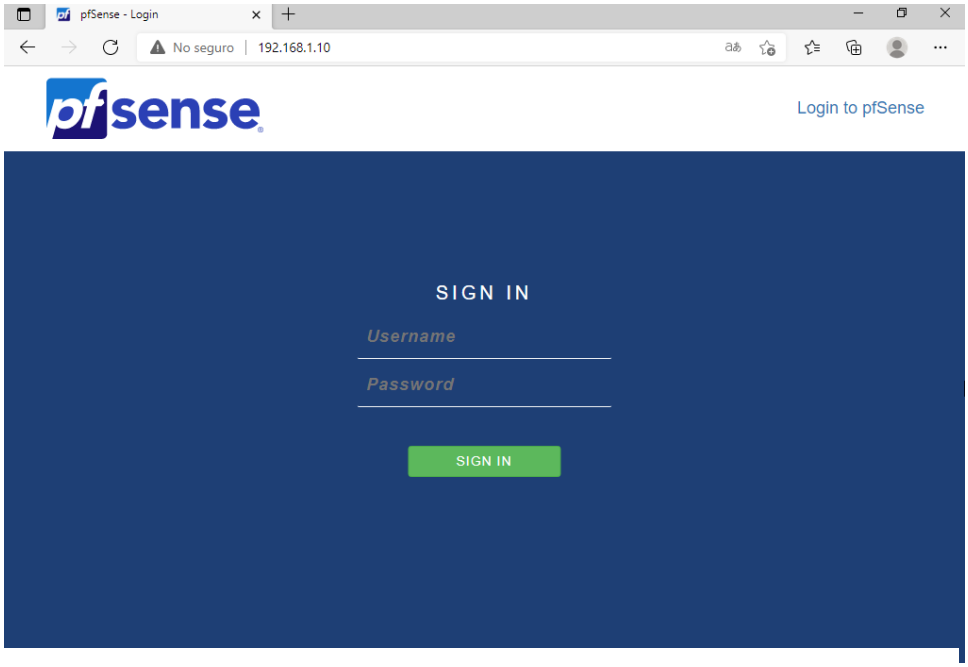


Figura 5.12 Página de ingreso Pfsense

Ingresando las credenciales nos muestra la página de inicio del pfsense, con el asistente de configuración, como se muestra en la figura Nº 5.13

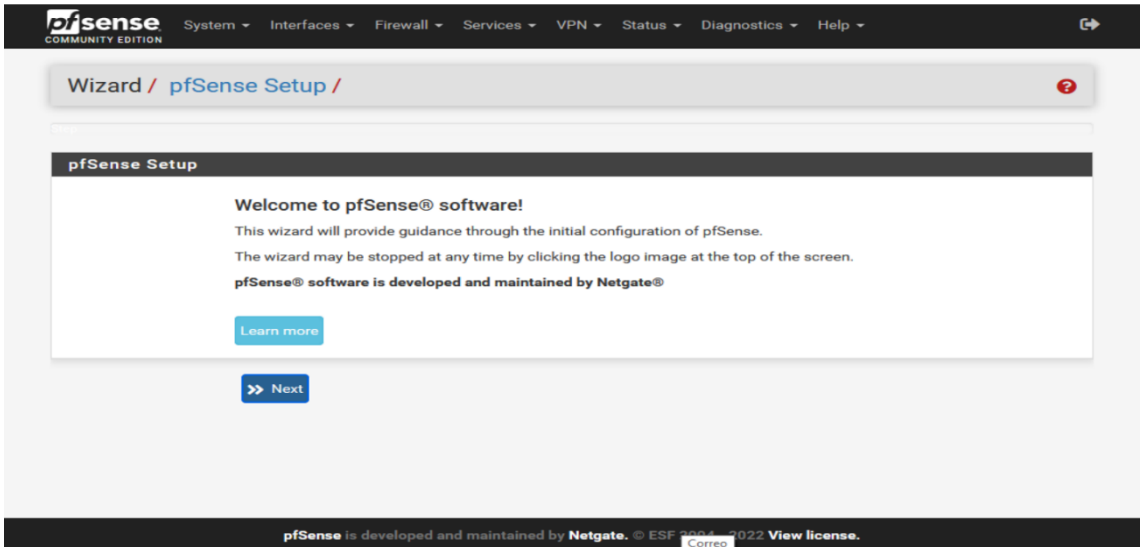


Figura 5.13 Asistente de configuración

En la figura Nº 5.14, Cambiamos nombre de hostname por SPpfSense y los dns ingresamos lo siguiente: 8.8.8.8 y 8.8.4.4, en el paso siguiente ingresamos la zona horaria, para luego cambiar la contraseña a una mucho más segura

