INSTITUTO SUPERIOR TECNOLÓGICO

SUDAMERICANO

QUITO - ECUADOR

ESCUELA DE

DESARROLLO DE SOFTWARE

PROYECTO DE TITULACIÓN

TEMA:

DISEÑO E IMPLEMENTACIÓN DE UN PORTAL CAUTIVO PARA EL EDIFICIO MATRIZ DEL INSTITUTO SUPERIOR TECNOLÓGICO SUDAMERICANO QUITO

AUTORAS: MORALES FREIRE STEFI GABRIELA

ZAMBRANO PILATASIG KELLY MISHELL

TUTOR: MSc. VILLASIS FABRIZIO

San Francisco de Quito, noviembre del 2023

AUTORÍA

Nosotras, Morales Freire Stefi Gabriela, portadora de la cédula de ciudadanía No.172011573-0 y Zambrano Pilatasig Kelly Mishell, portadora de la cédula de ciudadanía No. 172623945-0, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional y que hemos consultado he investigado en base a las referencias bibliográficas que se incluyen en este documento. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por nosotras.

Morales Freire Stefi Gabriela	**Zambrano Pilatasig Kelly Mishell**

CERTIFICACIÓN

Una vez que se ha culminado la elaboración del proyecto de titulación cuyo tema es: “Diseño e implementación de un portal cautivo para el edificio matriz del Instituto Superior Tecnológico Sudamericano Quito”, certifico que el mismo se encuentra habilitado para su defensa pública.

MSc. Fabrizio Villasís Chiriboga
Coordinador de la Escuela de Desarrollo de Software
Instituto Superior Tecnológico Sudamericano Quito

CERTIFICACIÓN

Por medio del presente certifico que las señoritas Morales Freire Stefi Gabriela y Zambrano Pilatasig Kelly Mishell, han realizado y concluido su trabajo de titulación, cuyo tema es: "Diseño e implementación de un portal cautivo para el edificio matriz del Instituto Superior Tecnológico Sudamericano Quito", para obtener el título de Tecnólogo en Desarrollo de Software, bajo mi tutoría.

MSc. Fabrizio Villasís Chiriboga
Coordinador de la Escuela de Desarrollo de Software
Instituto Superior Tecnológico Sudamericano Quito

AGRADECIMIENTOS

Primeramente, damos gracias a Dios por permitirnos realizar el presente proyecto dentro del Instituto Superior Tecnológico Sudamericano de la ciudad de Quito y poder aplicar los conocimientos adquiridos en nuestra institución. Queremos también reconocer los esfuerzos de nuestros padres, que con su apoyo incondicional nos ayudaron a perseverar hasta el final. Agradecemos a nuestro tutor MSc. Fabrizio Villasís Chiriboga que con su apoyo, dedicación y conocimiento supo encaminarnos en la culminación de la presente tesis.

Agradezco a aquellos que han sido parte del recorrido y han contribuido en este proyecto de tesis, reconocemos que sin su ayuda no hubiéramos podido finalizar con éxito.

Finalmente agradecemos a quien lee la presente tesis, por darnos la oportunidad de compartir nuestro trabajo y conocimientos.

DEDICATORIA

Este proyecto de titulación la dedicamos a nuestro Dios que con su guía, amor y bendición nos ha permitido culminar este proceso y dar este paso tan importante en nuestras vidas, reconocemos que sin él no hubiéramos llegado hasta aquí. A nuestros padres que han sido personas incondicionales en nuestras vidas y que en medio de los obstáculos nos han motivado a seguir adelante. Dedicamos también a nuestros hermanos y amigos quienes fueron nuestra fuente de inspiración y aliento en nuestras vidas.

RESUMEN

El presente proyecto tiene como objetivo principal el diseño e implementación de un Portal Cautivo en el edificio matriz del Instituto Superior Tecnológico Sudamericano de la ciudad de Quito, es una página web que se utiliza para autenticar y autorizar a los usuarios, en este caso a los alumnos, antes de permitirles el acceso a la red inalámbrica privada de la institución. Esta página aparecerá no solo a todos los estudiantes con actividades presenciales en el edificio matriz, sí no también a todos los visitantes que requieran internet vía wifi. El objetivo principal es proporcionar un mecanismo de autenticación y control de acceso a la red, así como también permite prevenir la congestión de la red de computadoras en el edificio principal del Instituto Superior Tecnológico Sudamericano Quito.

Adicionalmente, en este proyecto se ha implementado un dispositivo de almacenamiento conectado a la red del edificio para proporcionar almacenamiento de datos compartido y servicios de archivo a todos los dispositivos conectados en la red local (LAN) conocido como servidor NAS (Network-Attached Storage, por sus siglas en inglés). Su principal función es servir como un repositorio centralizado y accesible para almacenar y compartir archivos, lo que facilita la colaboración, el respaldo de información y el acceso a datos en la red del edificio, beneficiando a la Institución.

Contar con un Portal Cautivo y un servidor NAS en el edificio matriz de la Institución ofrece ventajas significativas. El Portal Cautivo asegura el acceso a la red Wi-Fi® de la institución solo a los usuarios autorizados, se tiene un dominio de difusión específico para los dispositivos móviles de los estudiantes lo que mejora la seguridad de datos, la navegación por Internet y también permite socializar mensajes del Instituto hacia este alumnado. Por otro lado, el servidor

NAS ofrece un lugar de almacenamiento centralizado de archivos y de servicios de red, dentro de la red de área local del Instituto, lo que permite la gestión eficiente de datos y recursos compartidos. Juntos, estos sistemas mejoran la conectividad, la seguridad de datos y la gestión de recursos digitales, beneficiando a estudiantes, personal docente y administrativo.

La instalación e implementación del Portal Cautivo se llevó a cabo utilizando software de código abierto llamado pfSense, que forma parte de la distribución FreeBSD y fue creado por la empresa Rubicon Communications, LLC (Netgate), especializada en soluciones de enrutamiento open source. Esto proporcionó la facilidad y versatilidad necesarias para configurar el acceso a Internet a través de váuchers lo que, a su vez, evita el uso indebido y la congestión de la red para los estudiantes y para el personal que trabaja en el edificio matriz. El servidor NAS fue implementado con el software de la empresa Synology.

En este documento se contempla el marco teórico con las definiciones y conceptos que sustentan al Portal Cautivo, como al servidor NAS, y por qué, dentro de las diferentes alternativas, se eligió trabajar con estos. También se desarrolla y explica la implementación de ambos, como una guía que sirve de evidencia del trabajo realizado.

ABSTRACT

The main objective of this project is the design and implementation of a Captive Portal in the main building of the South American Technological Institute of Quito, which is a web page used to authenticate and authorize users, specifically students, before allowing them access to the institution's private wireless network. This page will not only appear to all students with on-site activities in the main building but also to all visitors requiring Wi-Fi internet access. The primary aim is to provide an authentication and access control mechanism for the network, as well as to prevent network congestion in the main computer network of the South American Technological Institute in Quito.

Additionally, this project has implemented a network-attached storage (NAS) device connected to the building's network to provide shared data storage and file services to all devices connected to the local area network (LAN). Its primary function is to serve as a centralized and accessible repository for storing and sharing files, facilitating collaboration, data backup, and access to data within the building's network, benefiting the institution.

Having a Captive Portal and a NAS server in the main building of the institution offers significant advantages. The Captive Portal ensures access to the institution's Wi-Fi network only for authorized users. There is a specific broadcast domain for students' mobile devices, improving data security, internet browsing, and allowing the institution to communicate messages to its students. On the other hand, the NAS server provides centralized file storage and network services within the Institute's local area network, allowing for efficient data management and shared resources. Together, these systems improve connectivity, data security, and digital resource management, benefiting students, teaching staff, and administrators.

The installation and implementation of the Captive Portal were carried out using open-source software called pfSense, which is part of the FreeBSD distribution and was created by the company Rubicon Communications, LLC (Netgate), specializing in open-source routing solutions. This provided the necessary ease and versatility to configure internet access through vouchers, thereby preventing misuse and network congestion for students and staff working in the main building. The NAS server was implemented using Synology's software.

This document includes the theoretical framework with definitions and concepts that support the Captive Portal and the NAS server, as well as the reasons why, among different alternatives, these were chosen to work with. It also develops and explains the implementation of both as a guide that serves as evidence of the work carried out.

ÍNDICE

1. Introducción 1
2. Justificación 3
3. Antecedentes 5
4. Objetivos 7
4.1. Objetivo General 7
4.2. Objetivos Específicos 7
5. Marco Teórico 8
5.1. Redes de computadoras 8
5.1.1 Función de una red de computadoras 9
5.1.2 Componentes de una red 9
5.1.3 Equipos y servicios en una red de computadoras 10
5.2. Tipos de topología de red 18
5.2.1. Topología de red estrella 18
5.2.2. Topología de red bus 19
5.2.3. Topología de red anillo 20
5.2.4. Topología de red malla 20
5.3. Tipos de redes 21
5.3.1. Red de área personal (PAN) 21
5.3.2. Red de área local (LAN) 22
5.3.3. Red de área local inalámbrica (WLAN) 24
5.3.4. Red de área de campus (CAN) 25
5.3.5. Red de área metropolitana (MAN) 26
5.3.6. Red de área amplia (WAN) 27
5.3.7. Red de área de almacenamiento (SAN) 28
5.3.8. Red de área local óptica pasiva (POLAN) 29
5.3.9. Red privada empresarial (EPN) 30
5.3.10. Red privada virtual (VPN) 31
5.4. Redes inalámbricas 32
5.4.1. Tipos de redes inalámbricas 33
5.5. Wifi 34
5.6. IEEE 802.11 35
5.6.1. Tipos de redes IEEE 802.11 36

5.7. Encriptación 42
5.7.1. WPS 43
5.7.2. WPA2 44
5.7.3. WPA2-PSK 45
5.7.4. AES 47
5.8. Internet 48
5.9. Firewalls 49
5.10. Visual Studio Code 49
5.10.1. Para que sirve Visual Studio Code 49
5.11. Páginas web 51
5.11.1. HTML 53
5.11.2. CSS 55
5.12. Portales Cautivos 57
5.12.1. Wifidog 57
5.12.2. IPCop 59
5.12.3. pfSense 60
5.12.4. Comparación de pfSense vs otros portales cautivos 64
5.13. Correos electrónicos masivos 65
5.13.1. MailChimp 66
5.13.2. AWeber 68
5.13.3. Odoo 69
5.14. NAS 72
5.14.1. Synology 74
5.14.2. TerraMaster 75
5.14.3. Proyecto de Titulación de Galarza Vecilla Héctor Andrés 77
5.14.4. TrueNAS 78
6. Desarrollo del Proyecto 82
6.1. Infraestructura de la red informática del edificio matriz 82
6.2. Portal Cautivo pfSense 103
6.2.1. Descarga de pfSense 105
6.2.2. Instalación de pfSense 109
6.2.3. Configuración de pfSense 112
6.3. Correos masivos con MailChimp 138
6.4. Servidor NAS Synology 162

6.4.1. Instalación y configuración del servidor NAS Synology DSM 7.2 164
6.4.2. Creación de Usuarios y Grupos 177
6.4.3. Ubicación del servidor NAS y acceso a los servicios 182
6.5 Funcionamiento y pruebas 183
7. Conclusiones y Recomendaciones 205
7.1. Conclusiones 205
7.2. Recomendaciones 206
8. Referencias 208
ANEXOS 223

ÍNDICE DE FIGURAS

Figura 1. Idealización de una red de computadoras. 8
Figura 2. Esquema de conexión típico de un sistema en red. 9
Figura 3. Componentes habituales de una red. 10
Figura 4. Esquema de un Switch. 12
Figura 5. Equipo Router Home con Punto de Acceso inalámbrico incluido. 14
Figura 6. Tarjeta de red o network interface controller (NIC). 15
Figura 7. Tarjeta de red inalámbrica (wireless), conocida también como tarjeta de Wifi. 16
Figura 8. Tarjeta para red óptica. 17
Figura 9. Ejemplo de una topología de red en estrella. 19
Figura 10. Ejemplo de una topología de red en bus. 19
Figura 11. Ejemplo de una topología de red en anillo. 20
Figura 12. Ejemplo de una topología de red en malla. 21
Figura 13. Diagrama representativo de una Red PAN. 22
Figura 14. Diagrama representativo de una red LAN. Fuente: (concepto.de, 2023) 23
Figura 15. Diagrama representativo de una Red WLAN. 25
Figura 16. Diagrama representativo de una Red CAN. 26
Figura 17. Diagrama representativo de una Red MAN. 27
Figura 18. Diagrama representativo de una red WAN. 28
Figura 19. Diagrama representativo de una red SAN. 28
Figura 20. Diagrama representativo de una red POLAN. 29
Figura 21. Diagrama representativo de una red EPN. 30
Figura 22. Diagrama representativo de una red VPN. 31
Figura 23. Diagrama representativo de una red inalámbrica. 33
Figura 24. Diagrama representativo de una arquitectura lógica funcional IEEE 802.11. 36
Figura 25. Etiquetas HTML. 53
Figura 26. Estructura básica HTML. 54
Figura 27. Ejemplo de etiquetas básicas HTML. 55
Figura 28. Portal cautivo Wifidog. 58
Figura 29. Portal cautico IPCop. 60
Figura 30. Portal Cautivo pfSense 61
Figura 31. Portal cautivo con pfSense, ventana de autentificación. 63
Figura 32. Pantalla principal de MailChimp. 66

Figura 33. Planes de MailChimp. 67
Figura 34. Pantalla principal de AWeber. 68
Figura 35. Plataforma de Odoo, marketing por email. 70
Figura 36. Plan y precios de Odoo. 71
Figura 37. Representación general de la red informática del edificio matriz INTESUD. 84
Figura 38. Esquema de red original del edificio matriz del INTESUD. 87
Figura 39. Esquema de red organizada y reconfigurada del edificio matriz del INTESUD. ... 93
Figura 40. Esquema de red rediseñada con VLAN del edificio matriz del INTESUD. 96
Figura 41. Configuración del Router Cisco RV325. 99
Figura 42. Infraestructura de red con Portal Cautivo del edificio matriz del INTESUD. 101
Figura 43. Diagrama conexiones de red del servidor Portal Cautivo pfSense. 102
Figura 44. Pantalla de inicio de ingreso del Portal Cautivo. 105
Figura 45. Descarga de la imagen ISO de pfSense. 106
Figura 46. Programa para crear medios USB de arranque. 106
Figura 47. Configuración de la UEFI (o BIOS) para arrancar la PC por USB. 107
Figura 48. Instalación y configuración del programa pfSense, pantalla de inicio. 108
Figura 49. Instalación de pfSense, configuración de idioma de teclado. 109
Figura 50. Instalación de pfSense, particiones de disco. 110
Figura 51. Instalación de pfSense, barra de progreso de la instalación. 110
Figura 52. Instalación de pfSense, manual de configuración. 111
Figura 53. Instalación de pfSense, mensaje de instalación exitosa. 111
Figura 54. Terminal de configuración de pfSense en el servidor. 112
Figura 55. Configuración de pfSense, ingreso por PC cliente al modo gráfico de configuración, vía IP utilizando un navegador web. 113
Figura 56. Configuración de pfSense, pantalla de ingreso al modo de configuración gráfica de pfSense. 114
Figura 57. Configuración de pfSense, pantalla de inicio de bienvenida al dashboard de pfSense. 114
Figura 58. pfSense Dashboard. 115
Figura 59. pfSense, pantalla de configuración general. 116
Figura 60. pfSense, configuración de la ubicación geográfica (localización del tiempo). 117
Figura 61. pfSense, configuración de certificados para la seguridad de red y protección. 118
Figura 62. pfSense, configuración básica de certificados de los requisitos de seguridad. 119
Figura 63. pfSense, configuración de la tarjeta de red WAN (re0). 121

Figura 64. pfSense, configuración de la tarjeta de red LAN (re1). 122
Figura 65. pfSense, configuración de la tarjeta OPT1 (bge0). 123
Figura 66. pfSense, configuración del servicio DHCP para la LAN. 125
Figura 67. pfSense, configuración de DHCP server sobre OPT1. 126
Figura 68. pfSense, reglas de Firewall por defecto para WAN. 127
Figura 69. pfSense, edición de la regla general del Firewall para la interface WAN. 128
Figura 70. pfSense, configuración de la zona Portal Cautivo. 129
Figura 71. pfSense, configuración del Portal Cautivo. 131
Figura 72. pfSense, configuración de personalización del logo del Portal Cautivo. 132
Figura 73. pfSense, administración de archivos del Portal Cautivo. 133
Figura 74. pfSense, generador de váuchers. 135
Figura 75. pfSense, página web de inicio de sesión del Portal Cautivo para un usuario. 136
Figura 76. pfSense, redireccionamiento a la URL de inicio luego del ingreso exitoso por el Portal Cautivo. 136
Figura 77. pfSense, registro total de usuarios del Portal Cautivo. 137
Figura 78. Búsqueda de MailChimp en un buscador de Internet. 138
Figura 79. Resultado de búsqueda de MailChimp, Plataforma de marketing. 139
Figura 80. Página web principal de MailChimp. 140
Figura 81. Planes de servicio de correos masivos de MailChimp. 140
Figura 82. Ventana emergente para el registro de usuario nuevo en MailChimp. 141
Figura 83. Correo de aprobación de MailChimp. 142
Figura 84. Configuración de una nueva cuenta de MailChimp. 145
Figura 85. Selección del plan asociada a la nueva cuenta de MailChimp. 146
Figura 86. Proceso de creación de la nueva cuenta de MailChimp. 146
Figura 87. Página principal de la cuenta MailChimp. 147
Figura 88. Creación y configuración de “Campañas” en MailChimp. 148
Figura 89. Opciones de diseño de un correo electrónico en MailChimp. 148
Figura 90. Partes del diseño de un correo electrónico. 149
Figura 91. Título de la campaña. 149
Figura 92. Selección de destinatarios para envió del correo electrónico. 150
Figura 93. Importación de usuarios mediante la carga de archivo CSV. 151
Figura 94. Carga y envió de archivos. 151
Figura 95. Organización de contactos. 152
Figura 96. Etiquetado de contactos. 152