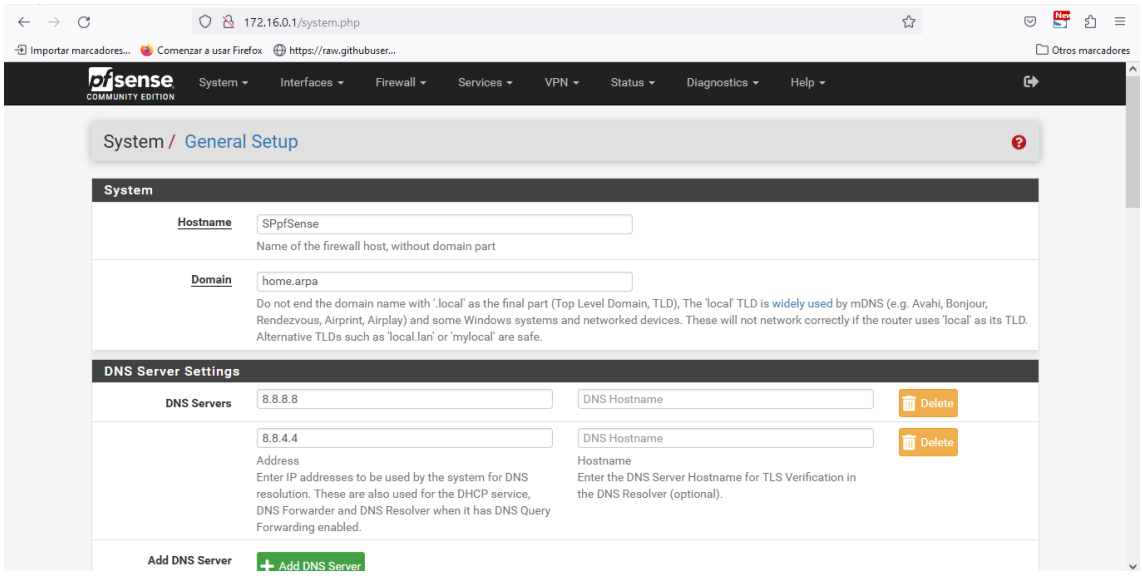


Figura 5.14 Nombre de Hostname y DNS

Luego nos muestra el Dashboard del pfsense, tal como se muestra en la figura Nº 5.15

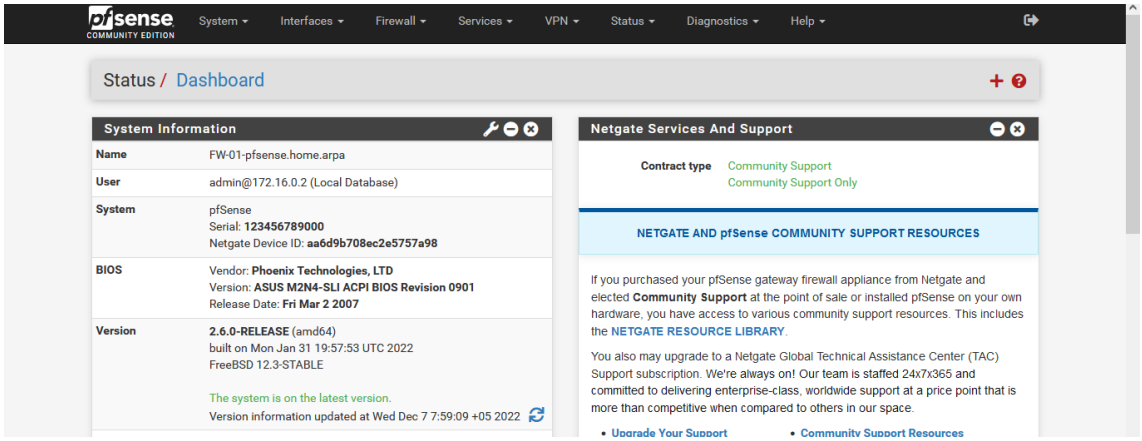


Figura 5.15 Dashboard del pfsense

Se ingresa una IP estática a la WAN con el objeto de evitar algún inconveniente más adelante, figura Nº 5.16

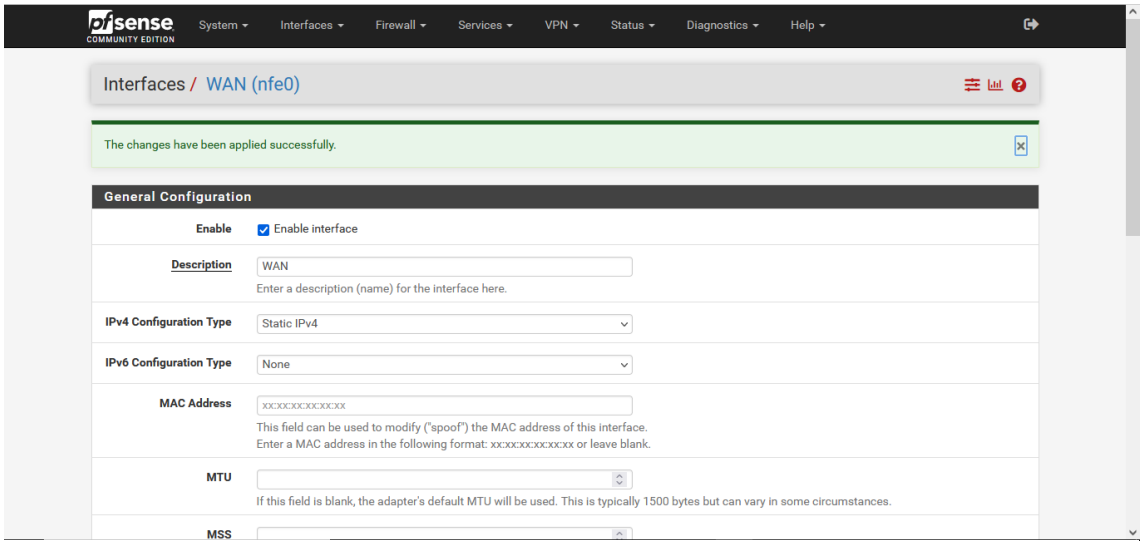


Figura 5.16 Interfaz WAN pfsense

Ahora nos toca activar el DHCP en la interfaz WLAN, para ello es necesario establecer la IP estática en dicha interfaz, también se asigna el rango de IPs, como se muestra en la figura Nº 5.17