Figura 97. Detalles de ¿Quién envía este correo electrónico? 153
Figura 98. Tema designado para envío de información a usuarios. 153
Figura 99. Hora de envió por defecto del correo electrónico. 154
Figura 100. Diseño del contenido del correo electrónico. 154
Figura 101. Plantillas de correo electrónico de MailChimp. 154
Figura 102. Plantilla base para la personalización. 155
Figura 103. Personalización del correo masivo con el logo institucional. 155
Figura 104. Carga de archivos a la plataforma MailChimp. 156
Figura 105. Introducción de información personalizado, envió correos masivos. 156
Figura 106. Diseño de plantilla institucional para el envío de correos masivos por MailChimp. 158
Figura 107. Ejemplo de correo electrónico masivo para la socialización del ingreso al Wifi por váucher. 161
Figura 108. Topología de red administrativa y sus servidores. 163
Figura 109. Terminal del servidor NAS. 166
Figura 110. Acceso al servidor NAS Synology por navegador web. 167
Figura 111. Pantalla de inicio del Login del servidor NAS. 168
Figura 112. Descarga de aplicaciones en el servidor NAS. 169
Figura 113. Centro de paquetes de instalación de aplicaciones del servidor NAS. 170
Figura 114. Estación de archivos, ubicación de archivos multimedia. 171
Figura 115. Audio Station, reproductor de música o gestor de música. 171
Figura 116. Aplicación “fotos” donde se ubican los archivos de imágenes del usuario. 172
Figura 117. Video Station, reproductor de videos y de películas. 172
Figura 118. Configuración de usuario y de carpeta compartida. 173
Figura 119. Drive (carpeta compartida), sincronización de los archivos. 174
Figura 120. Drive, descarga de aplicación para escritorio y celular. 174
Figura 121. Ejecución de programa Synology Drive Client. 175
Figura 122. Configuración de las carpetas de sincronización. 175
Figura 123. Descargar aplicaciones en el celular desde Synology Drive para móvil. 176
Figura 124. Acceso al servidor NAS desde un celular. 177
Figura 125. Evidencia de la creación de usuarios en el servidor NAS. 179
Figura 126. Creación de grupos en el servidor NAS 181
Figura 127. Ubicación del servidor NAS Synology DSM7.2 en el Rack de piso. 182
Figura 128. Reorganización del rack. 185

Figura 129. Shell o terminal del servidor pfSense. 189
Figura 130. Ubicación del servidor pfSense Portal Cautivo en el Rack de piso. 189
Figura 131. Estadísticas del Gráfico Interactivo de pfSense. 190
Figura 132. Estadísticas del tráfico de datos WAN en el servidor pfSense. 191
Figura 133. Estadísticas del tráfico de datos de LAN. 191
Figura 134. Pruebas de arrendamiento de direcciones IPv4 por el DHCP del Portal Cautivo. 192
Figura 135. Pruebas de configuración y generación de váuchers Portal Cautivo. 193
Figura 136. Prueba del rol de estudiantes (váuchers) para el ingreso por el Portal Cautivo.. 195
Figura 137. Archivo Excel formateado para MailChimp para la campaña de socialización de váuchers. 196
Figura 138. Pantalla de pfSense para dar de baja a usuarios del Portal Cautivo. 197
Figura 139. Pruebas del envío de correo masivo con MailChimp. 197
Figura 140. Ingreso por el Portal Cautivo a la red Wifi sin utilización de váuchers. 198
Figura 141. Ingreso por el Portal Cautivo a la red Wifi con utilización de váuchers. 199
Figura 142. Ubicación del servidor NAS en el Rack de piso. 201
Figura 143. Pruebas de funcionamiento del servidor NAS Synology, pantalla principal administrativa por la app DS Find desde un dispositivo móvil. 202
Figura 144. Aplicaciones para dispositivos móviles para la gestión de servicios del servidor NAS. 204

ÍNDICE DE TABLAS

Tabla 1. Comparación entre WPA Y WPA2. 46
Tabla 2. Comparativa entre portales cautivos investigados. 64
Tabla 3. Comparativa entre plataformas de correos masivos investigados. 71
Tabla 4. Comparativa entre plataformas NAS investigadas. 80
Tabla 5. Puntos de red del edificio matriz y su nomenclatura. 90
Tabla 6. Puntos de red del edificio matriz y su reorganización. 91
Tabla 7. Tabla de usuarios en el servidor NAS Synology institucional. 178
Tabla 8. Tabla de grupos del servidor NAS Synology institucional. 180

LISTA DE ANEXOS

Anexo 1: Documentación de pfSense 224
Anexo 2: Documentación de correo masivos MailChimp 225
Anexo 3: Documentación del servidor NAS 226

1. Introducción

Las redes wifi y el acceso a Internet han transformado radicalmente el mundo actual al convertirse en un tejido vital de nuestra sociedad digital. Han derribado barreras geográficas y permitido una comunicación instantánea, el acceso a información global, la educación en línea, la colaboración remota y la expansión del comercio electrónico. Estas tecnologías han empoderado a las personas, empresas y gobiernos, acelerando la innovación, mejorando la eficiencia y creando oportunidades económicas sin precedentes.

Sin embargo, las redes Wi-Fi® pueden dar lugar a varios problemas y desafíos, especialmente si la red no está diseñada adecuadamente para manejar muchos usuarios. Tener muchas conexiones simultáneas causa congestión en la red LAN, es decir, ralentiza la velocidad de la conexión para todos los usuarios y, por lo tanto, hace que las aplicaciones y servicios en línea funcionen más lentamente. Esto también conlleva una pérdida del ancho de banda, ya que, cuantos más usuarios haya, más ancho de banda se consume y esto puede llevar a una disminución significativa de la velocidad de Internet disponible para cada usuario con una latencia de red aumentada, lo que provoca retrasos en la carga de páginas web, la transmisión de video y la interacción en tiempo real.

Por último, una red wifi con mucha carga provoca problemas de seguridad, ya que es más vulnerable a ataques de seguridad y a intrusiones a información confidencial, también provoca problemas de gestión y de escalabilidad, lo que conlleva que, para acomodar un crecimiento repentino de nuevos usuarios, sea necesario nuevas inversiones en hardware y configuraciones más avanzadas.

Un portal cautivo es una solución que puede ayudar a abordar los problemas asociados con tener una red wifi con muchos usuarios, ya que, al requerir que estos autentifiquen su identidad, antes de acceder a la red inalámbrica, mejora la seguridad y el control de acceso. Además, permite a los administradores definan reglas de acceso y recopilen datos sobre los usuarios, lo que facilita la gestión de recursos y la personalización de la experiencia.

Por lo tanto, en este proyecto de titulación, se realiza el diseño e implementación de un portal cautivo para el edificio matriz del Instituto Superior Tecnológico Sudamericano de la ciudad de Quito, con el objetivo de desarrollar una solución efectiva que cumpla con los requisitos de seguridad y de control de acceso.

El portal cautivo trae consigo beneficios para los alumnos que asisten de manera presencial al edificio matriz de la institución, los cuales, como consumidores de servicios de Internet, se les garantiza una conexión segura al requerir autenticación y control de acceso mediante un código único de once dígitos, proporcionado a través de un váucher que se les entrega vía correo electrónico.

Adicionalmente, se implementa un Sistema de Almacenamiento en Red, conocido como NAS, el cual complementa servicios de red en la LAN de la Institución, como lo son gestionar y compartir archivos de forma segura, así como aplicaciones de administración de videos, de imágenes, de música, entre otros servicios. En cuanto a los recursos, se utilizó todo el hardware disponible en la institución, evitando inversiones adicionales, y se seleccionó el software más adecuado, tanto para el Portal Cautivo como para el NAS, terminando con las pruebas de funcionamiento para evaluar la funcionalidad de la nueva infraestructura de red.

2. Justificación

El Instituto Superior Tecnológico Sudamericano Quito ofrece el Internet de forma gratuita para el personal administrativo, docentes e invitados, así como también a los estudiantes que asisten presencialmente a sus actividades académicas en el edificio matriz de la institución. Esto conlleva a una creciente dependencia de las redes wifi y justifica la necesidad de innovar continuamente la infraestructura y gestión de las redes informáticas para mantenerse al día con las demandas de estudiantes y personal. En este sentido, el Instituto Superior Tecnológico Sudamericano de Quito reconoce la importancia de proporcionar una red segura, eficiente y confiable para su comunidad. El diseño e implementación de un portal cautivo abordan directamente esta necesidad, alineándose con las tendencias y necesidades de administración de redes que priorizan la seguridad, el servicio y el rendimiento.

Como institución educativa, en cada nuevo periodo académico, existe un aumento significativo en el volumen de dispositivos conectados a la red del instituto, por lo que se tiene la necesidad de garantizar la seguridad de la red, el control de acceso, la escalabilidad y la gestión eficiente de recursos. Esto requiere una solución que no sólo mejore la capacidad de la red existente sin inversiones significativas en hardware adicional, sino que también refuerce las políticas de seguridad informática y ofrezca una experiencia satisfactoria a los estudiantes y al personal que utilizan la red Wi-Fi® en el edificio matriz. Garantizar un acceso seguro y gestionar los recursos de manera efectiva, es una mejora sustancial en la calidad de los servicios educativos ofrecidos.

La justificación de este proyecto se basa en la importancia de proporcionar una solución que mejore la experiencia de los usuarios, también garantice la integridad de la red y la seguridad de la información. Además, al utilizar los recursos disponibles en la institución y seleccionar cuidadosamente el software adecuado, se busca minimizar la inversión adicional y optimizar la eficiencia operativa. El portal cautivo se presenta como parte de la solución y como la herramienta estratégica para gestionar el acceso a la red, mitigar el riesgo de uso inadecuado y proporcionar una capa adicional de seguridad contra accesos no autorizados o malintencionados.

El Portal Cautivo utiliza váuchers, lo que permite el acceso a la banda ancha de Internet solo a los usuarios debidamente registrados, evitando así un uso inadecuado de la conexión a Internet y la saturación de la red. El váucher que se proporciona a los estudiantes es mediante correo electrónico y únicamente a aquellos que hayan cumplido con las responsabilidades económicas establecidas por la institución.

Por otro lado, la implementación de un NAS se justifica como una extensión natural de la mejora de la infraestructura de red que beneficia a la comunidad académica y administrativa, permitiendo el almacenamiento de información, compartir archivos, vídeos, fotos y acceso a servicios de red adicionales como un media center.

Por todo lo anterior, el diseño e implementación de un portal cautivo con NAS incorporado en el Instituto Superior Tecnológico Sudamericano de Quito se justifica como un paso crucial hacia el fortalecimiento de las capacidades tecnológicas y educativas de la institución, y establece un precedente valioso para futuras iniciativas de mejora en la infraestructura de red, inclusive para otras sedes u otras organizaciones educativas.

3. Antecedentes

El Instituto Superior Tecnológico Sudamericano de Quito ha ofrecido históricamente acceso a Internet como parte de sus servicios educativos, fomentando una infraestructura que respalda la conectividad para el aprendizaje y la administración académica. No obstante, con el paso del tiempo y la creciente adopción de tecnologías móviles, la institución ha enfrentado desafíos significativos relacionados con la congestión de la red, afectando la calidad de la conexión a Internet para los usuarios legítimos y cumplidores de sus responsabilidades económicas.

El análisis de la situación reveló que la causa principal del problema residía en el uso compartido de una única contraseña de wifi, la cual era ampliamente conocida debido a su difusión en el campus. Esta práctica resultaba en una saturación de la red, puesto que no había restricciones ni control sobre quién accedía a la red ni sobre el uso que se le daba. Como resultado, se vio la necesidad de implementar un mecanismo que permitiera un manejo más eficiente y seguro del acceso a Internet.

Para enfrentar esta problemática, el proyecto propuso la creación de un portal cautivo, buscando mejorar la administración del acceso a la red y garantizar un servicio estable y confiable. Este portal limitaría el acceso a los estudiantes activos y autorizados mediante la generación de váuchers únicos, asegurando que solo los miembros de la comunidad educativa al día con sus pagos pudieran disfrutar de este servicio. El sistema de váuchers sería administrado a través de un servidor dedicado, operando con software gratuito y diseñado para emitir váuchers con o sin restricciones de tiempo, priorizando el acceso a la plataforma estudiantil (aula virtual).

La transición hacia un portal cautivo refleja un esfuerzo por parte del Instituto para abordar las deficiencias de una política de acceso abierto y sin restricciones, que históricamente había llevado a un uso ineficiente de los recursos de la red. Además, se consideró la implementación de un Sistema de Almacenamiento en Red (NAS) para fortalecer la gestión de la información y compartir recursos dentro de la red LAN del Instituto, proporcionando así una solución integral que mejora la infraestructura tecnológica y el manejo de la red para responder a las necesidades actuales y futuras de la comunidad académica.

La decisión de avanzar hacia un portal cautivo y la integración de un NAS demuestra un compromiso con la mejora continua y la adaptación a las nuevas exigencias de la era digital, sentando las bases para una experiencia educativa mejorada y más segura para todos los miembros del Instituto Superior Tecnológico Sudamericano de Quito.

4. Objetivos

4.1. Objetivo General

Diseñar e implementar un portal cautivo en el edificio matriz del Instituto Superior Tecnológico Sudamericano Quito para mejorar la gestión y seguridad del acceso a la red Wifi.

4.2. Objetivos Específicos

1. Realizar una revisión bibliográfica de las tecnologías y marcos teóricos relacionados con portales cautivos para fundamentar el diseño del sistema.
2. Evaluar y optimizar la infraestructura actual de la red de computadoras del edificio matriz, asegurando su compatibilidad con la implementación del portal cautivo y la configuración de puntos de acceso Wifi (hotspots).
3. Diseñar y configurar una red de área local virtual (VLAN) en los equipos existentes para segmentar el tráfico de la red y mejorar la seguridad y eficiencia de la red interna.
4. Seleccionar, instalar y configurar el software apropiado para gestionar el portal cautivo, basándose en criterios de seguridad, estabilidad y compatibilidad.
5. Desarrollar un sistema de distribución de váuchers que asegure un acceso restringido y monitoreado a la red Wifi, reservado para los miembros autorizados de la comunidad institucional.
6. Implementar un Sistema de Almacenamiento en Red (NAS) que soporte la centralización y el acceso seguro a los archivos y recursos compartidos de la institución exclusivamente por la red LAN.
7. Realizar pruebas de funcionamiento para verificar la efectividad del portal cautivo, ajustando la configuración según sea necesario para cumplir con los funcionamientos esperados.

5. Marco Teórico

5.1. Redes de computadoras

(Equipo editorial, Etecé, 2021)

Los sistemas interconectados aseguran una buena comunicación e intercambio de información entre los dispositivos informáticos, incluyendo computadoras, servidores, impresoras, enrutadores y dispositivos móviles. Estas redes facilitan el acceso y el uso compartido de recursos como archivos, aplicaciones, datos y servicios dentro de una organización o mediante conexiones remotas. La red de información conecta diferentes y múltiples sistemas informáticos utilizando diversos equipos de telecomunicaciones y medios físicos. Su función principal es compartir información en paquetes de datos que se transmiten con la asistencia de impulsos eléctricos y ondas electromagnéticas.

En la siguiente figura 1 tenemos una idealización de una red de computadoras que, si hay varias computadoras en la red, es posible que ellas establezcan comunicación entre ellas y también realicen la función de compartir el punto de acceso a Internet o la gestión de dispositivos periféricos. También se le permite a él que los archivos de datos se envíen rápidamente sin utilizar dispositivos de almacenamiento secundarios como discos.

Figura 1. Idealización de una red de computadoras.
Fuente: (Equipo editorial, Etecé, 2021)

5.1.1 Función de una red de computadoras

Las redes informáticas permiten a las personas compartir recursos de forma remota, lo que aumenta la velocidad de transmisión de datos. El acceso a un archivo a través de una red es más rápido que a través de Internet. Las opciones para conectar computadoras incluyen el cable coaxial, que transmite datos a través de dos conductores concéntricos (tiene un conductor interno rodeado por un conductor externo); el cable de par trenzado, que entrelaza los conductores concéntricos para reducir la interferencia; y la fibra óptica, que transmite datos a través de un cable extremadamente fino. En la transmisión, se utilizan pulsos de luz para transportar los datos. (Pérez Porto, 2011)

La figura siguiente muestra un esquema genérico de la conexión típica en un sistema de red:

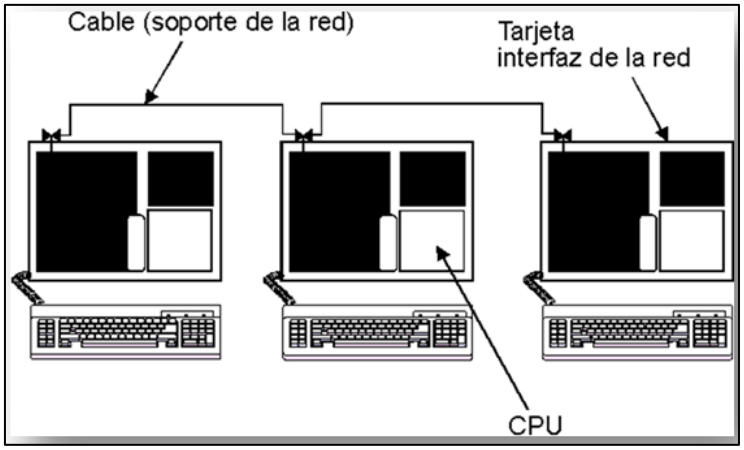


Figura 2. Esquema de conexión típico de un sistema en red.
Fuente: (profesores, s.f.)

5.1.2 Componentes de una red

Para una correcta conexión de una red de computadoras, es necesario que haya una buena comunicación entre el hardware, que incluye todas las computadoras, impresoras, celulares, etc. (conocidos como equipos finales), que ellos incluyen a las tarjetas de interfaz de red, así como también se tiene como componentes de red a los routers y switches (conocidos como equipos intermedios), sin olvidar a los cables que los conectan. Además, se debe considerar al software,

quien abarca a todos los controladores, es decir, son los programas que se utilizarán para gestionar los dispositivos; y, por último, el sistema operativo de la red encargado de administrarla. (profesores, s.f.)

Los componentes básicos y habituales que conforman una red, se las presenta en la figura 3 y son los siguientes:

1. El servidor.
2. Las estaciones de trabajo.
3. Las placas de interfaz de red (NIC).
4. Los recursos periféricos y compartidos.