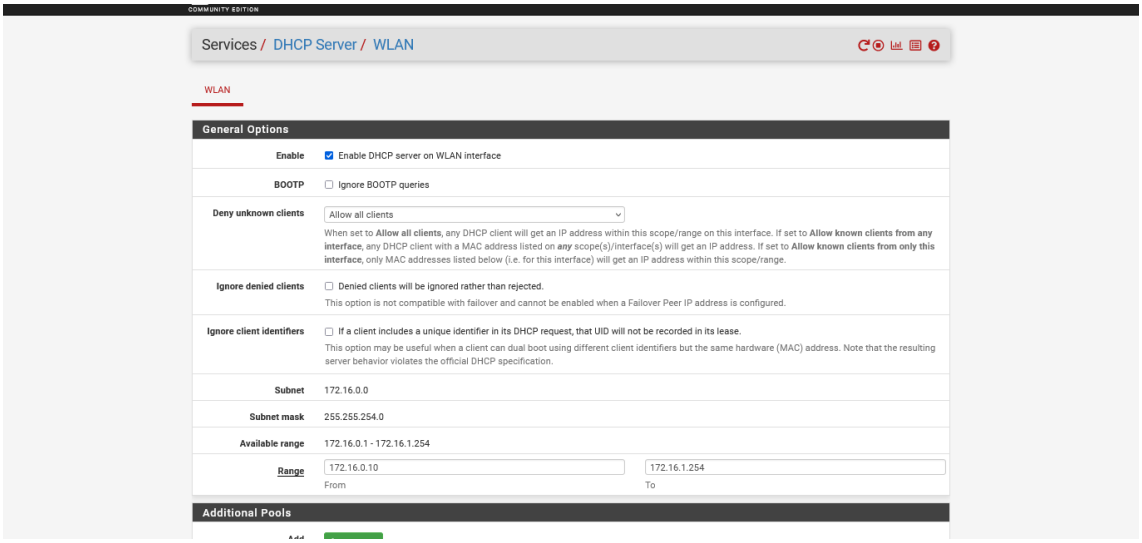


Figura 5.17 Configuración DHCP pfsense

Instalación de Módulos

- NtopNg

  Esta herramienta se utiliza para realizar seguimiento a todos los dispositivos conectados a la red inalámbrica, es un monitor de tráfico en tiempo real, figura Nº 5.18, se puede observar aplicación, protocolo, cliente, servidor, duración, y total de bytes usados.

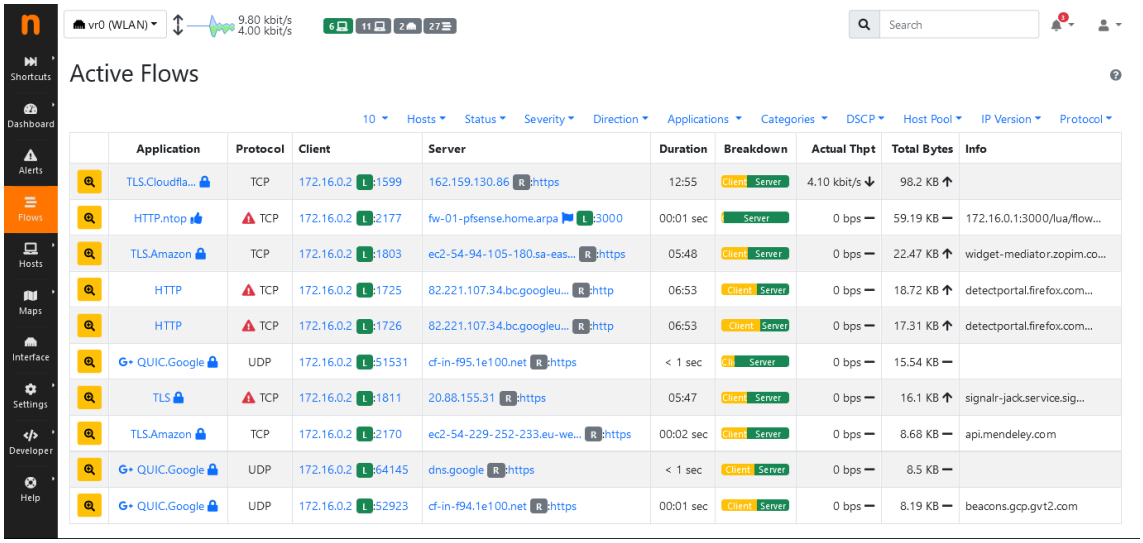


Figura 5.18 Visualización de la herramienta NtopNg

y en la figura Nº 5.19, se visualiza todos los hosts, sus IPs, dirección MAC, Nombre, tiempo de conexión, rendimiento y total de bytes usados. Con todos esos datos el administrador puede dar seguimiento a aquellos equipos que consumen demasiado los recursos de la red.

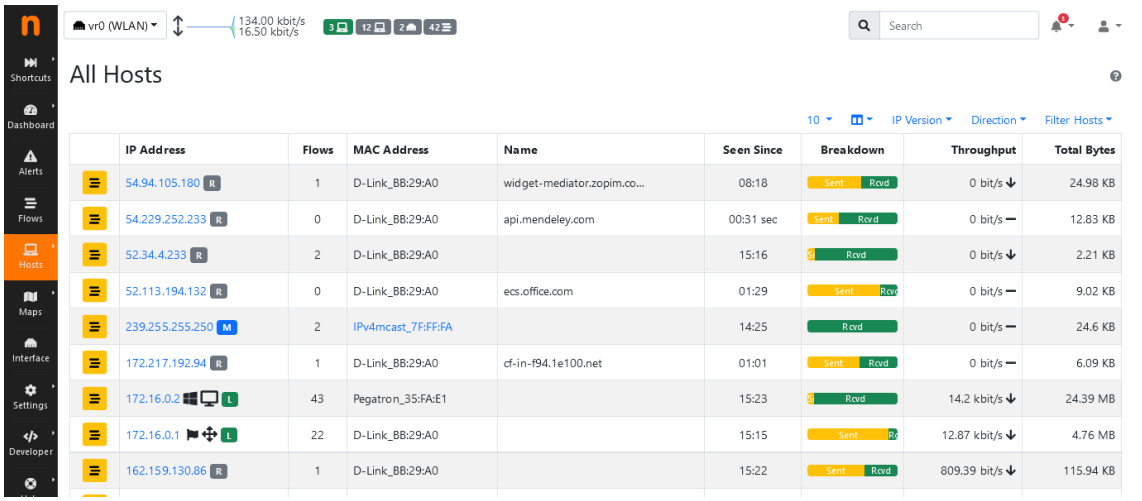


Figura 5.19 Todos los hosts

- **FreeRadius**

  Se implementa para la verificación y autenticación de usuarios, se muestra en la figura Nº 5.20

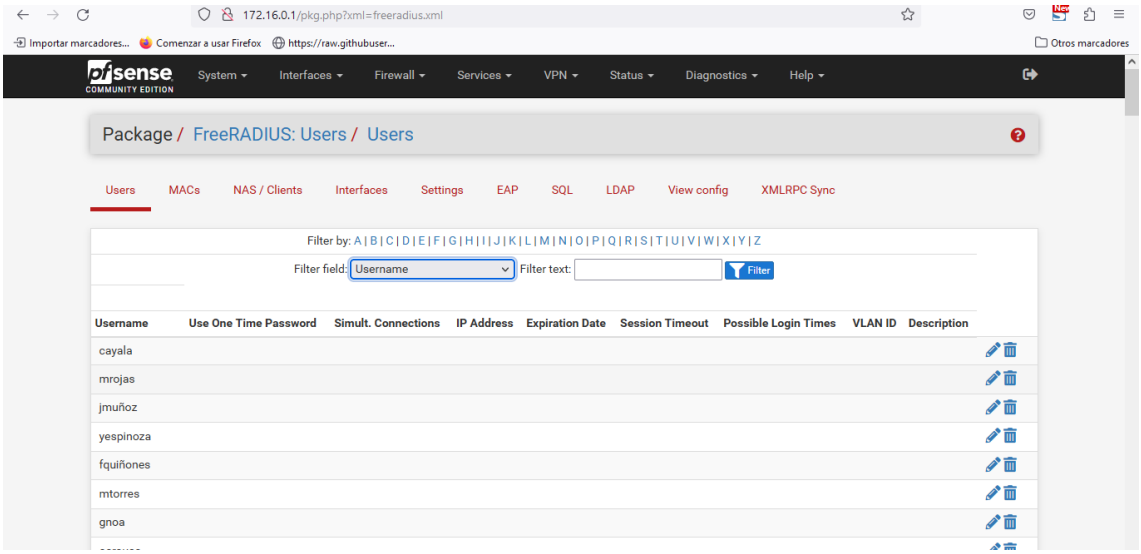


Figura 5.20 FreeRadius

Se crean los usuarios que tienen acceso a red inalámbrica, como se muestra la figura Nº 5.21, ahora seguimos con la creación de usuarios, teniendo en cuenta el primer nombre y apellido, por ejemplo, para el alumno: Pablo Pérez el usuario es pperez y la contraseña se genera utilizando la página web https://pinetools.

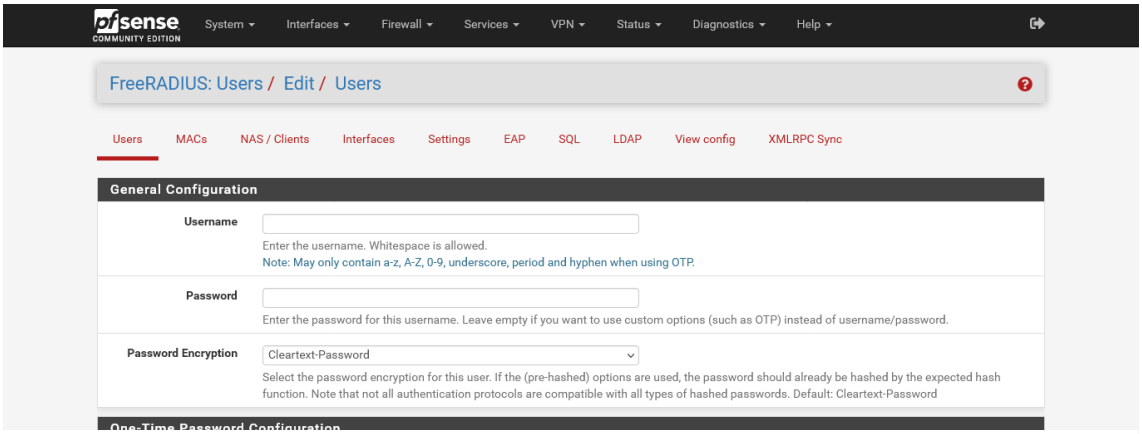


Figura 5.21 Creación de usuarios

- **Portal Cautivo**

  Se encarga de gestionar el acceso a usuarios redirigiéndolos a una página web, donde el usuario debe colocar su usuario y contraseña para poder navegar por internet. Se aplica generalmente en redes inalámbricas como este es el caso.

  Ingresamos a la opción captive portal, se agrega una zona nueva y se realiza las respectivas configuraciones como se muestra en la figura Nº 5.22

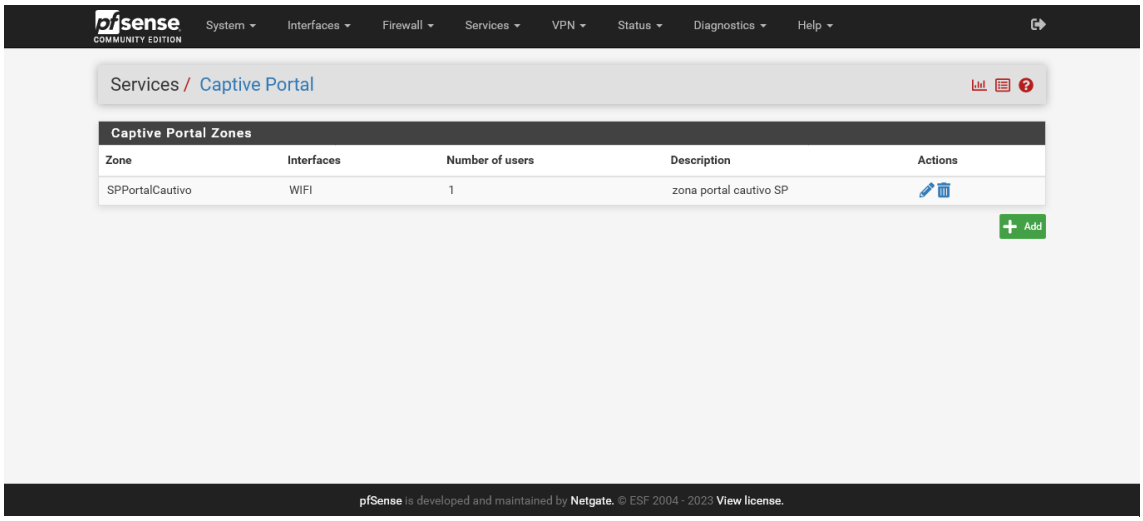


Figura 5.22 Portal cautivo en pfsense

Se crea una zona y se elige la interfaz (WLAN) donde se va implementar el portal cautivo, figura Nº 5.23