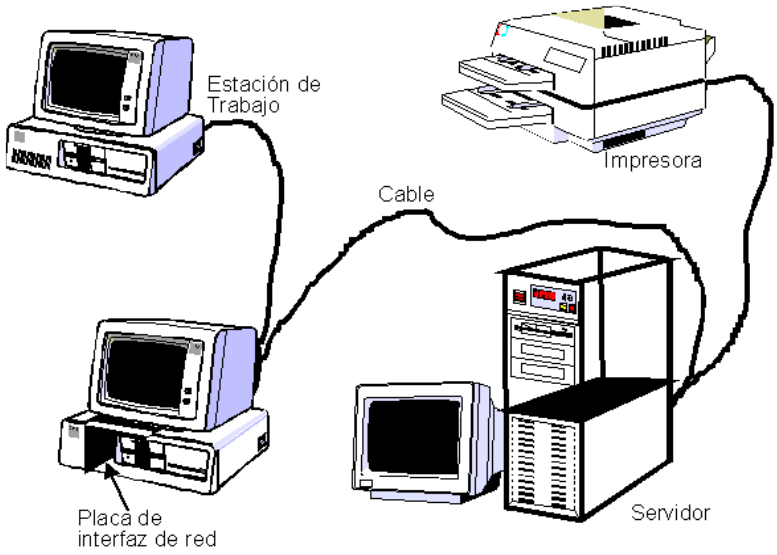


Figura 3. Componentes habituales de una red.
Fuente: (profesores, s.f.)

5.1.3 Equipos y servicios en una red de computadoras

Los equipos y servicios de red son un conjunto de hardware y software que están conectados física o inalámbricamente entre sí y se encargan de transmitir y recibir datos a través de impulsos eléctricos u ondas electromagnéticas para transportar datos. Por lo general, ofrecen algunos servicios únicos y comparten recursos e información. Estas redes se desarrollaron para

aumentar la velocidad de transmisión de datos y, al mismo tiempo, permitir el intercambio de información remota, confiable y segura. (Hernández, s.f.)

Servidores

Es una herramienta informática que proporciona, distribuye y almacena información. Los servidores operan bajo una arquitectura "cliente-servidor". Un programa informático o de software que depende del servidor para su funcionamiento se denomina cliente. Siempre que el cliente esté autorizado, un servidor proporcionará la información solicitada por el cliente. Los servidores físicos o virtuales están disponibles. (ticportal, 2022)

Router

Los enrutadores usan paquetes, que pueden contener una variedad de tipos de datos, incluidos archivos, comunicaciones y transmisiones sencillas, como interacciones web, para dirigir y guiar los datos de la red. (CISCO, 2021)

Una de las capas o secciones de un paquete de datos, que se compone de varios componentes como el remitente, el tipo de datos, el tamaño y, lo que es más importante, la dirección IP (Protocolo de Internet) de destino, contiene información de identificación. El enrutador selecciona la mejor ruta para cada transmisión después de priorizar los datos y leer esta capa. (CISCO, 2021)

Switch

Un conmutador o switch es una herramienta que se utiliza para conectar diferentes componentes de la red. Cualquier dispositivo con una tarjeta Ethernet o Wifi califica, incluida una computadora, una impresora, un televisor, una consola de juegos y otros. Los interruptores

se utilizan tanto en entornos residenciales como comerciales, donde es típico tener al menos un interruptor por piso, y permitir la interconexión de varios equipos. (Sanchez, s.f.)

Aunque la complejidad de estos dispositivos aumenta debido a los avances tecnológicos, su funcionalidad fundamental no ha cambiado. En esencia, cuando un dispositivo transmite un mensaje, el conmutador se encarga de retransmitirlo únicamente a través de la salida donde se encuentra el destinatario previsto. (Sanchez, s.f.)

El conmutador utiliza la dirección MAC de la tarjeta de red, también conocida como dirección física, para realizar esta tarea. En el caso de que haya varios conmutadores conectados, dependerá de ellos comunicarse de manera efectiva para determinar dónde se deben enviar los datos. Por tanto, es una herramienta pensada para facilitar la comunicación en equipo. (Sanchez, s.f.)

La siguiente figura muestra un esquema de la función de un switch:

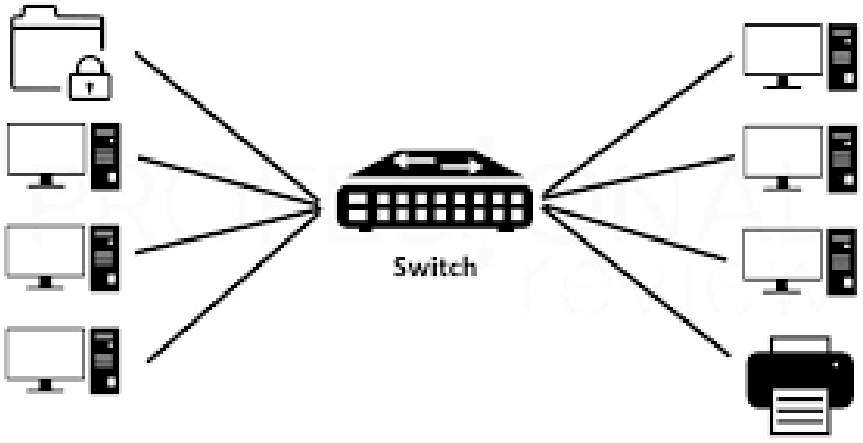


Figura 4. Esquema de un Switch.
Fuente: (Antonio, s.f.)

Access Point (Punto de Acceso)

Los dispositivos llamados puntos de acceso permiten la conexión inalámbrica de dispositivos a la red local. Sirven como puente entre la infraestructura de red cableada y los dispositivos inalámbricos, lo que permite la conectividad Wifi en la red local. (ordenadores-y-portatiles, 2020)

Un punto de acceso, también conocido como AP, es un componente de red inalámbrica que permite que los dispositivos se unan a una LAN a través de conexiones Wifi. Al proporcionar acceso inalámbrico a la red, funciona como un puente entre los dispositivos inalámbricos y la red cableada. (ordenadores-y-portatiles, 2020)

Tanto un transmisor como un receptor de señales inalámbricas, el punto de acceso realiza estas funciones. Los dispositivos le envían señales Wifi, y él las recibe y las transmite a través de la red cableada. Esto hace posible que dispositivos como computadoras portátiles, teléfonos móviles, tabletas y otros dispositivos habilitados para Wifi se unan a la red local y utilicen recursos compartidos como Internet, impresoras, servidores y otros dispositivos conectados a la red. (ordenadores-y-portatiles, 2020)

Los puntos de acceso suelen tener una conexión por cable a un enrutador o conmutador, lo que les permite expandir la cobertura de la red y ofrecer conectividad inalámbrica en áreas más grandes. Algunos puntos de acceso también pueden servir como enrutadores, combinando las capacidades de los dos dispositivos en uno. (ordenadores-y-portatiles, 2020)

Para evitar el acceso no autorizado a la red inalámbrica, los puntos de acceso se pueden configurar con varios niveles de seguridad, incluida la autenticación del usuario y el cifrado de datos (como WPA2 o WPA3). (ordenadores-y-portatiles, 2020)

Un punto de acceso es un dispositivo que, en resumen, permite que los dispositivos inalámbricos se conecten y accedan a una red local a través de conexiones Wifi. Proporciona conectividad inalámbrica y amplía la cobertura de la red en un área específica, sirviendo como puente entre los dispositivos cableados e inalámbricos. (ordenadores-y-portatiles, 2020)

La siguiente figura muestra un router con switch y access point:

Figura 5. Equipo Router Home con Punto de Acceso inalámbrico incluido.
Fuente: (ordenadores-y-portatiles, 2020)

Tarjetas Ethernet

Una tarjeta de red es un componente que permite la conexión de varios dispositivos entre sí y, a través de esta conexión, facilita el intercambio y la transmisión de datos e información de un dispositivo a otro. En informática, las tarjetas de red son comúnmente utilizadas. (Bembibre., 2009)

Es posible una tarjeta de red externa o interna, también conocida como adaptador de red. Es decir, se puede insertar en la placa base, pero también es posible utilizar las ranuras correspondientes para conectar una tarjeta de red a una computadora externa. Estas tarjetas son un hardware muy práctico porque les permiten a los usuarios realizar varias conexiones (permanentes o temporales) entre una o más computadoras, simplificando así el uso, la transferencia y el acceso a datos cruciales. (Bembibre., 2009)

La siguiente figura muestra la típica tarjeta de red Ethernet de conexión interna para PC de 10/100/1000 Mbps para slot PCIe - x16:

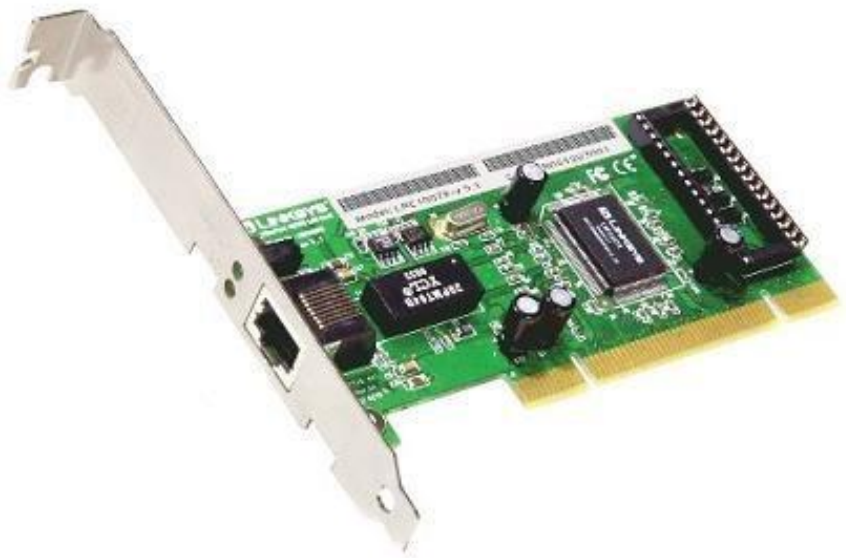


Figura 6. Tarjeta de red o network interface controller (NIC).
Fuente: (Bembibre., 2009)

Tarjetas Wifi

Este tipo de tarjeta, de conexión interna como se muestra en la figura 5 y que puede ser de conexión externa vía USB, permite conexiones inalámbricas, lo cual es una ventaja para las oficinas y una forma de aumentar la productividad en una empresa. Estos dispositivos se pueden conectar a su ordenador tanto internamente, mediante tarjetas convencionales que ofrecen una alta cobertura, como externamente, lo cual es ideal para profesionales y posible con puertos USB. (Plieshakov, 2023)

Figura 7. Tarjeta de red inalámbrica (wireless), conocida también como tarjeta de Wifi.
Fuente: (Plieshakov, 2023)

Tarjeta de Fibra

Esta tarjeta de comunicación como se muestra en la figura 6, tiene la habilidad de enviar y recibir datos a través de redes de área local comúnmente conocidas como "LAN" (redes de computadoras interconectadas cercanas) mediante fibra óptica, se monta en el gabinete después de ser insertada en las ranuras de expansión, también denominadas "Ranuras," que están integradas en la placa principal o "Placa base," con el fin de prevenir movimientos y fallos

subsiguientes. Todas las tarjetas de red óptica incluyen uno o más puertos para llevar a cabo la conexión de los cables de fibra óptica. (informaticamoderna, s.f.)

Figura 8. Tarjeta para red óptica.
Fuente: (informaticamoderna, s.f.)

Sistema de cableado

El cable de par trenzado se ha vuelto cada vez más común, aunque el cable coaxial fue uno de los primeros en usarse. Aún son posibles velocidades de transmisión más rápidas a través del cable coaxial o de par trenzado gracias a los avances en el diseño de tarjetas de interfaz de red, pero aún se prefiere el cable de fibra óptica cuando la velocidad es crucial. Hoy en día, cuando se requiere una transferencia de datos de alta velocidad, el cable de fibra óptica sigue siendo la mejor opción. (profesores, s.f.)

Cable

La infraestructura requerida para conectar equipos informáticos y permitir que los datos se muevan a través de una red se denomina cableado de red. El tamaño y el tipo de red determinan los distintos tipos de cables. (aurum-informatica, 2021)

Conectores

Un conector es un componente mecánico que sirve como elemento de conexión entre un cable de computadora y el aparato que necesita ser conectado o entre un cable y un adaptador. (microinformatica.jimdofree, s.f.)

Patch Panels y Gabinetes de Cableado

Mantener el centro de datos o sala de servidores organizados y simplificar el traslado, la adición o la modificación de su infraestructura de cableado en el futuro son objetivos que un panel de conexiones, un dispositivo de red confiable y adaptable busca alcanzar. (John, 2021)

Seguridad de la red

La protección de todos los recursos informáticos contra errores y ataques a su integridad, confidencialidad y disponibilidad se conoce como seguridad de red. En esto se incluyen programas antimalware, cortafuegos, sistemas de detección de intrusos, herramientas de prevención de pérdida de datos y otras medidas de seguridad. (trendmicro, 2023)

5.2. Tipos de topología de red

5.2.1. Topología de red estrella

Este es el tipo de configuración más común. Como se muestra en la figura 7, los nodos de red se configuran conectándolos a un dispositivo central (hub) que actúa como servidor. Un concentrador gestiona la transmisión de datos a través de la red. Es decir, todos los datos transmitidos por la red pasan por un dispositivo central hasta llegar a su destino. (internationalit, 2021)

La siguiente imagen muestra un esquema de la topología de red en estrella:

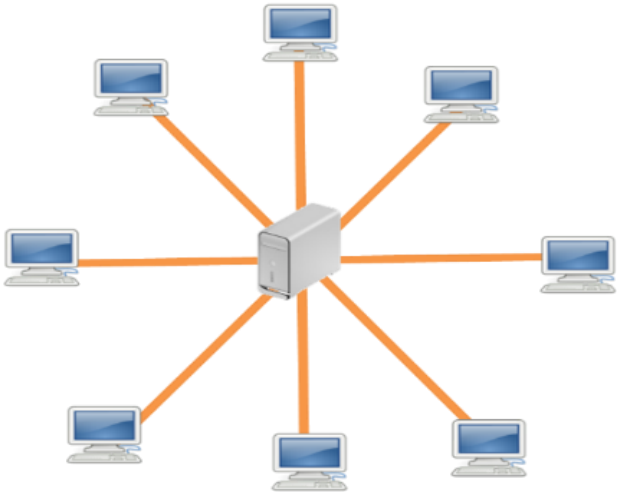


Figura 9. Ejemplo de una topología de red en estrella.
Fuente: (wordpress, 2017)

5.2.2. Topología de red bus

Dirige los dispositivos a lo largo de un solo cable que conecta los dos extremos de la red, y esta topología se conoce también como topología de red troncal, bus o línea. A medida que el cable se desplaza hacia su destino, los datos fluirán a lo largo de él. (internationalit, 2021)

La siguiente figura muestra un esquema de la topología de red en bus:

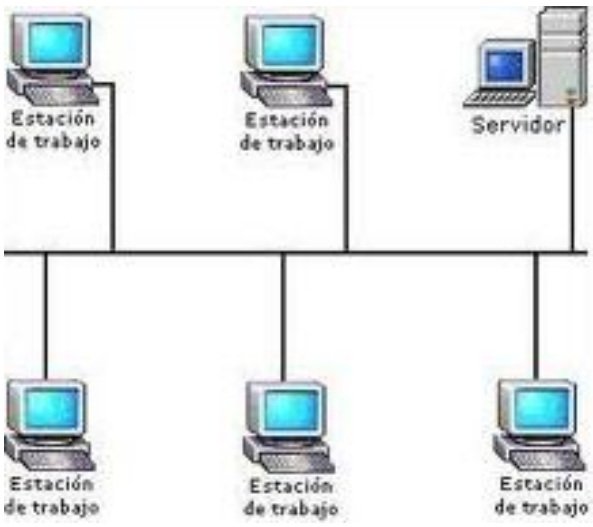


Figura 10. Ejemplo de una topología de red en bus.
Fuente: (jimdofree, s.f.)

5.2.3. Topología de red anillo

Los nodos están conectados en una configuración circular. El anillo actúa como un conducto para los datos que pasan por cada dispositivo. Para evitar la pérdida de paquetes durante la transmisión en una red grande, es posible que se requieran repetidores. Para permitir que el tráfico fluya en ambas direcciones simultáneamente, las topologías de anillo se pueden configurar como anillos simples (semidúplex) o anillos dobles (dúplex completo). (internationalit, 2021)

La siguiente ilustración muestra un esquema de la topología de red en anillo:

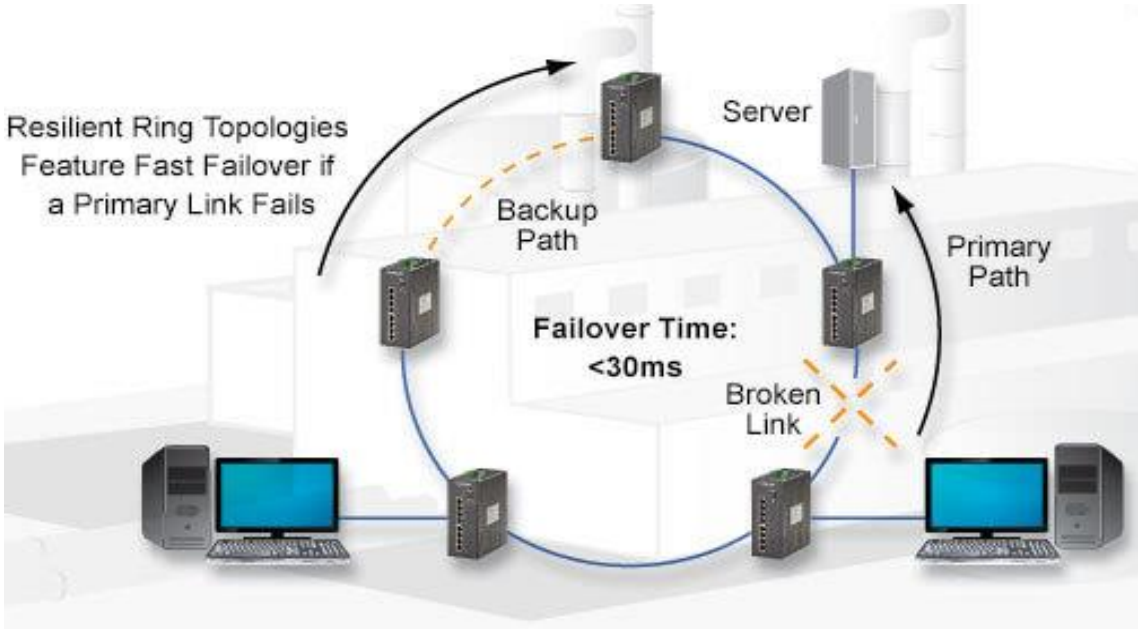


Figura 11. Ejemplo de una topología de red en anillo.
Fuente: (blackbox, s.f.)