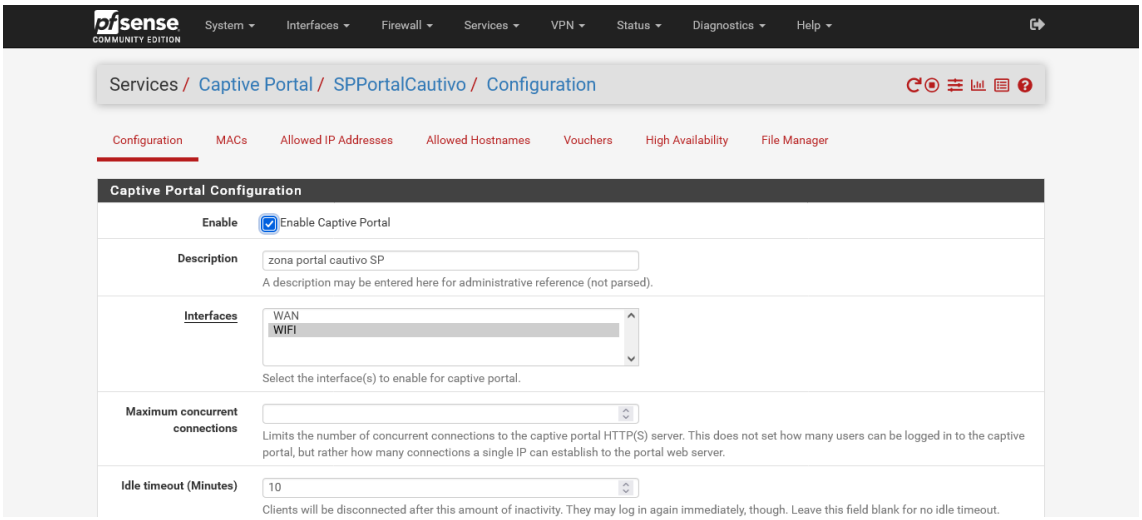


Figura 5.23 Interfaz de red para el portal cautivo

se introduce la página web de redirección una vez se haya autenticado de forma correcta (https://www.istsanpedro.edu.pe/), figura Nº 5.24

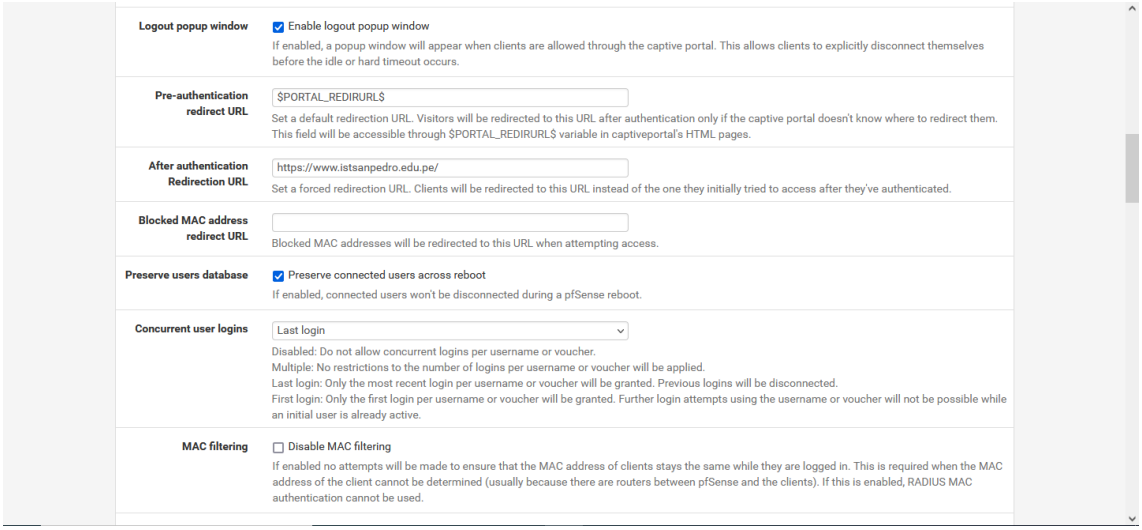


Figura 5.24 Redirección, una vez autenticado en el portal cautivo

Se selecciona el servidor de autenticación FreeRadius

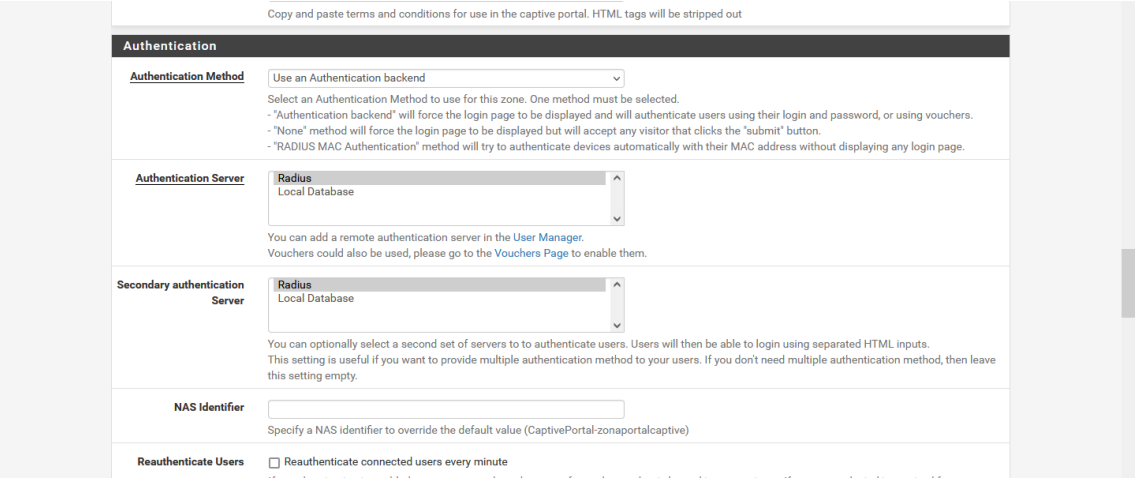


Figura 5.25 selección del servidor FreeRadius

también adjuntamos el logo de la institución, con el objeto que se muestre al momento de solicitar el usuario y contraseña, figura Nº 5.25 y Nº 5.26

Figura 5.26 Adjuntamos el logo de la institución

Finalmente se tiene acceso al portal cautivo, una vez loqueados con las credenciales correctas, tenemos acceso a la navegación web. En la figura Nº 5.27 se muestra la web de logueo

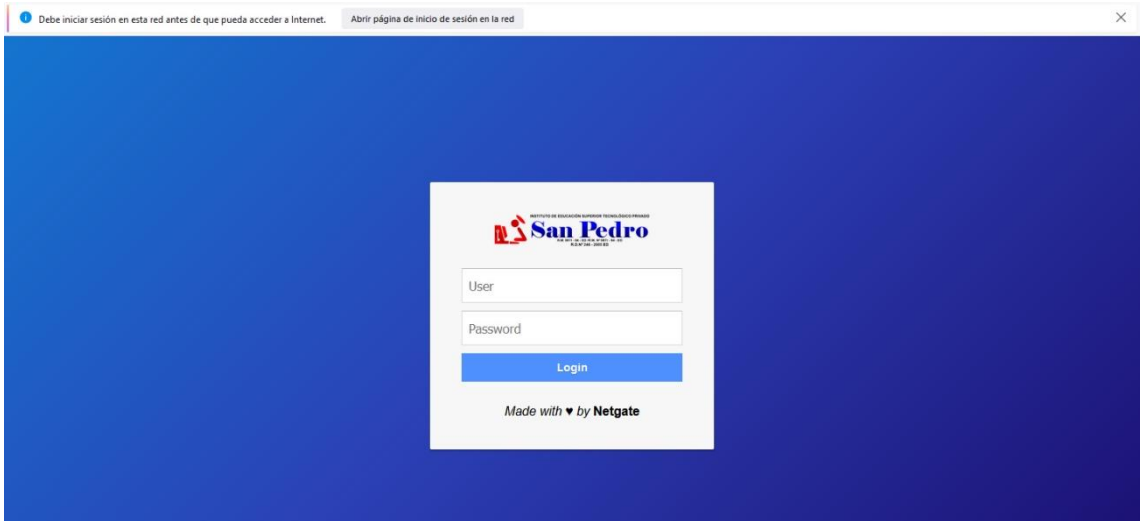


Figura 5.27 página de inicio de sesión del portal cautivo

Una vez finalizado la fase de implementación, se puede observar los servicios instalados en el servidor pfsense, como se muestra en las figuras 5.28, 5.29 y 5.30.

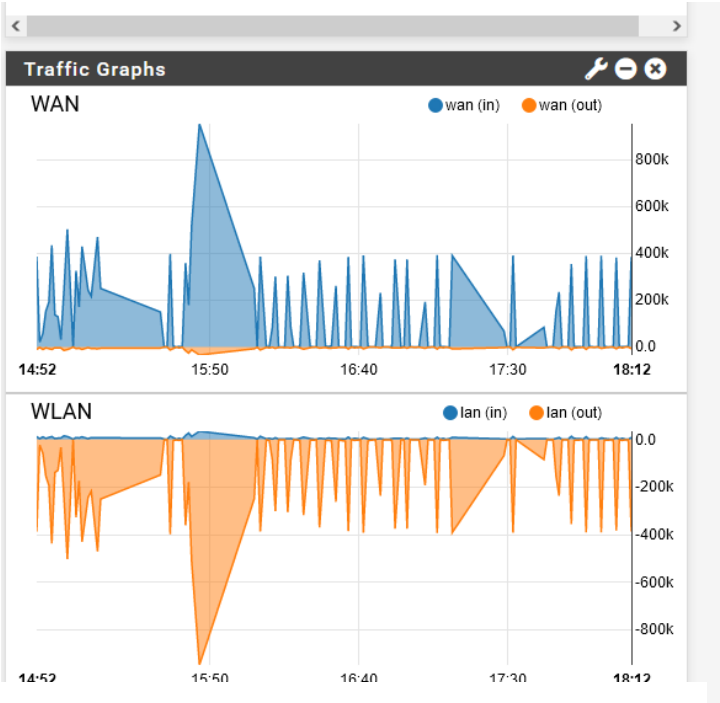
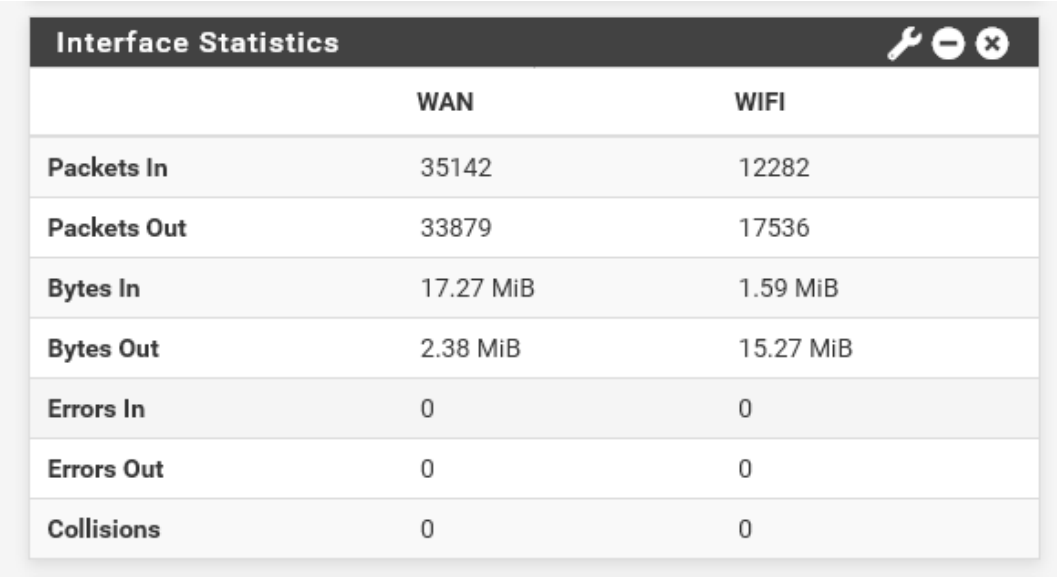