5.2.4. Topología de red malla

Todos los dispositivos en la red están conectados directamente en modos de malla completa. La mayoría de los dispositivos se conectan directamente en una topología de malla parcial. Esto proporciona opciones de entrega de datos. Se utiliza la distancia de transmisión más corta para enviar datos. (internationalit, 2021)

La siguiente figura muestra un esquema de la topología de red en malla:

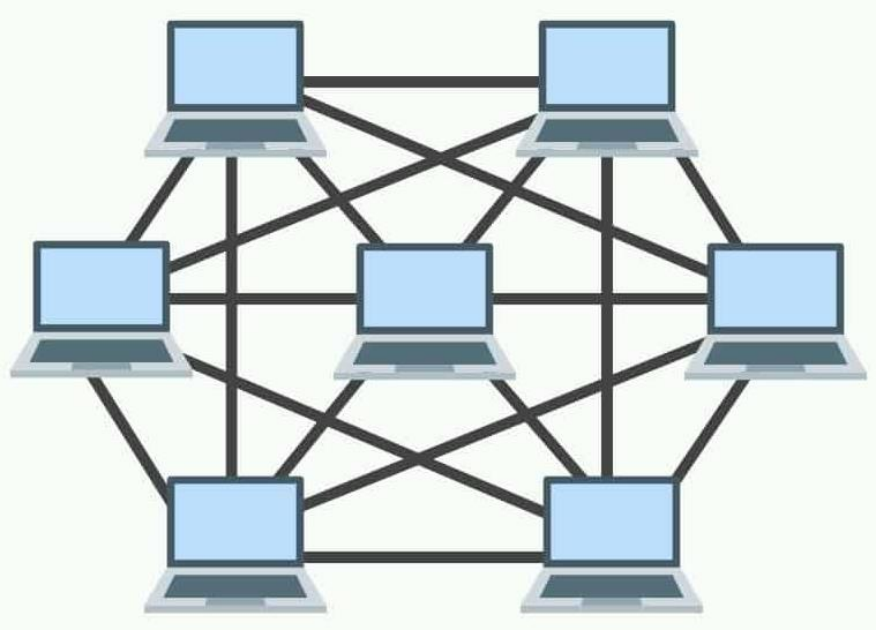


Figura 12. Ejemplo de una topología de red en malla.
Fuente: (Bhatti, 2022)

5.3. Tipos de redes

5.3.1. Red de área personal (PAN)

Este es un tipo de red informática básica: una red PAN consta de un módem y puede incluir una o dos computadoras, teléfonos, impresoras, tabletas, etc. Por lo tanto, es una red que conecta varios dispositivos electrónicos en un área pequeña y directa. La PAN es una red que suele estar presente en pequeñas oficinas o casas particulares. Estas redes son gestionadas por una sola persona o empresa desde una única unidad. (tokioschool, 2023)

Las redes diseñadas para conectar dispositivos personales cercanos, como teléfonos móviles, tabletas, computadoras portátiles y dispositivos periféricos, son conocidas como redes PAN. El Bluetooth o Wi-Fi siguen siendo unas de las tecnologías comúnmente utilizada para establecer conexiones PAN. (tokioschool, 2023)

La siguiente figura muestra un esquema de una red PAN:

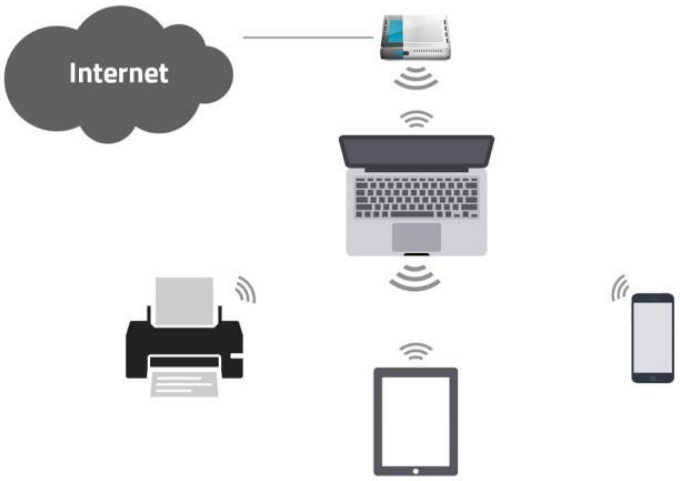


Figura 13. Diagrama representativo de una Red PAN.
Fuente: (conceptoabc, 2021)

Características

Cubren una extensión desde unos centímetros a unos pocos metros, promedio de 10 metros. Por estar usualmente compuesta de unos pocos dispositivos en una corta distancia, suelen ser muy eficientes. (conceptoabc, 2021)

5.3.2. Red de área local (LAN)

Se trata de un tipo de red ampliamente utilizado que conecta un grupo de computadoras o dispositivos ubicados en la misma habitación para compartir información y recursos. (tokioschool, 2023)

Es una red de área local en la que se pueden conectar varios dispositivos ubicados en la habitación. Si la conexión se establece entre más de dos dispositivos, se requieren componentes de red para estabilizar y garantizar una buena conexión de red LAN. (tokioschool, 2023)

Las redes LAN casi siempre emplean Ethernet, Wifi o ambos para conectar los dispositivos de la red. Ethernet es un protocolo de conexión física a la red que requiere el uso de cables Ethernet. Wifi, por otro lado, es un protocolo utilizado para la conexión a una red a través de ondas de radio. (cloudflare.com, 2023)

Una variedad de dispositivos puede conectarse a las LAN, incluyendo servidores, ordenadores de escritorio, portátiles, impresoras, dispositivos IoT e incluso videoconsolas. En las oficinas, las LAN suelen ser utilizadas para proporcionar acceso compartido a los empleados internos a las impresoras o servidores conectados. (cloudflare.com, 2023)

La siguiente ilustración muestra una idealización de una red LAN:

Figura 14. Diagrama representativo de una red LAN.
Fuente: (concepto.de, 2023)

5.3.3. Red de área local inalámbrica (WLAN)

WLAN actúa como una LAN, utilizando tecnologías de redes inalámbricas como Wifi. Básicamente, es lo mismo que una LAN, excepto que proporciona una conexión de red inalámbrica. (tokioschool, 2023)

Su propósito general es el mismo que el de una LAN, con la única diferencia de que una conexión WLAN a una red no requiere el uso de cables físicos. Además, facilita la conexión de múltiples dispositivos sin necesidad de componentes adicionales, ya que las redes Wifi funcionan conectando dispositivos entre sí mediante tecnología inalámbrica. (tokioschool, 2023)

Como funciona las redes WLAN

Una WLAN opera utilizando tecnología inalámbrica para conectar dispositivos. Los dispositivos se conectan a puntos de acceso inalámbrico (WAP) que transmiten señales de radio, lo que permite que los dispositivos se conecten y se comuniquen entre sí. Las conexiones inalámbricas en una WLAN son establecidas a través de una técnica conocida como modulación de amplitud en cuadratura (QAM), la cual se emplea para transmitir datos mediante ondas de radio. (redesinformaticas, s.f.)

Los puntos de acceso (WAP) y los dispositivos utilizan protocolos de red para la comunicación y coordinación de la actividad de la red, como el Protocolo de Internet (IP). Una WLAN puede ser configurada de varias maneras, por ejemplo, una topología en estrella en la que todos los dispositivos están conectados directamente a la red WAP, o una topología en malla en la que los dispositivos pueden comunicarse directamente entre sí. (redesinformaticas, s.f.)

La siguiente figura muestra un esquema de una red WLAN:

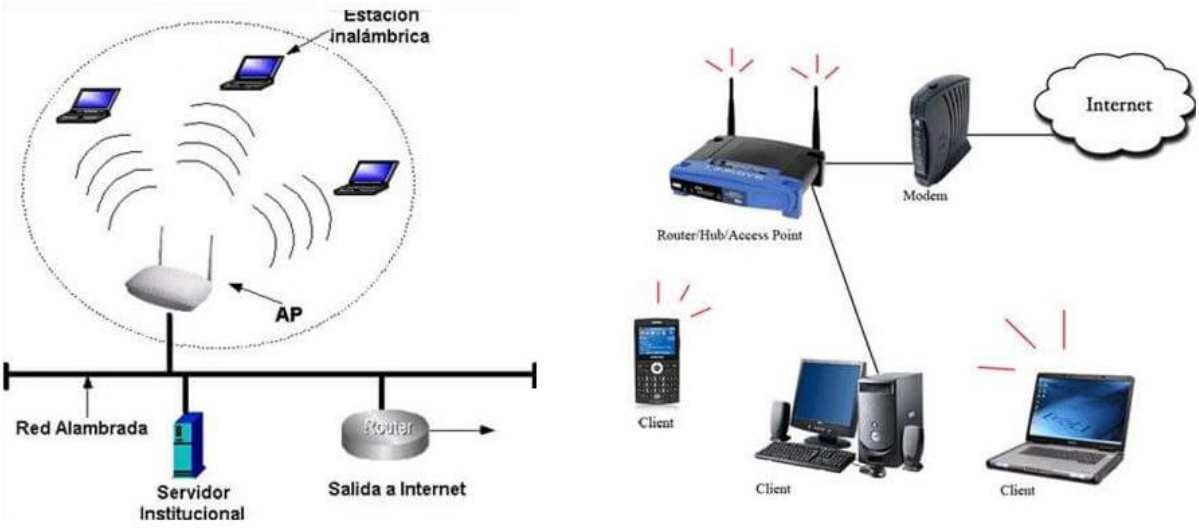


Figura 15. Diagrama representativo de una Red WLAN.
Fuente: (Rojas, 2023)

5.3.4. Red de área de campus (CAN)

Estos tipos de redes son más grandes que las LAN, pero más pequeñas que las que se analizan a continuación. A menudo, se encuentran en las universidades, lo que conduce a uno de los tipos de redes informáticas más comunes en el ámbito académico. (tokioschool, 2023)

Estas redes suelen estar ubicadas en varios edificios próximos entre sí, permitiendo a los usuarios compartir recursos. Además, se trata de una red de computadoras que generalmente está conectada públicamente a Internet. (tokioschool, 2023)

La siguiente ilustración muestra un esquema de una red CAN:

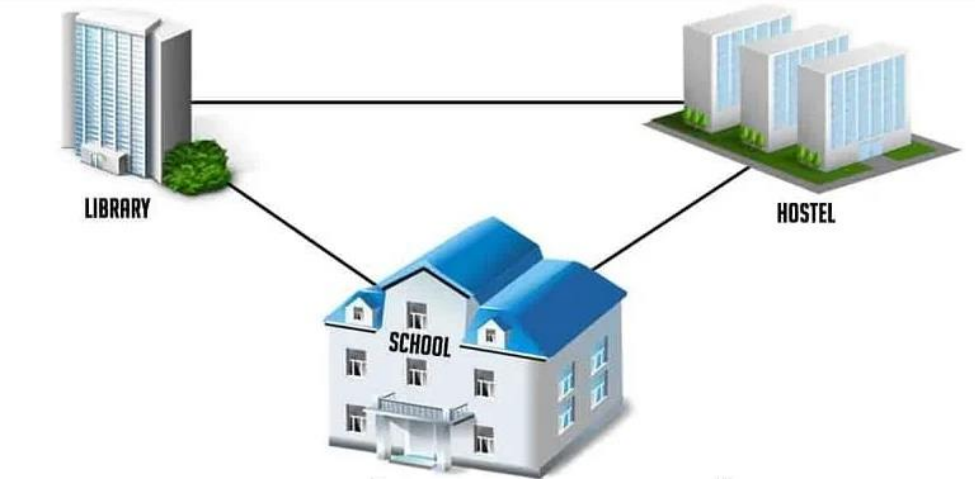


Figura 16. Diagrama representativo de una Red CAN.
Fuente: (Jariam, 2020)

5.3.5. Red de área metropolitana (MAN)

La red de área local (LAN) es más pequeña que la red de área metropolitana (MAN). La red MAN solo cubre el territorio de un país. En este caso, una red de área local (LAN) se conecta a otras redes LAN para crear una red de área más grande. Se puede obtener más información sobre qué es una red de área metropolitana. (Javired, 2020)

En un campus o en un área razonablemente grande, como una ciudad, se puede encontrar la Red de Área Metropolitana (MAN). Las redes de área metropolitana (MAN) son aquellas que suelen ser propiedad de varias empresas diferentes. (Javired, 2020)

La tecnología inalámbrica utilizada en una red de área metropolitana (MAN) es similar a la utilizada en una red de área local (LAN) en cuanto a sus ventajas e inconvenientes. Además de admitir datos de texto y voz, la Red de Área Metropolitana (MAN) también posee capacidades de conexiones de radio y televisión por cable. (Javired, 2020)

La siguiente figura muestra un esquema de una red MAN:

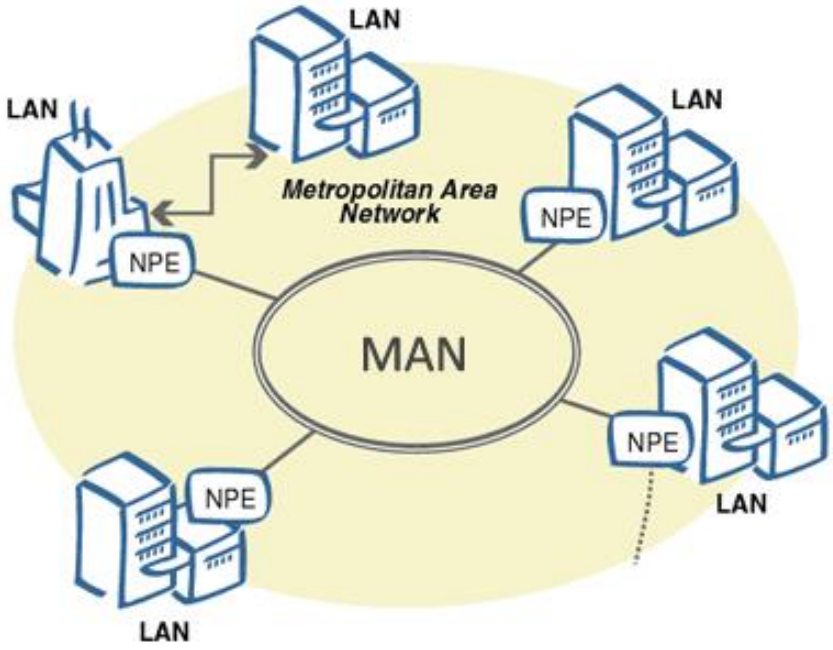


Figura 17. Diagrama representativo de una Red MAN.
Fuente: (wikipedia, 2023)

5.3.6. Red de área amplia (WAN)

Una WAN es una red que conecta computadoras que están ubicadas a una distancia física significativa. Permite que los dispositivos se conecten de forma remota a través de redes extensas y se comuniquen incluso cuando están a kilómetros de distancia. (tokioschool, 2023)

Internet es el ejemplo más simple de una WAN que conecta todos los dispositivos del mundo que pueden acceder a ella. Sin embargo, a nivel técnico, cualquier red que cubra un área geográfica amplia puede considerarse una WAN, incluso si su acceso es privado. Son redes que abarcan áreas geográficas extensas, como ciudades, países o incluso continentes. Las redes WAN se utilizan para interconectar LAN dispersas geográficamente. (tokioschool, 2023)

La siguiente imagen muestra un esquema de una red WAN:

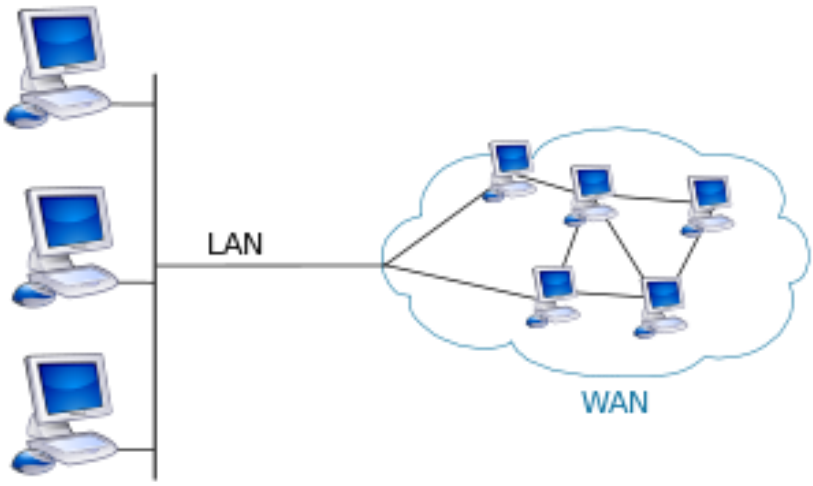


Figura 18. Diagrama representativo de una red WAN.
Fuente: (wikipedia, 2023)

5.3.7. Red de área de almacenamiento (SAN)

SAN es una red informática de alta velocidad que conecta grupos de dispositivos de almacenamiento compartido a varios servidores. Las redes tipo SAN generalmente se ensamblan con cables, adaptadores y conmutadores conectados a diferentes estructuras, como almacenamiento de datos y tipos de servidores. Cada elemento que conforma dicha red debe estar interconectado. (tokioschool, 2023)

La siguiente ilustración muestra una idealización de una red SAN:

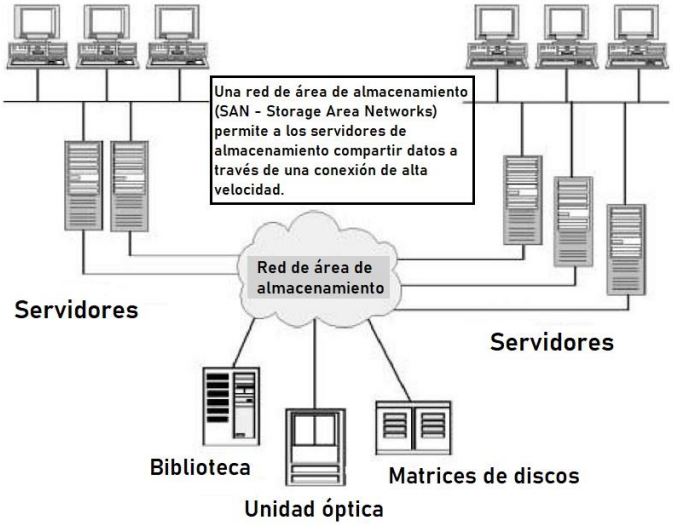


Figura 19. Diagrama representativo de una red SAN.
Fuente: (redesinformaticas, s.f.)