Figura 5.28 tráfico de red de las interfaces WAN y WLAN



Interface Statistics

	WAN	WIFI
Packets In	35142	12282
Packets Out	33879	17536
Bytes In	17.27 MiB	1.59 MiB
Bytes Out	2.38 MiB	15.27 MiB
Errors In	0	0
Errors Out	0	0
Collisions	0	0

Figura 5.29 estadísticas de las interfaces WAN y WLAN

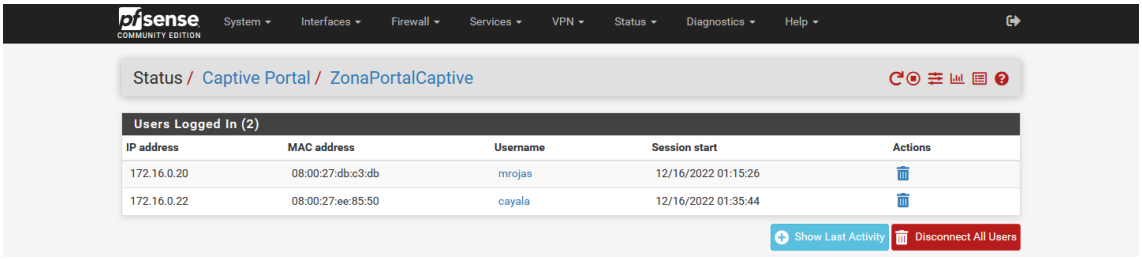


Figura 5.30 Usuarios conectados al portal cautivo

- **pfBlockerNG**

  Se realizó la instalación del pfblocker con el objetivo de bloquear páginas web no autorizadas por el administrador, se gestiona listas de forma automática. Se muestra en la figura Nº 5.31

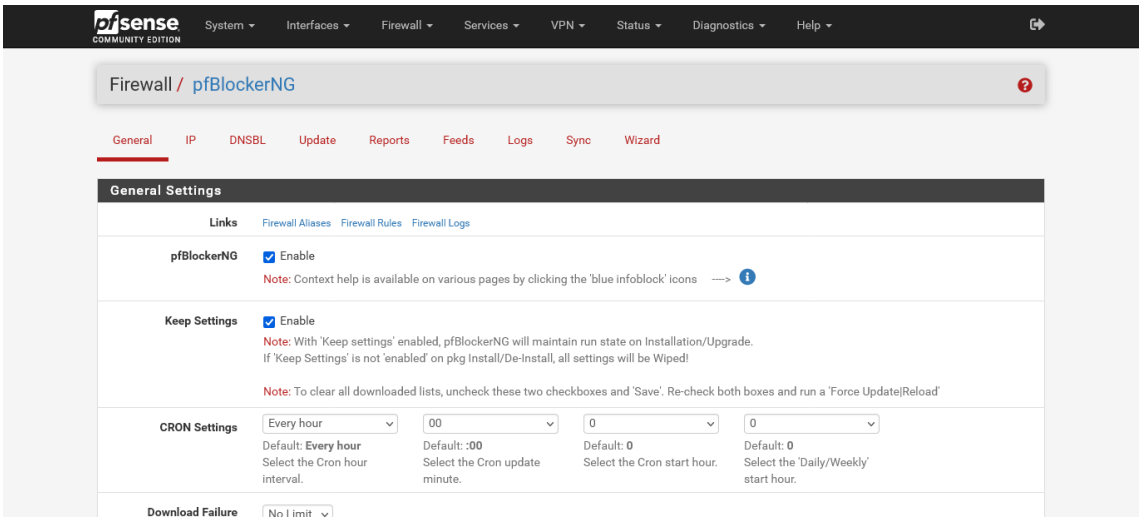


Figura 5.31 pfBlockerNG

Se configuró el pfBlocker, con las listas negras para impedir su navegación, se creó dos listas negras, el primero para bloquear anuncios en las páginas web y el segundo para bloquear páginas web para adultos, se muestra en la figura Nº 5.32

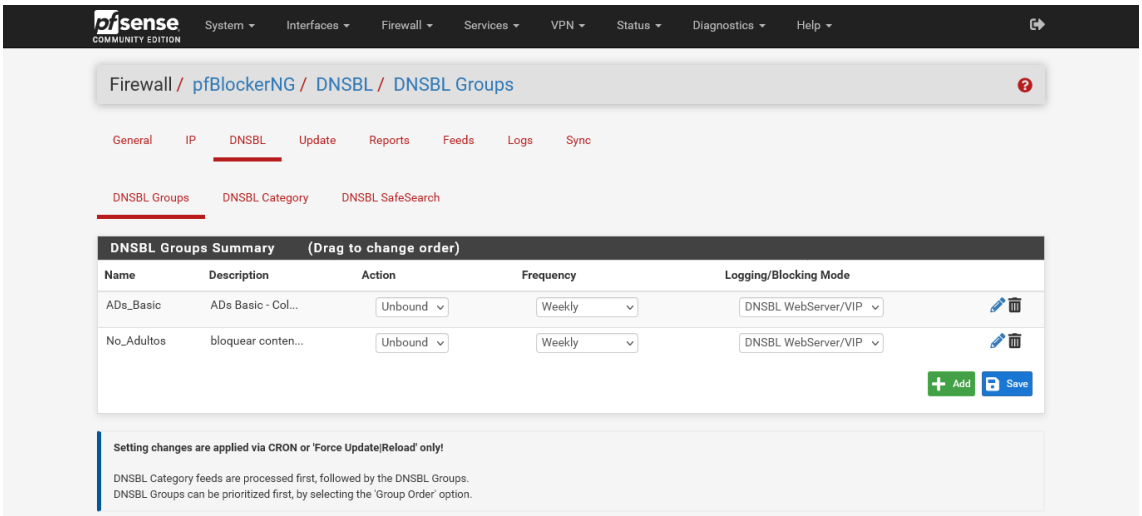


Figura 5.32 Listas negras

- **Reglas de Firewall.**

  Para culminar la implementación, se instala algunas reglas de firewall, con el objeto de tener una mejor administración de seguridad en la red inalámbrica de la institución

  Regla 1. Impedir que se realice ping al servidor

  Regla 2. El tráfico con protocolo TCP/UDP que tenga como destino la red WAN pasará por el puerto 53 (DNS).

  Regla 3. Permite el tráfico del protocolo TCP/UDP entre todos los hosts pertenecientes a la red.

  Regla 4. Permite el tráfico del protocolo TCP/UDP, de todos los hosts de la red hacia los puertos 80, 443, 53, 8443

  Regla 5: Se bloquea todo lo no enumerado en las reglas anteriores

En la figura Nº 5.33, se muestra el dashboard del servidor pfsense, con todos los servicios funcionando.

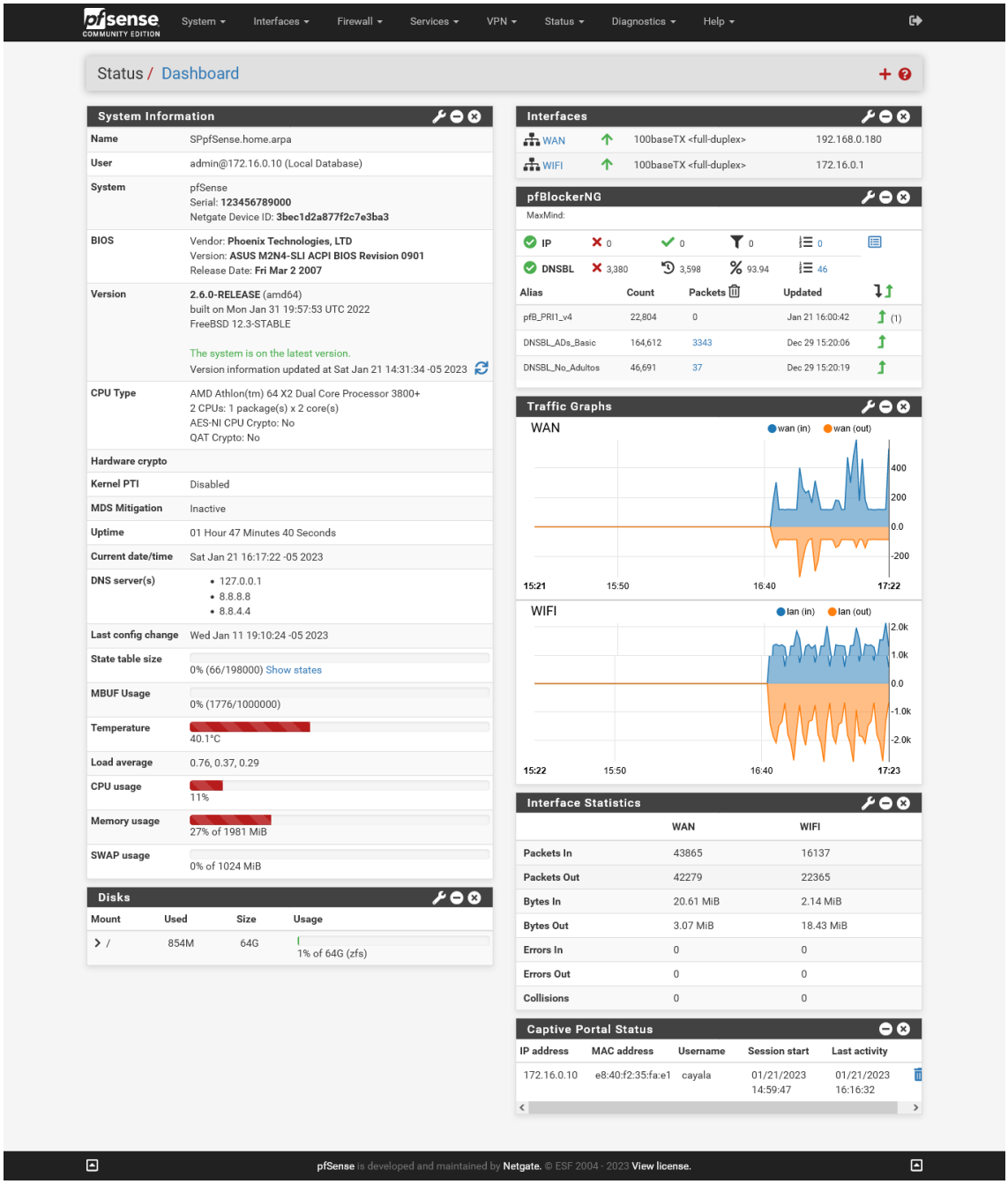


Figura 5.33 Dashboard del PFSense