5.3.8. Red de área local óptica pasiva (POLAN)

Como alternativa a las LAN tradicionales basadas en conmutadores, la tecnología POLAN se integra en los cables con el propósito de resolver los problemas de compatibilidad con los protocolos Ethernet más antiguos. POLAN representa una arquitectura LAN de punto a multipunto que emplea divisores ópticos para multiplexar señales de hebras de fibra monomodo y distribuirlas a usuarios y dispositivos. (tokioschool, 2023)

La siguiente figura 18 muestra un esquema de la una red óptica pasiva (PON) es una red de fibra óptica para la transmisión y recepción bidireccional de datos; utiliza un transmisor principal y numerosos receptores finales, como se muestra en la siguiente ilustración. La ausencia de componentes activos, como un repetidor o divisor, entre el transmisor y el receptor se denomina pasiva. Estas redes utilizan fibra óptica; por lo tanto, se han creado dispositivos especiales para ellas. Por un lado, está el transmisor conocido como OLT (Optical Line Terminal); por otro, está el receptor conocido como ONT/ONU (Optical Network Unit). Ambos dispositivos permiten la conversión de señales ópticas en señales eléctricas y viceversa. (blog.incom, s.f.)

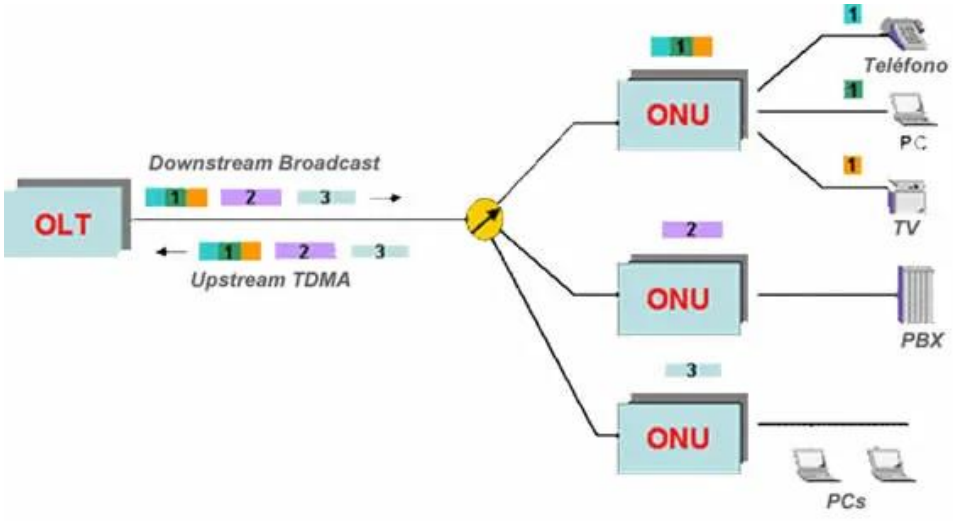


Figura 20. Diagrama representativo de una red POLAN.
Fuente: (Fortiz, 2013)

5.3.9. Red privada empresarial (EPN)

Estos tipos de redes están construidas y son propiedad de empresas que desean conectar de forma segura sus ubicaciones dispares para compartir recursos informáticos. De esta forma, se encuentran diferentes tipos de redes EPN, cada una con un uso específico. Cabe señalar que son creadas, mantenidas y proporcionadas por la propia empresa. Estos accesos pueden ser temporales para un propósito específico o permanentes si es necesario. (tokioschool, 2023)

Cada LAN de oficina está conectada a otras LAN a través de una WAN corporativa más amplia, generalmente construida utilizando enrutamiento de conmutación de etiquetas multiprotocolo (MPLS) dedicado. (cloudflare, s.f.)

La siguiente ilustración muestra un esquema de la red EPN:

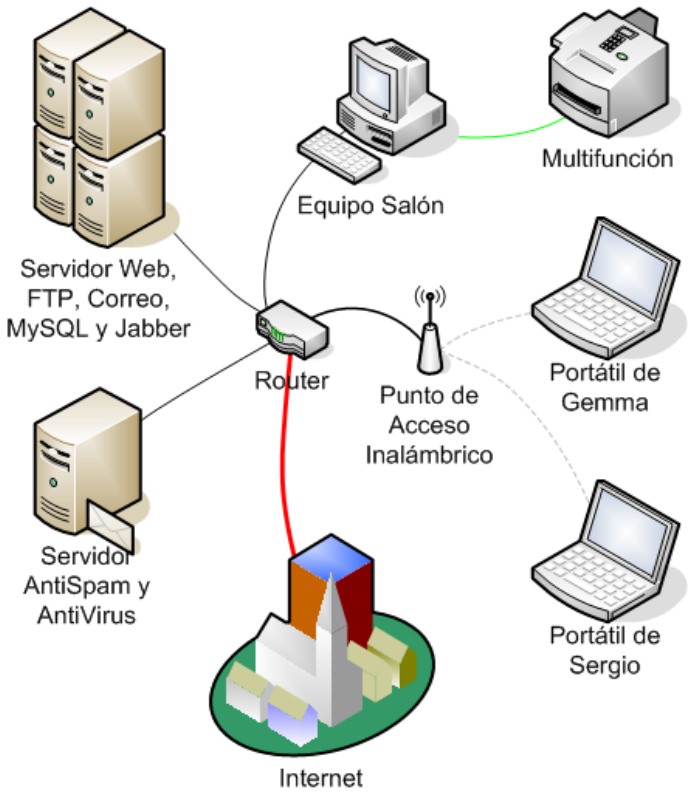


Figura 21. Diagrama representativo de una red EPN.
Fuente: (wikipedia, s.f.)

5.3.10. Red privada virtual (VPN)

Una VPN (red privada virtual) permite a los usuarios enviar y recibir datos como si sus dispositivos estuvieran conectados a una red privada, aunque no lo estén. De esta manera, los usuarios pueden acceder a la red privada de forma remota mediante una conexión virtual. Este tipo de red VPN les permite crear una red local sin que todos sus miembros se conecten directamente entre sí. Además, este tipo de conexión a la red permite el acceso a puntos de Internet que la propia conexión del usuario no puede alcanzar. (tokioschool, 2023)

La siguiente imagen muestra un esquema de una red VPN:

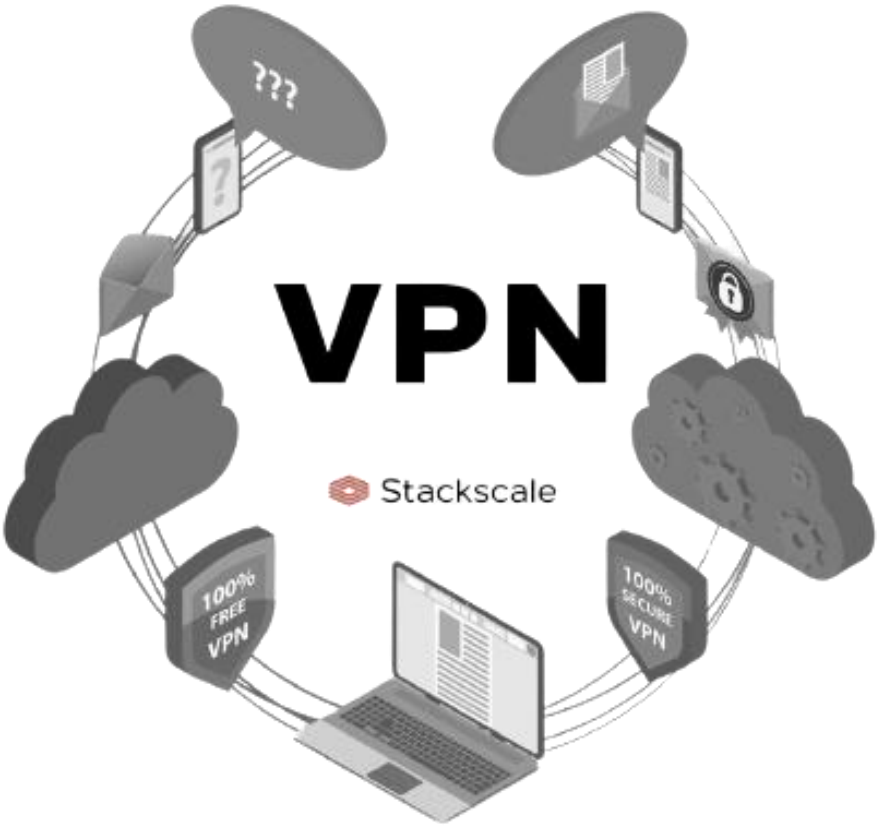


Figura 22. Diagrama representativo de una red VPN.
Fuente: (stackscale, 2023)

5.4. Redes inalámbricas

Una red inalámbrica es un sistema de comunicación que permite transferir datos entre dispositivos sin el uso de cables físicos. Se utilizan tecnologías de transmisión inalámbrica como ondas de radio, infrarrojos o señales de microondas para establecer conexiones y facilitar la comunicación y el intercambio de datos. (ConceptoABC, 2020)

Las redes inalámbricas son conexiones realizadas a través de ondas electromagnéticas que permiten la transmisión y recepción de datos sin necesidad de una conexión de cableado físico. (ConceptoABC, 2020)

Mientras se encuentran dentro del área de la red, esto permite que los dispositivos remotos se conecten rápidamente. Además, las redes inalámbricas permiten establecer la comunicación entre varios terminales sin necesidad de una conexión por cable. (ConceptoABC, 2020)

Las computadoras que son móviles se pueden conectar fácilmente mediante redes inalámbricas. Existen, a grandes rasgos, dos tipos de redes inalámbricas: redes de larga distancia y redes de corta distancia. Desde 1997, este fenómeno ha ido en aumento y es más frecuente que nunca, desde las conexiones Wifi hasta la transmisión de datos por Bluetooth. (ConceptoABC, 2020)

La siguiente figura muestra un esquema de una red inalámbrica:

Figura 23. Diagrama representativo de una red inalámbrica.
Fuente: (ConceptoABC, 2020)

5.4.1. Tipos de redes inalámbricas

Los tipos de redes inalámbricas son:

WPAN

WPAN significa red de área personal inalámbrica. Las redes inalámbricas de área personal son aquellas que tienen un alcance de hasta 10 metros. Estas se emplean con frecuencia para que los usuarios puedan conectar sus dispositivos personales a una red. (ConceptoABC, 2020)

WLAN

WLAN significa red de área local inalámbrica. Un tipo de red que puede abarcar hasta 100 metros es una red de área local inalámbrica. Se utilizan para crear una red más económica y evitar los costos asociados con una conexión por cable. Se implementan bajo protocolos wifi o bluetooth. (ConceptoABC, 2020)

WMAN

WMAN significa red de área metropolitana inalámbrica. El rango de cobertura de la red inalámbrica del área metropolitana suele ser de unos 50 km. Como era de esperar, estas redes están diseñadas para ofrecer cobertura dentro de áreas metropolitanas, como una colección de edificios del centro o cualquier área considerable (como un área rural o un campus universitario). (ConceptoABC, 2020)

WWAN

WWAN significa red inalámbrica de área amplia. Una red de área amplia inalámbrica proporciona un área de cobertura mayor que la de todas las demás redes inalámbricas. Los proveedores de telefonía móvil utilizan este tipo de red para conectar a sus clientes y ofrecer sus servicios. (ConceptoABC, 2020)

5.5. Wifi

Es una tecnología de telecomunicaciones que permite la interconexión inalámbrica entre la computadora y los sistemas electrónicos, como computadoras, consolas de videojuegos, televisores, teléfonos celulares, reproductores, punteros, etc., se conoce en informática como Wifi (derivado de la marca Wifi). Estos dispositivos pueden conectarse entre sí utilizando esta tecnología para intercambiar datos o pueden conectarse a un punto de acceso de red inalámbrica para acceder a Internet. Aunque una empresa que certifica los estándares de la tecnología que admite esta capacidad de conexión se identifica con la marca Wifi, el término "Wifi" se suele utilizar para referirse a esta última y no a la empresa. (Equipo editorial, Etecé., 2021)

Wi-Fi es una marca de la Alianza Wi-Fi, la organización comercial que cumple con los estándares 802.11 relacionados con redes inalámbricas de área local. Su primera denominación en inglés fue Wireless Ethernet Compatibility Alliance. (wikipedia, 2023)

Como resultado de la necesidad de estandarización y compatibilidad en los modelos de conexión inalámbrica de varios dispositivos digitales, surgió Wifi, superando otras formas de conexión incompatibles como Bluetooth, GPRS, UMTS, etc. Wifi, a diferencia de estos, transmite datos utilizando ondas de radio. (Equipo editorial, Etecé., 2021)

Esta tecnología está pensada para enlazar dispositivos en distancias cortas (100 metros como máximo), especialmente en situaciones donde hay mucho ruido de señal o interferencia, como cuando el espectro de radio está saturado por múltiples emisiones. También es más lenta que una conexión por cable, pero es mucho más flexible y cómoda. Debido a la probabilidad de que cualquier dispositivo que capte la señal tenga acceso al punto de emisión, este tipo de conexión también tiene un inconveniente de seguridad. Por lo general, se configura para lograr esto mediante el uso de contraseñas y otras medidas de seguridad, pero la posibilidad de una infracción cibernética siempre está presente. (Equipo editorial, Etecé., 2021)

5.6. IEEE 802.11

Para la capa física y la subcapa MAC de los enlaces inalámbricos, el estándar WLAN IEEE 802.11 especifica cómo se usa la RF en las bandas de frecuencia ISM sin licencia. (wikipedia, 2023)

Su objetivo es certificar que los productos Wifi se adhieren al conjunto de estándares inalámbricos 802.11 de IEEE. Sin embargo, en el mundo de la tecnología inalámbrica, el

término Wifi es sinónimo de acceso inalámbrico en general, con nombres como 802.11b y 802.11ac, estos estándares pertenecen a una familia de especificaciones que comenzó en la década de 1990 y todavía se está expandiendo. (Shaw, 2018)

La siguiente figura muestra un esquema de una arquitectura lógica funcional IEEE 802.11:

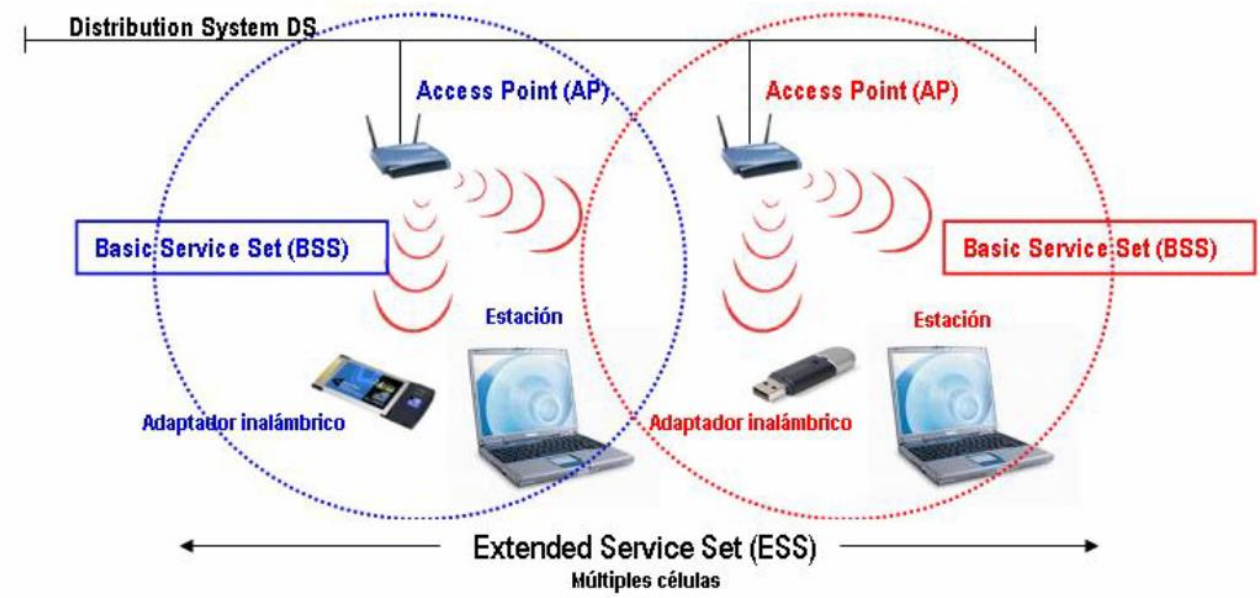


Figura 24. Diagrama representativo de una arquitectura lógica funcional IEEE 802.11. Fuente: (biblus, s.f.)

5.6.1. Tipos de redes IEEE 802.11

Se tienen los siguientes tipos de redes inalámbricas estandarizados por la IEEE:

IEEE 802.11a

Fue lanzado simultáneamente con el estándar 802.11b. Opera en la banda de frecuencia de 5 GHz y ofrece una velocidad máxima teórica de hasta 54 Mbps. Sin embargo, su alcance es más limitado en comparación con 802.11b. (Sossa, s.f.)

IEEE 802.11b

Fue uno de los primeros estándares en ser ampliamente adoptado. Opera en la banda de frecuencia de 2.4 GHz y ofrece una velocidad máxima teórica de hasta 11 Mbps. (Sossa, s.f.)

IEEE 802.11c

No hay interés para el público en general en este estándar combinado. Simplemente permite la combinación de dispositivos compatibles con 802.1d y 802.11 (a nivel de enlace de datos), modificando el estándar 802.1d. (Sossa, s.f.)

IEEE 802.11d

Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo móvil. (Sossa, s.f.)

IEEE 802.11e

A nivel de la capa de enlace de datos, se pretende aumentar la calidad del servicio. Para mejorar las transmisiones de audio y video, el estándar tiene como objetivo especificar los requisitos para varios paquetes en términos de ancho de banda y demora de transmisión. (Sossa, s.f.)

IEEE 802.11f

Es una sugerencia hecha a los proveedores de puntos de acceso que hace que los productos sean más compatibles. Independientemente de las marcas de puntos de acceso que se utilicen en la infraestructura de red, utiliza el protocolo IAPP para permitir que los usuarios itinerantes

cambien sin problemas de un punto de acceso a otro mientras están en movimiento. Otro nombre para esta cualidad es roaming. (Sossa, s.f.)

IEEE 802.11g

Esto supondría una mejora en la velocidad de transmisión y estaría motivado por 802.11b. Los hornos de microondas, los dispositivos Bluetooth y los teléfonos inalámbricos digitales son ejemplos de dispositivos que funcionan dentro de este rango, lo que con frecuencia provoca graves perturbaciones. Además, con frecuencia hay problemas con una alta densidad y cantidad de usuarios en las áreas urbanas. (Sossa, s.f.)

IEEE 802.11h

Su objetivo es armonizar el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la h en 802.11h) y adherirse a las leyes europeas que rigen el uso de frecuencia y la eficiencia energética. Para la regulación europea, sucede. (Sossa, s.f.)

IEEE 802.11i

Quieren mejorar la seguridad de la transferencia de datos administrando claves, dispersándolas y poniendo en práctica el cifrado y la autenticación. Este estándar, que se basa en AES (Advanced Encryption Standard), puede cifrar transmisiones realizadas con las tecnologías 802.11a, 802.11b y 802.11g. (Sossa, s.f.)

IEEE 802.11j

Dado que pueden cumplir con sus regulaciones para la operación de radio para aplicaciones interiores, exteriores y móviles, es para la regulación japonesa porque fue creado para el mercado japonés. (Sossa, s.f.)

IEEE 802.11k

Este permite que los conmutadores y AP inalámbricos puedan calcular y valorar recursos de radiofrecuencia para WLAN con el fin de que sea mejor su función, es por software por lo que solo es instalar y actualizar desde el equipo, es compatible para varios sectores. (Sossa, s.f.)

IEEE 802.11n

Con un aumento de la velocidad de transmisión máxima de 54 Mbps a un máximo de 600 Mbps, esta versión, que es bastante independiente de lo que sucedería con sus otras versiones (802.11b y 802.11g), brinda un mejor rendimiento de la red; aunque los resultados reales pueden variar según el entorno. (Sossa, s.f.)

IEEE 80.11m

El objetivo de este estándar es proporcionar mantenimiento editorial, correcciones, mejoras, aclaraciones e interpretaciones pertinentes a la documentación de las especificaciones de la familia 802.11. Esto se conoce como "limpieza del hogar 802.11". (Sossa, s.f.)

IEEE 802.11p

La tecnología de corto alcance (DSRC) se utiliza para transmitir frecuencias de 5,90 GHz y 6,20 GHz en lo que sería ideal para automóviles, lo que permite el intercambio de datos de vehículos y automóviles mientras se conduce. En este caso, se puede agregar WAVE (acceso inalámbrico en entornos vehiculares), un sistema de comunicación vehicular. (Sossa, s.f.)

IEEE 802.11r

Fast Basic Service Set Transition es lo que se llama, y es la transición rápida de conjuntos de servicios básicos lo que permite que la red establezca protocolos de seguridad y pueda

administrarlos. Esto es crucial para el sistema de datos inalámbrico porque cuando se encuentra un dispositivo en un AP, puede identificar cuándo lo abandona y lo visita. (Sossa, s.f.)

IEEE 802.1q

El grupo de trabajo IEEE 802 desarrolló el protocolo .1Q, también conocido como protocolo IEEE 802.1Q, como un proyecto para crear un mecanismo que permita que múltiples redes compartan de manera transparente el mismo medio físico sin encontrar problemas de interferencia (Trunking). Como el nombre del estándar creado como parte de este proyecto, también se usa para describir el protocolo de encapsulación que usan las redes Ethernet para implementar este mecanismo. Todos los dispositivos de interconexión que admiten VLAN deben cumplir el estándar IEEE 802.1Q, que describe con gran detalle el funcionamiento y la gestión de redes virtuales. La función principal del estándar 802.1Q es permitir la segmentación y etiquetado del tráfico de red en redes Ethernet mediante el uso de VLAN (Virtual LAN). (wikiwand, s.f.)

IEEE 802.11s

Por sí solo, esto permite que los dispositivos inalámbricos se conecten entre sí y creen una red de malla WLAN para el uso de topologías fijas; en este caso, los teléfonos móviles no entrarían. (Sossa, s.f.)

IEEE 802.11v

Es para la configuración remota de dispositivos que las centrales telefónicas utilizan la capa de enlace de datos para monitorear, configurar y actualizar la capacidad de la red de los usuarios que están afiliados a la central. (Sossa, s.f.)

IEEE 802.11w

Es un protocolo basado en 802.11i diseñado para defender las redes WLAN de los ataques suaves en los marcos de gestión inalámbrica, que son vulnerables a los ataques cuando se envían. Al hacer esto, ayuda a defenderse contra ataques maliciosos. Interactúa con IEEE 802.11r e IEEE 802.11u. (Sossa, s.f.)

IEEE 802.11u

Facilita el descubrimiento de redes apropiadas anunciando el tipo de red de acceso (red privada, red pública libre, red pública libre). Además, tiene un protocolo de consulta de red de acceso y da una respuesta que es utilizada por un dispositivo móvil para descubrir una variedad de información, incluido el nombre de dominio del operador del punto de acceso. (Sossa, s.f.)

IEEE 802.11ac

Por su banda de 5 GHz, las aplicaciones de este estándar para los equipos que se implementen con él y su alto rendimiento para redes de área local (WLAN), es ventajoso para el público en general porque ofrece un servicio mucho más interesante, el HD a quienes están logueados en la red, entre otras ventajas. (Sossa, s.f.)

IEEE 802.11ad

Este estándar se caracteriza por la alta frecuencia, lo que le permite usar más ancho de banda; esto, a su vez, permite la transmisión de datos a altas velocidades de hasta varios gigabits por segundo, permitiendo su uso como transmisión de video UHD sin comprimir a través de una red inalámbrica. (Sossa, s.f.)

IEEE 802.11ah

También se conoce como Wifi HaLow y, aunque su alcance es mayor que el promedio, utiliza menos energía eléctrica que Bluetooth. Wifi HaLow también permite el desarrollo de redes considerables de estaciones o sensores que trabajan juntos para compartir señales. (Sossa, s.f.)

IEEE 802.11ax

Esta es una de las versiones más recientes que se está implementando gradualmente y está hecha para operar en todas las bandas ISM entre 1 y 6 GHz. Esto ayudaría a que los equipos de servicio inalámbrico tuvieran un mayor alcance y cobertura, y también aumentaría la velocidad, lo que redundaría en una disminución del consumo de energía. (Sossa, s.f.)

5.7. Encriptación

El proceso de tomar cierta información comprensible y codificarla para que no pueda ser interceptada mientras se viaja por Internet se conoce como cifrado o cifrado de archivos. El cifrado se utiliza para salvaguardar información confidencial, incluidas contraseñas, números de cuentas bancarias y otros datos personales y de registro. (Urrutia, 2023)

Al ocultar el contenido de un mensaje a simple vista y hacer que requiera una interacción específica para descifrarlo, se dice que la información está encriptada. El contenido de este mensaje puede incluir archivos, datos, mensajes o cualquier otro tipo de información que se te ocurra. Cada vez que envía datos a través de Internet desde su computadora a una red, se pueden cifrar. (Fernández Y. , Encriptación, 2020)

5.7.1. WPS

WPS, significa Wifi Protected Setup (o Wifi protected setup en español), es un acrónimo. Con esto, el usuario puede dar por sentado que se trata de un sistema para configurar la conexión Wifi de un dispositivo de forma rápida y segura. Su función es dar a otros dispositivos una forma de "emparejarse" con el Wifi de su casa. Esto significa que puede usar este botón para conectarse al enrutador y luego obtener acceso a la red sin usar una contraseña o nombre Wifi. (Fernandez, 2021)

¿Cómo funciona el botón WPS del router?

Debe realizar las siguientes acciones para poder utilizar el botón WPS para conectar un dispositivo a su red Wifi:

1. Verifique que la compatibilidad con WPS esté disponible encendiendo su dispositivo.
2. Se debe presionar el botón WPS de su enrutador.
3. El LED WPS del enrutador no comenzará a parpadear durante unos segundos.
4. La opción "Conectar vía WPS" debe encontrarse y elegirse en su dispositivo.

Sin necesidad de contraseña, su dispositivo ahora está vinculado a su red Wifi. Es importante recordar que, si bien esto simplifica la conexión a la red, también puede ser menos seguro que ingresar la contraseña manualmente. (Muñoz, 2023)

5.7.2. WPA2

La segunda generación del protocolo de seguridad Wi-Fi Protected Access, conocido por sus siglas WPA2, aborda los errores y proporciona un cifrado más sólido. Es un protocolo de seguridad que salvaguarda el tráfico de Internet en redes inalámbricas. (Ghimiray, 2022)

Su enrutador es vulnerable a las amenazas de seguridad porque construye redes y controla los datos enviados y recibidos por los dispositivos conectados. Los datos privados, ya sea que los almacenen grandes o pequeñas empresas, son valiosos para los piratas informáticos. (Ghimiray, 2022)

El sucesor de WPA Y WEP, WPA2, codifica los datos utilizando tecnología de encriptación en un esfuerzo por hacerlos ininteligibles para los piratas informáticos. Los piratas informáticos tienen una connotación tanto positiva como negativa. (Ghimiray, 2022)

En la esfera negativa, hay grupos que violan la ley y obtienen acceso no autorizado a sitios web, dejándolos vulnerables. En el lado positivo, los piratas informáticos son expertos en el campo de la informática, lo que les permite identificar problemas o puntos débiles en el software y ayudar a solucionarlos. (Ghimiray, 2022)

¿Cómo funciona WPA2?

Todos los protocolos funcionan mediante el uso de claves criptográficas para cifrar y hacer ininteligibles los datos; la misma clave también se utiliza para descifrar los datos. (Ghimiray, 2022)

No todos los protocolos de seguridad utilizan la misma tecnología; por el momento, WPA2 es el estándar de seguridad de la red debido a las técnicas de encriptación de datos. También puede seleccionar configuraciones de seguridad WPA2 específicas según sus necesidades para mejorar la seguridad. (Ghimiray, 2022)

5.7.3. WPA2-PSK

Puede personalizar su seguridad para uso doméstico o de oficina configurando el enrutador para WPA2. WPA2-personal (WPA2-PSK) es preferible para redes domésticas o pequeñas empresas, mientras que WPA2-enterprise está configurado para grandes empresas. (Ghimiray, 2022)

Los enrutadores están protegidos por claves de cifrado, que cifran sus datos y los protegen de los piratas informáticos. WPA2 emplea encriptación de clave dinámica, que cambia con frecuencia la clave y, por lo tanto, es más difícil de descifrar. (Ghimiray, 2022)

Cuando un cliente personal WAP2 proporciona una clave compartida, cada cliente individual en la red recibe una clave de cifrado especial. Los caracteres ingleses entre 8 y 63 componen la clave. (Ghimiray, 2022)

Dado que WPA2-PSK se basa en una sola contraseña para todos los clientes de la red, solo es apropiado para uso comercial. Sin embargo, debe usarse para redes domésticas, ya que permite que los clientes conecten la red sin necesidad de un servidor de autenticación empresarial. (Ghimiray, 2022)

¿Hasta qué punto WAP2 es seguro?

Todos los protocolos de seguridad tienen como objetivo abordar los errores de sus predecesores. WAP2 mejoró los problemas de seguridad que surgieron con WPA y WEP. Estos protocolos de seguridad anteriores demostraron ser de calidad, ya que el cifrado fue fácilmente atacado por hábiles hackers; el cifrado AES utilizado por WAP2. (Ghimiray, 2022)

WPA frente a WPA2

La tabla siguiente que se presenta a continuación, compara las diferencias entre WPA y WPA2:

	WPA	**WPA2**
Fecha de lanzamiento	2003	2004
Tipo de cifrado	TKIP, un sistema imperfecto que se puede descifrar	AES, un sistema más seguro y ampliamente disponible
Compatibilidad	Compatible con software más antiguo	Solo compatible con software más reciente
Uso típico	Solo para el hogar	Opciones para el hogar y para la empresa
Potencia de procesamiento requerida	Mínima	Más que WPA, pero insignificante para la mayoría de los sistemas

Tabla 1. Comparación entre WPA Y WPA2.
(Ghimiray, 2022)

5.7.4. AES

Las técnicas de cifrado de bloques como el Estándar de cifrado avanzado, también conocido como AES (por su abreviatura en inglés), se desarrollaron en Bélgica y todavía se usan ampliamente en la actualidad. Fue seleccionado en 2001 como el sistema de encriptación para proteger la información clasificada del gobierno de EE. UU., luego de ser creado en 1997 en el Instituto Nacional de Estándares y Tecnología de la nación europea. Finalmente, fue aprobado como estándar de seguridad cibernética en 2002, luego de un proceso de revisión prolongado. (Pablo, 2022)

La velocidad y adaptabilidad del cifrado simétrico son sus principales beneficios. Por el contrario, la solidez de la información se ve disminuida por el hecho de que la clave debe ser compartida entre el remitente y el destinatario. Los cifrados asimétricos son muy seguros, pero también muy lentos. Como resultado, AES es un método rápido y en gran medida seguro para cifrar los datos que se envían a través de una red. Servicios como WhatsApp y Signal, que son muy conocidos, lo utilizan para el cifrado, entre muchos otros fines. (Pablo, 2022)

¿Para qué se utiliza el cifrado AES?

Redes Wifi AES: es uno de los sistemas de encriptación más utilizados y, cuando se combina con WPA2, crea una de las barreras de seguridad más efectivas. (Pablo, 2022)

La mayoría de los servicios VPN disponibles en la actualidad utilizan tecnologías de cifrado de última generación, como AES-256. Lo crucial es elegir una contraseña segura. El cifrado AES se utiliza para proteger a casi todos los administradores de contraseñas. Windows, Android y otras plataformas. también utiliza sistemas de encriptación AES para salvaguardar algunos de sus componentes cruciales. (Pablo, 2022)

5.8. Internet

Una red de computadoras conectadas globalmente para compartir información se conoce como Internet. Es una red de dispositivos informáticos que se comunican entre sí mediante un lenguaje común. Las palabras inglesas "interconnected" (que significa "interconectado") y "networks" (que significa "redes") son la base de la idea de Internet, que consiste en redes interconectadas. Dado que se refiere a "La Red" (el sistema que utiliza el protocolo TCP/IP para conectar computadoras a nivel mundial), siempre se debe escribir con mayúsculas. Existen varios tipos de conexiones a Internet, o maneras de conectarse a la red de redes, disponibles en la actualidad. El primero de ellos fue una conexión de acceso telefónico, que implicaba conectarse a una línea telefónica a través de un cable. Posteriormente, surgieron tipos más nuevos para la conectividad de dispositivos móviles, incluidos 3G y 4G (LTE), ADSL, fibra óptica y otros. Internet constituye una vasta red de redes, y los navegadores web (software) se utilizan para acceder a los miles de millones de sitios web que están disponibles en ella. Algunos de los navegadores web más populares son Google Chrome, Internet Explorer, Mozilla Firefox y Safari, todos creados por varias empresas de tecnología. (Equipo editorial Etecé, 2021)

Servicios y usos de Internet:

- Las personas pueden buscar cualquier tipo de información que necesite (por ejemplo, en Google).
- Las personas pueden comprar productos de diversa índole (por ejemplo, en Amazon o MercadoLibre).
- Las personas pueden comunicarse con familiares o amigos que estén en otros países o ciudades mediante una videollamada (por ejemplo, de Skype o WhatsApp).
- Las personas pueden jugar juegos en línea (como el League of Legends) con personas de distintas nacionalidades y edades, en tiempo real. (concepto.de, 2023)

5.9. Firewalls

Los usuarios no autorizados no pueden unirse a una red privada que está conectada a Internet mediante un firewall, un componente de una computadora. Como resultado, el cortafuegos se concentra en examinar de cerca cada mensaje que entra y sale de la red para bloquear la llegada de aquellos que no cumplen con los estándares de seguridad y permitir que los que sí lo hacen avancen sin obstáculos. (Moes, 2023)

Usaremos una analogía muy sencilla para ayudar a explicar este concepto: imagina un cortafuegos como una puerta en tu casa que se conecta a las redes informáticas. Tal puerta mantiene a los extraños fuera de nuestra casa de manera similar a como un firewall mantiene a los usuarios no autorizados fuera de una red privada. (Moes, 2023)

Sin un firewall, una computadora o una red de computadoras podría ser atacada e infectada con frecuencia. Esto hace que la función del firewall sea esencial. Junto a los firewalls que normalmente podemos activar desde el sistema operativo del dispositivo, algunas empresas de antivirus también brindan protección de firewall adicional para fortalecer el sistema de defensa y detener la entrada e instalación de código malicioso. (Moes, 2023)

5.10. Visual Studio Code

Es un editor de código fuente desarrollado por Microsoft que se puede descargar gratuitamente y es multiplataforma para Windows, GNU/Linux y macOS. (Flores, 2022)

5.10.1. Para que sirve Visual Studio Code

Permite escribir código en una variedad de idiomas, es altamente personalizable. En Visual Studio Code, se incluye una terminal con todas las funciones necesarias, la cual puede ser

iniciada fácilmente desde el directorio de trabajo del usuario. El terminal integrado admite cualquier shell instalado en la computadora, como PowerShell, Bash u otros, permitiendo una amplia flexibilidad en la elección de la interfaz de línea de comandos. (Flores, 2022)

Al usar las extensiones adecuadas, puede conectarse a máquinas virtuales de forma remota mediante SSH, contenedores y WSL (Subsistema de Windows para Linux), acceder al sistema de archivos, controlar el terminal y trabajar con aplicaciones en contenedores e implementarlas. (Flores, 2022)

Los beneficios de usar Visual Studio Code incluyen la capacidad de instalar solo las herramientas de desarrollo necesarias y personalizarlo para satisfacer las necesidades del usuario. (Flores, 2022)

Características de Visual Studio:

- **Compatibilidad multiplataforma:** Windows, GNU/Linux y macOS son sistemas operativos compatibles con Visual Studio Code. Con la facilidad de extensión, el usuario puede personalizar y obtener un IntelliSense más completo. IntelliSense está relacionado con la edición de código, el autocompletado y el resaltado de sintaxis, lo que proporciona más facilidad al crear código. (Flores, 2022)

- **Depuración:** Ayuda a encontrar errores en el código, ahorrando tiempo dedicado a corregirlos línea por línea. (Flores, 2022)

- **Uso del control de versiones:** Visual Studio Code es compatible con Git, lo que les permite a los usuarios organizar archivos y buscar diferencias de manera eficiente. (Flores, 2022)

- **Extensiones:** Visual Studio Code es un editor poderoso debido a su amplia variedad de extensiones. Estas extensiones permiten a los usuarios personalizar y agregar nuevas funcionalidades de manera modular y aislada. (Flores, 2022)

5.11. Páginas web

Una página web, página electrónica o página digital es un documento digital con capacidades multimedia (capaz de incluir audio, video, texto y sus combinaciones) que ha sido optimizado para la World Wide Web (WWW) y se puede acceder a través de un sitio web, un navegador y una conexión a Internet activa. En la red, constituye el formato de contenido fundamental. (Equipo editorial E. , s.f.)

En Internet hay más de mil millones de páginas web en varios idiomas, siendo el mayor depósito de conocimiento humano. Estas páginas están en miles de servidores y se acceden fácilmente mediante protocolos de comunicación (HTTP). (Equipo editorial E. , s.f.)

En muchos casos, el acceso a una página web o su contenido particular puede estar restringido, sujeto a pagos de terceros o requerir formas adicionales de identificación (como registro en línea). (Equipo editorial E. , s.f.)

Además, el contenido de esta vasta biblioteca virtual no está totalmente supervisado, y su regulación plantea un desafío y un punto de discordia para las instituciones tradicionales de la

humanidad, incluyendo la familia, la escuela e incluso el derecho internacional. (Equipo editorial E. , s.f.)

Las páginas web programadas en HTML o XHTML se distinguen por su relación entre sí a través de hipervínculos: enlaces a diversos contenidos que permiten una lectura compleja, simultánea y variada, muy diferente de la que se encuentra en libros y revistas. (Equipo editorial E. , s.f.)

¿Qué diferencia existe entre un sitio web de una página web?

Un sitio web consta de páginas web, que son archivos individuales con nombres específicos. Esto se asemeja a un libro completo (sitio web) que contiene capítulos individuales (páginas web). (Carmen, 2023)

Páginas web estáticas

Estas páginas funcionan descargando un archivo HTML que proporciona al navegador todas las instrucciones para mostrar la página web de forma estática sin interacción del usuario. Son informativas y no interactivas. (Equipo editorial E. , s.f.)

Sitios web dinámicos

A diferencia de las anteriores, las páginas web dinámicas se crean justo cuando un usuario accede a ellas, utilizando para ello un lenguaje interpretado (como PHP). Esto le permite recibir solicitudes de los usuarios, procesarlas en bases de datos y brindar una respuesta que satisfaga sus necesidades. (Equipo editorial E. , s.f.)

5.11.1. HTML

HTML (Hyper Markup Language) es un lenguaje de marcado que cumple con la funcionalidad de crear y estructurar el contenido de páginas web. Es un conjunto de etiquetas; su función principal es definir el texto y otros elementos que compondrán una página web, como imágenes, listas, videos, etc. (DesarrolloWeb, 2001)

Estructura Básica HTML

La estructura básica se compone de etiquetas, las cuales muestran el inicio de la página, como <html>, la información descriptiva en <head> y los elementos visibles en <body>. (DesarrolloWeb, 2001)

Debemos de tomar en cuenta que las etiquetas están conformadas con un inicio y un fin como <p> en donde notamos claramente la apertura y el cierre de la etiqueta que vamos a usar. Dentro de estas etiquetas existen dos como vemos en la siguiente figura:

Etiquetas emparejadas: Tienen una apertura y un cierre como < >.

Etiquetas vacías: Son las que no requieren un cierre.

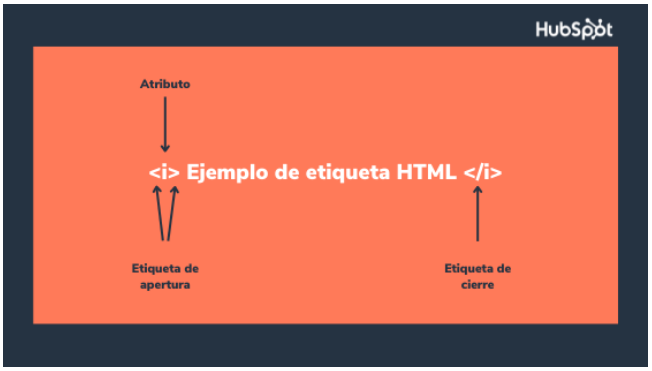


Figura 25. Etiquetas HTML.
Fuente: (Coppola, s.f.)

Entendiendo lo mencionado anteriormente la estructura básica HTML seria de la siguiente forma, como lo muestra la siguiente figura 26:

Figura 26. Estructura básica HTML.
Fuente: (Adrián, 2013)

¡En donde, si se desea se pude agregar un <!**DOCTYPE html**> dónde se indica la versión HTML. De ahí se tiene:

<html> </html>: Elemento raíz que contiene etiquetas de atributos de la página.

<head> </head>: La etiqueta principal se refiere es un elemento del lenguaje HTML, se utiliza para incluir atributos que no son visibles para el usuario final, pero que son relevantes para la página web. Dichos atributos pueden consistir en información como el título de la página o las referencias a archivos CSS que se utilizan para dar estilo al contenido.

<body> </body>: Etiqueta que desarrolla todo el cuerpo de la página web, el cual también engloba datos como textos y enlaces.

En la etiqueta <body> existen elementos y etiquetas como los siguientes:

- **<h1>, <h2>, <h3>, <h4>, <h5>, <h6>:** Son etiquetas de títulos.
- **<p>:** indicar la apertura y cierre de un párrafo.
- ** :** es una división la cual crea secciones o puede agrupar información.
- **:** da formato al texto o agrupar elementos en línea mediante la aplicación de estilos.

- **<b>, <i>, <u>:** agrega a un texto negritas, cursiva y subrayado.
- **<a>:** agrega un vínculo o enlace.
- **<img>, <audio>, <video>, <iframe>:** insertar imagen, audio, video o documento HTML.
- **<form>:** inserta un formulario.
- **<label>:** etiqueta de elemento en interfaz de usuario.
- **<input>:** da control interactivo a un formulario para poder recibir información del usuario.

La siguiente figura ejemplifica un esquema HTML:

```
<!DOCTYPE html>
<html>
<head>
    <title>Blog de HubSpot</title>
</head>
<body>
    <h1>¿Cuál es la estructura HTML de una página web?</h1>
    <h2>¿Para qué sirve conocer la estructura HTML?</h2>
<p>La estructura HTML hace uso de etiquetas y atributos predefinidos para
indicarle al navegador cómo mostrar su contenido; es decir, en qué formato,
estilo, tamaño de fuente, imágenes o videos se debe configurar.
</p>
<img src="escritorio/estructura-html.png"/>
</body>
</html>
```

Figura 27. Ejemplo de etiquetas básicas HTML.
Fuente: (Coppola, s.f.)

5.11.2. CSS

CSS (Cascading Style Sheets) es un lenguaje de hojas de estilo utilizado para dar estilo y formato al contenido de una página web. Fue desarrollado por W3C (World Wide Web Consortium) en 1996 por una razón muy sencilla. HTML no fue diseñado para tener etiquetas que ayuden a formatear la página. Está hecho solo para escribir el marcado para el sitio. (Gustavo, 2023)

HTML estructura el contenido, CSS define su apariencia. CSS separa estilo y estructura con selectores como clases, identificadores y atributos. Utiliza herencia y cascada para aplicar estilos eficientemente, incluyendo la aplicación automática de estilos a elementos secundarios.

Las propiedades controlan aspectos como el color, el tamaño, el margen, el relleno y la fuente, entre otros, mientras que los valores especifican las características específicas de cada propiedad. CSS utiliza propiedades y valores para definir cómo se mostrarán los elementos seleccionados. (Gustavo, 2023)

El atributo "Estilo" en HTML permite la adición directa de estilos en línea a elementos HTML en la sección del documento HTML. Mediante el uso de archivos CSS separados, los estilos externos se definen y vinculan al archivo HTML mediante la etiqueta. (Gustavo, 2023)

Beneficios de CSS

1. Se puede utilizar CSS para separar la presentación visual de un documento HTML de su contenido. Esto implica que se puede crear un archivo HTML limpio y bien organizado sin agregar estilos en línea o directamente al código HTML.
2. Ofrece una amplia flexibilidad y control sobre el diseño del sitio web.
3. Permite la producción de hojas de estilo globales que pueden utilizarse en numerosas páginas web. Esto simplifica la actualización y el mantenimiento del diseño general y garantiza una apariencia uniforme en todas las páginas.
4. Se pueden crear diseños que respondan y se ajusten automáticamente a diferentes dispositivos y tamaños de pantalla. (Gustavo, 2023)

5.12. Portales Cautivos

Un portal cautivo es un servicio utilizado generalmente cuando una persona se conecta a una red para controlar el acceso y la velocidad de esta, ya sea en una red cableada o inalámbrica. El funcionamiento se basa en que, al conectarse a la red, se presenta al usuario una página de registro en la que este debe introducir sus datos. Estos datos son verificados y, si son correctos, se permite el acceso a la red.

En resumen, un portal cautivo es una página web que intercepta a los usuarios cuando intentan acceder a una red Wifi pública o privada y les solicita autenticación o aceptación de términos antes de permitirles el acceso completo a Internet. Los portales cautivos son comunes en redes Wi-Fi públicas, hoteles, aeropuertos y empresas. (Nettix, s.f.)

Existe pequeña variedad entre portales cautivos, a continuación, se detallan los más representativos:

5.12.1. Wifidog

El proyecto Wifidog fue desarrollado hacia el año 2003 por la empresa canadiense Île sans fil (isla inalámbrica), con el objetivo de crear una solución de portal cautivo que, al no necesitar una gran cantidad de espacio de almacenamiento y capacidad de procesamiento, pudiera implementarse en equipos integrados, como, por ejemplo, en los routers Linksys WRT54G. Este software se distribuye bajo las licencias CC (Creative Commons) y GNU GPL. (Lorente, 2014)

Wifidog, a diferencia de otros portales cautivos como NoCat, no requiere que una ventana del navegador web del cliente se mantenga siempre activa, lo que permite su funcionamiento con cualquier plataforma que incluya un navegador, como teléfonos inteligentes y tabletas. El

control del mantenimiento de la conexión entre el sistema y los usuarios se realiza mediante la comprobación de la actividad del adaptador de red, realizando ping cada cierto tiempo. (Lorente, 2014)

Wifidog consta de dos partes bien diferenciadas: la puerta de enlace (gateway) y el servidor de autenticación. El gateway, desarrollado en lenguaje C, maneja las reglas de cortafuegos, denegando el acceso a la red a los usuarios no autenticados y estableciendo los puertos y protocolos permitidos a los usuarios registrados. Se conecta con el servidor de autenticación, desarrollado en PHP y que utiliza una base de datos PostgreSQL para almacenar la información de las sesiones. El servidor de autenticación verifica las credenciales del usuario, ya sea utilizando una base de datos local o algún servidor externo tipo Radius, y dependiendo de las configuraciones, puede aplicar algunas restricciones de uso, como, por ejemplo, un límite de tiempo o una cantidad de ancho de banda disponible para cada usuario. (Lorente, 2014)

La siguiente figura muestra una captura de pantalla del portal cautivo Wifidog:

Figura 28. Portal cautivo Wifidog.
Fuente: (Randrianarimanana)

5.12.2. IPCop

Es un software enfocado a realizar las funciones de un firewall, lo que le permite al usuario asegurar sus redes de una forma totalmente transparente y con un coste de implementación muy bajo. Los requerimientos de este software son mínimos, y además, al ser software libre, elimina los costes de licenciamiento. Aunque es cierto que otros sistemas, como puede ser ISA Server (Internet Security and Acceleration Server), pueden mantener una mejor convivencia con sistemas Windows Server, estos son muy caros. Sin embargo, IPCop y este tipo de soluciones ofrecen la posibilidad de disponer de una mayor protección en la red con un coste de implementación mínimo. (soporteti, 2015)

IPCop, es una distribución de Linux dedicada a actuar como cortafuegos de red, ofrece ventajas como el control y monitoreo del tráfico de datos en una red local. Sin embargo, presenta desventajas significativas. Su configuración resulta compleja, especialmente para usuarios sin experiencia, requiere hardware específico para su funcionamiento y carece de configuraciones avanzadas de firewall. En consecuencia, esta alternativa no se considera la mejor opción para el proyecto, dado que, a pesar de ser de software libre, no cuenta con las funcionalidades necesarias. (Ecured, s.f.)

La siguiente figura muestra una captura de pantalla del dashboard de IPcop:

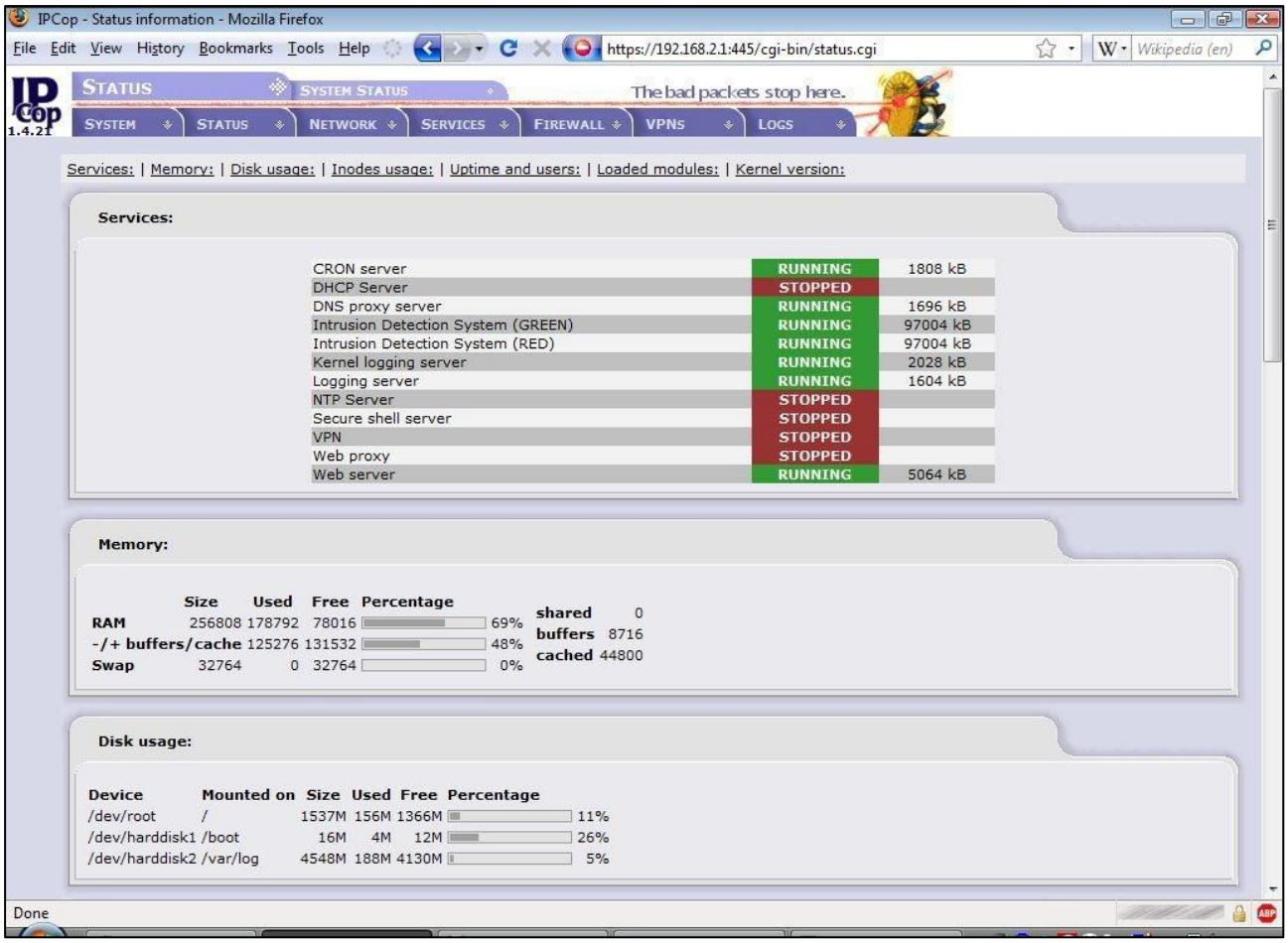


Figura 29. Portal cautico IPCop.
Fuente: (Pardo, 2022)

5.12.3. pfSense

Es un sistema operativo de código abierto basado en FreeBSD que se utiliza comúnmente como un firewall y enrutador de red. Es una plataforma de seguridad y gestión de red altamente flexible que ofrece una amplia gama de características y funcionalidades para proteger y administrar redes de diferentes tamaños y complejidades. (keepcoding, 2023)

Algunas de las características clave de pfSense incluyen:

- Firewall: pfSense proporciona un firewall de última generación con capacidades avanzadas de filtrado de paquetes y seguridad perimetral.

- Enrutamiento: Puede funcionar como un enrutador, permitiendo la interconexión de redes y la gestión de rutas.
- VPN (Virtual Private Network): pfSense admite la creación de conexiones VPN seguras, incluyendo VPN de acceso remoto y VPN de sitio a sitio.
- Proxy y filtrado de contenido: Ofrece capacidades de proxy web y filtrado de contenido para aplicar políticas de navegación web.
- Portal cautivo: Una de las características notables de pfSense es su capacidad para implementar portales cautivos. (keepcoding, 2023)

La siguiente figura muestra una captura de pantalla del dashboard inicial de pfSense:

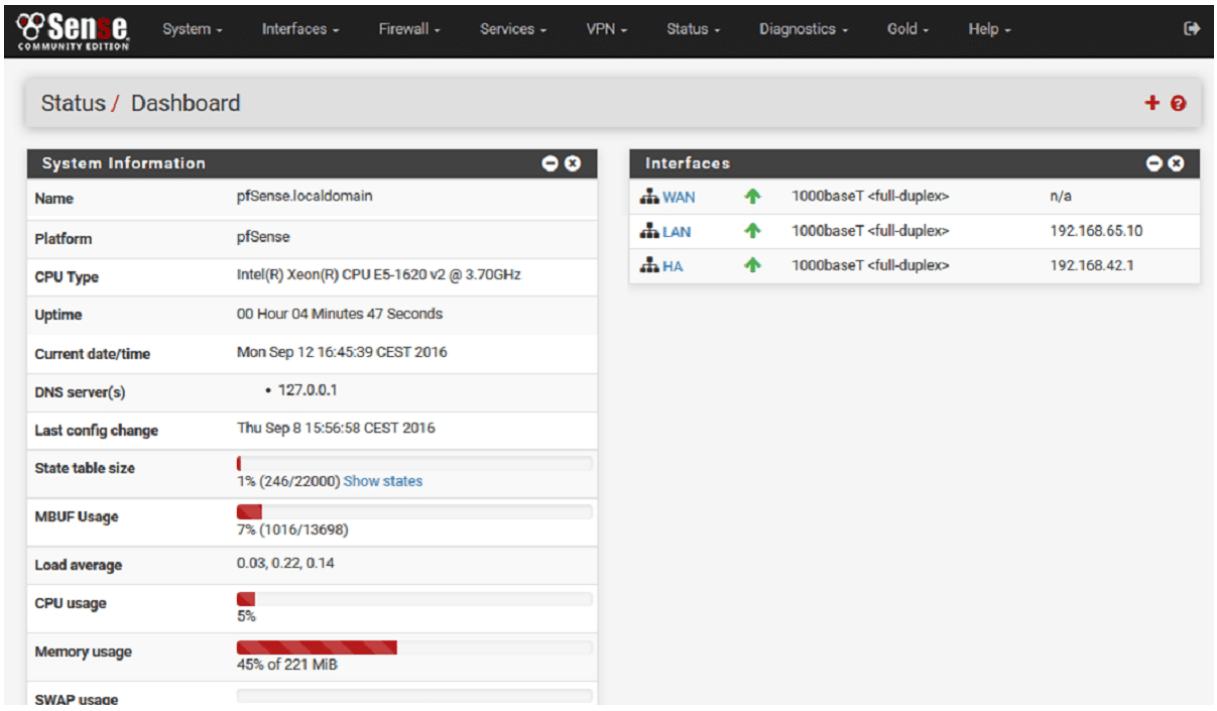


Figura 30. Portal Cautivo pfSense.
Fuente: (Nettix, 2021)

pfSense como portal cautivo

Con pfSense, es posible configurar la forma en que los usuarios de una red acceden a Internet. Se pueden establecer configuraciones simples, como mostrar únicamente una página de información al usuario, o implementar diferentes sistemas de validación. (Nettix, s.f.)

Los cupones son códigos de un solo uso, utilizados para obtener acceso a Internet a través de un Portal Cautivo. Cada rollo de vales se genera criptográficamente e incluye un conjunto límite de tiempo. Los cupones son comunes en lugares donde las organizaciones desean acceso a Internet autenticado, pero con tiempo limitado, sin necesidad de proporcionar un nombre de usuario y contraseña. (Netgate, s.f.)

El tiempo del cupón no deja de contar hacia abajo si un usuario cierra la sesión; permiten el acceso solo desde el inicio de la sesión hasta la duración del cupón transcurrido. Durante ese tiempo, el cupón puede ser reutilizado por la misma o diferente computadora. Si el cupón es utilizado nuevamente por otra computadora, la sesión anterior se detiene. (Netgate, s.f.)

Los cupones requieren un par de claves RSA público/privado para generar y verificar. Un conjunto de claves de 32 bits es generado automáticamente por el firewall la primera vez que la página carga. La GUI también puede generar manualmente un par de claves personalizadas. La longitud máxima de la clave es de 64 bits. El uso de claves más cortas hará que los códigos de cupones sean más cortos, pero eventualmente menos seguros. (Netgate, s.f.)

La siguiente figura muestra una captura de pantalla del Login de pfSense, donde se ingresan el usuario y la contraseña o el váucher:

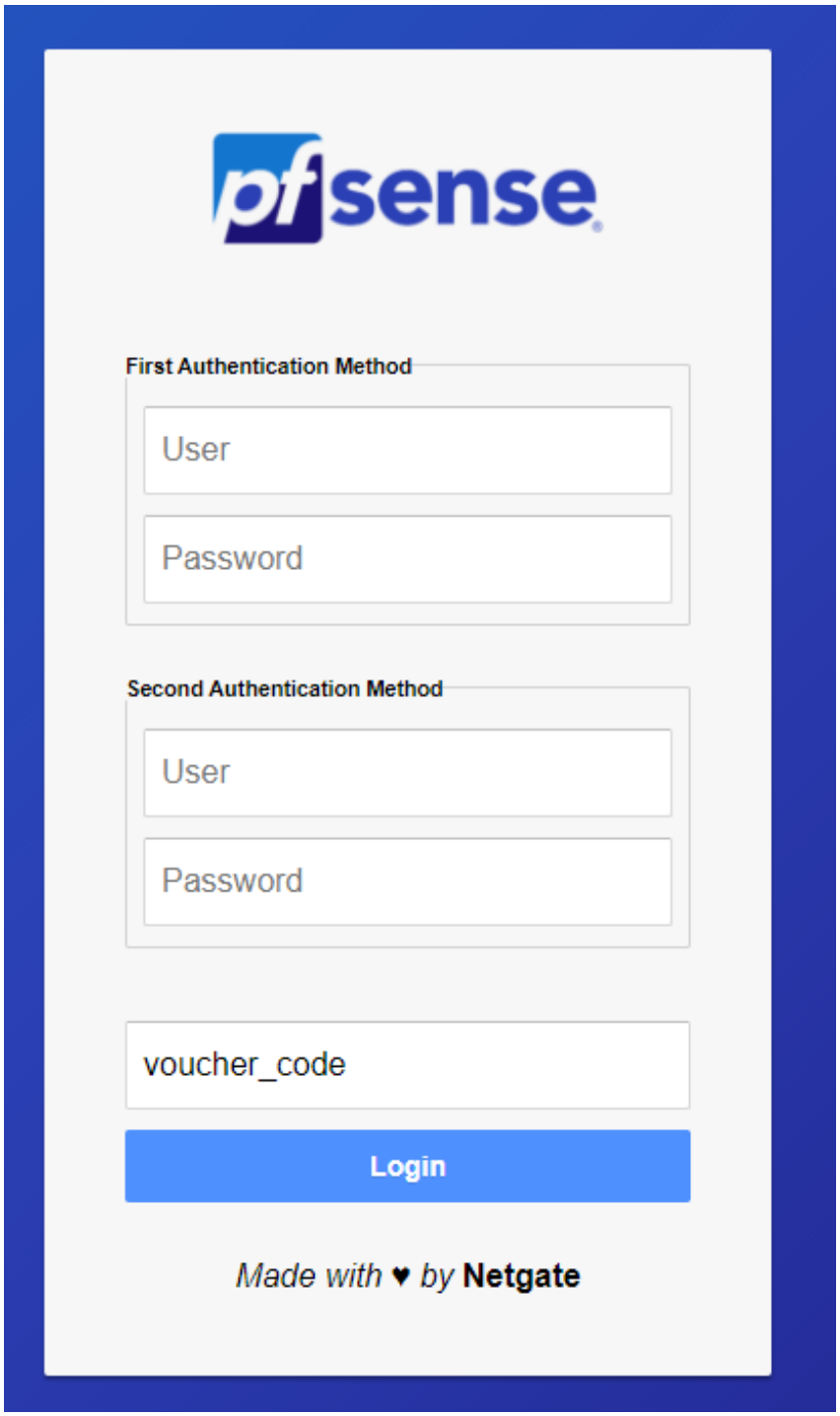


Figura 31. Portal cautivo con pfSense, ventana de autentificación.
Fuente: (Zawi, 2020)

5.12.4. Comparación de pfSense vs otros portales cautivos

A continuación, se presenta una tabla comparativa entre pfSense, Wifidog e IPCop en términos de portal cautivo y otras características clave:

Característica	**pfSense**	**Wifidog**	**IPCop**
Tipo de Software	Firewall y Enrutador	Portal Cautivo	Firewall y Enrutador
Interfaz de Usuario	Web GUI	Web GUI	Web GUI
Autenticación de Usuarios	Sí	Sí	Sí
Personalización de Páginas	Sí	Sí	Sí
Integración de Base de Datos	Sí	Sí	Sí
Soporte para VLAN	Sí	Sí	Sí
Soporte para RADIUS	Sí	Sí	Sí
Captura de Información de Cliente	Sí	Sí	Sí
Redireccionamiento de URLs	Sí	Sí	Sí
Autenticación de Múltiples Factores	Sí	No	No
Registro y Auditoría	Sí	Sí	Sí
Soporte para Hotspot 2.0	No	No	No
Gestión de Ancho de Banda	Sí	No	No
Licencia	Open Source (varias)	Open Source (GPLv2)	Open Source (GPLv2)

Tabla 2. Comparativa entre portales cautivos investigados.
Fuente: las autoras.

Algunas observaciones para mencionar son:

- pfSense es una solución completa que incluye portal cautivo además de sus capacidades de firewall y enrutamiento. Es una opción robusta y versátil para la gestión de redes.
- Wifidog se centra en la función de portal cautivo y es una solución más ligera y específica para la autenticación de usuarios en redes públicas o abiertas.

- IPCop es un sistema de firewall y enrutador que, si bien es capaz de algunas funciones de portal cautivo, se centra más en la seguridad perimetral y no ofrece las mismas capacidades avanzadas de portal cautivo que pfSense.

Se ha seleccionado pfSense como la solución de Portal Cautivo, al ser software libre y el manejo de váuchers son las razones centrales para esta elección. pfSense permite implementar un Portal Cautivo altamente personalizable, lo que significa que se puede ofrecer a los usuarios una experiencia de inicio de sesión segura y fluida en la red Wifi de la institución. La función de manejo de váuchers es excepcional, permitiendo generar y administrar fácilmente códigos de acceso temporales e inclusive si fuera necesario de pago para algunos usuarios.

Esto es esencial para el entorno del edificio matriz, ya que brinda un control completo sobre quién accede a la red y cuándo. En combinación con sus sólidas capacidades de firewall y enrutamiento, pfSense se destaca como la elección perfecta para la red haciéndola segura y brindando un acceso gestionado de manera eficiente a la comunidad institucional.

5.13. Correos electrónicos masivos

El proceso de enviar un correo electrónico idéntico a numerosos destinatarios se denomina envío masivo de correos electrónicos. En contraste con los correos transaccionales, que se activan mediante acciones del usuario, los correos masivos generalmente se distribuyen de una sola vez a una lista de suscriptores predefinida. En los correos masivos existen “campos” que se pueden personalizar en función de cada destinatario (InvestGlass, 2023)

5.13.1. MailChimp

MailChimp representa una de las herramientas más utilizadas y accesibles en la creación de campañas de email marketing. Facilita la elaboración de correos electrónicos desde cero, comparándola con la resolución de un rompecabezas. Su interfaz web es clara, extremadamente fácil de usar e intuitiva, proporcionando una guía detallada sobre el proceso de creación de correos electrónicos mediante plantillas que sirven como punto de partida para diseñar. (Roymo)

En la actualidad se pueden encontrar varios programas que pueden realizar esta tarea, pero la gran ventaja de MailChimp es que cuenta con una versión totalmente gratuita, permite enviar correos electrónicos automáticos a 2.000 direcciones de correo electrónico o suscriptores de la newsletter, con un máximo de 12.000 correos al mes. Y todo esto sin necesidad de pagar. En caso de que la actividad requiera un volumen de mensajes mayor, siempre existe la opción de acceder a la versión Premium. (Cabrera, 2021)

La siguiente figura muestra una captura de pantalla de MailChimp, donde podemos apreciar un ejemplo de cómo brinda ayuda para diseñar un correo electrónico:

Figura 32. Pantalla principal de MailChimp.
Fuente: (Moraestudiocreativo, s.f.)

Como funcionan los precios de MailChimp

El plan de marketing gratuito que ofrece es perfecto para aquellos que están dando sus primeros pasos y desean expandir su audiencia, así como crear correos electrónicos, experimentando con algunas de las funciones y herramientas de MailChimp. Este plan abarca todas las funciones esenciales que necesitas para iniciar una estrategia de marketing. Dentro del plan gratuito, se proporciona la capacidad de gestionar hasta 500 contactos y realizar hasta 1,000 envíos al mes, con un límite diario de envíos establecido en 500.

MailChimp dispone de otros tipos de planes, como el Premium, Standard, Essentials y el plan Free, adaptados a las necesidades específicas del negocio. Estos planes escalan según la cantidad de contactos. Además, cuenta con opciones que se ajustan a las demandas de correos electrónicos transaccionales, diseñados especialmente para desarrolladores. (Rada, 2023)

La siguiente figura muestra una captura de pantalla de MailChimp, donde se pueden visualizar los diferentes tipos de planes:

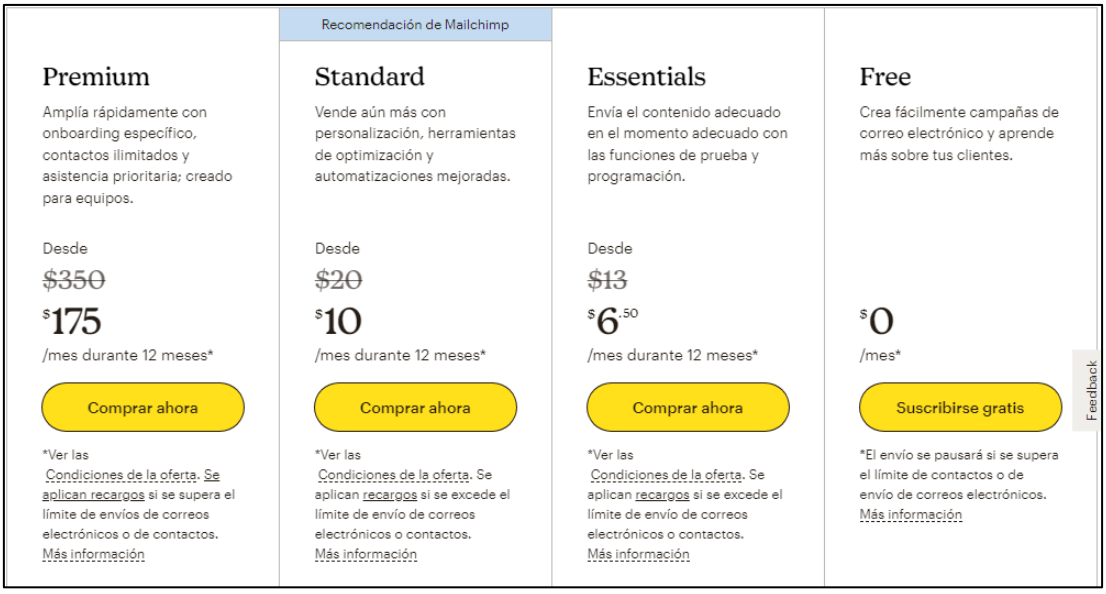


Figura 33. Planes de MailChimp.
Fuente: (Mailchimp, 2023)

5.13.2. AWeber

AWeber se presenta como un servicio de Email Marketing diseñado para la creación de listas de correos automáticas y páginas de aterrizaje. Una de sus principales ventajas radica en que no se necesitan habilidades de programación. Con solo unos clics, los usuarios pueden modificar sus campañas, segmentar a los suscriptores y configurar secuencias de entrega de mensajes o auto respuestas. (Atecnis, 2021)

AWeber no es una plataforma gratuita, no obstante, brinda un período de prueba de 30 días que abarca la mayoría de las funciones. Así, es posible diseñar las estrategias iniciales de Email Marketing en esta plataforma sin incurrir en ningún costo. En caso de satisfacción, el usuario tiene la opción de acceder a diferentes planes de pago, comenzando desde 19 dólares al mes. El paquete básico permite gestionar hasta 500 suscriptores y no presenta restricciones en cuanto a la cantidad de correos electrónicos enviados. (Atecnis, 2021)

La siguiente figura muestra una captura de pantalla de la plantilla de AWeber:

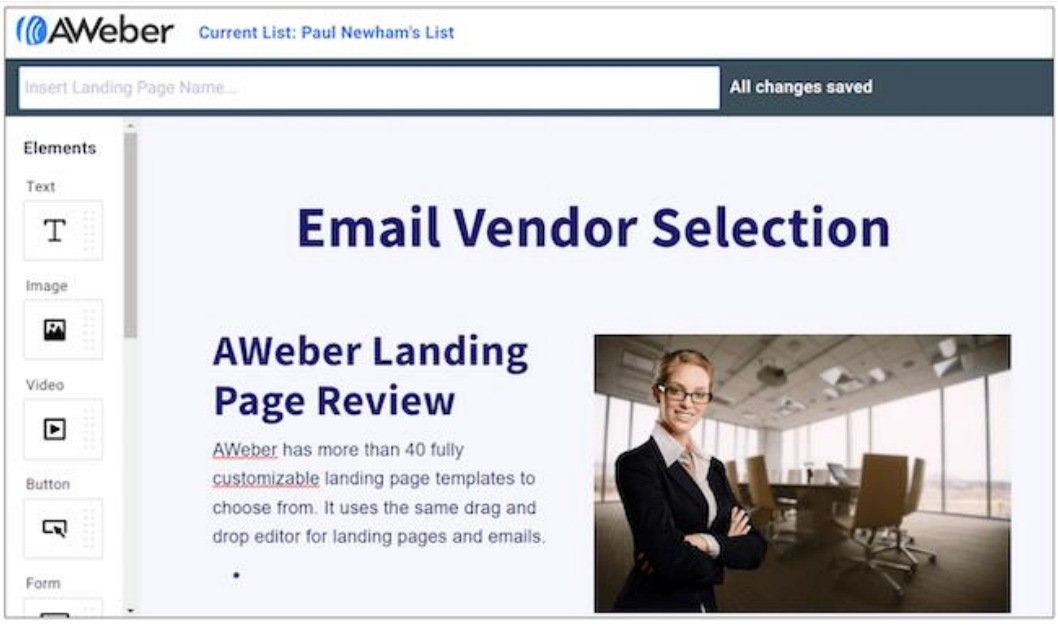


Figura 34. Pantalla principal de AWeber.
Fuente: (Newman, 2023)

Principales caracteristicas de AWeber

- Plantillas personalizables: El programa cuenta con una base de datos que incluye más de 700 plantillas de correos electrónicos completamente adaptables. En el modo de construcción, simplemente arrastrar y soltar permite la inserción de botones, texto o contenido multimedia en el mensaje. Además, las newsletters resultantes son compatibles tanto con computadoras como con dispositivos móviles. (Atecnis, 2021)
- Automatización de correos electrónicos: Otra característica destacada de AWeber es su capacidad para automatizar correos electrónicos o respuestas automáticas. El proceso es fácil: elige una plantilla, crea un correo tipo y programa su envío a los suscriptores deseados en un intervalo de tiempo específico. Esta función resulta especialmente beneficiosa para los negocios, ya que impulsa significativamente las conversiones y ahorra considerable tiempo. (Atecnis, 2021)

5.13.3. Odoo

Odoo es un conjunto de aplicaciones diseñado para cada necesidad empresarial, reuniendo en una sola plataforma su solución personalizada, rentable y modular. Esto permitirá organizar y ahorrar tiempo y recursos mientras se administra el negocio de manera integrada. (indaws, s.f.)

Es importante destacar que Odoo cuenta con una herramienta sumamente útil denominada E-Marketing. Esta herramienta centraliza en una única aplicación los procedimientos vinculados con la creación de correos masivos, la configuración de listas de seguimiento, la planificación y diseño de campañas publicitarias, así como su integración con otras aplicaciones encargadas de supervisar los prospectos de clientes generados. Este enfoque se diseñó con el objetivo de asegurar la integridad de la información al prevenir posibles filtraciones y eliminar pasos superfluos en el proceso, manteniéndolo simple y eficiente. (Mit Mut, 2021)

La siguiente figura muestra una captura de pantalla de Odoo en donde se aprecia una plantilla para crear un correo:

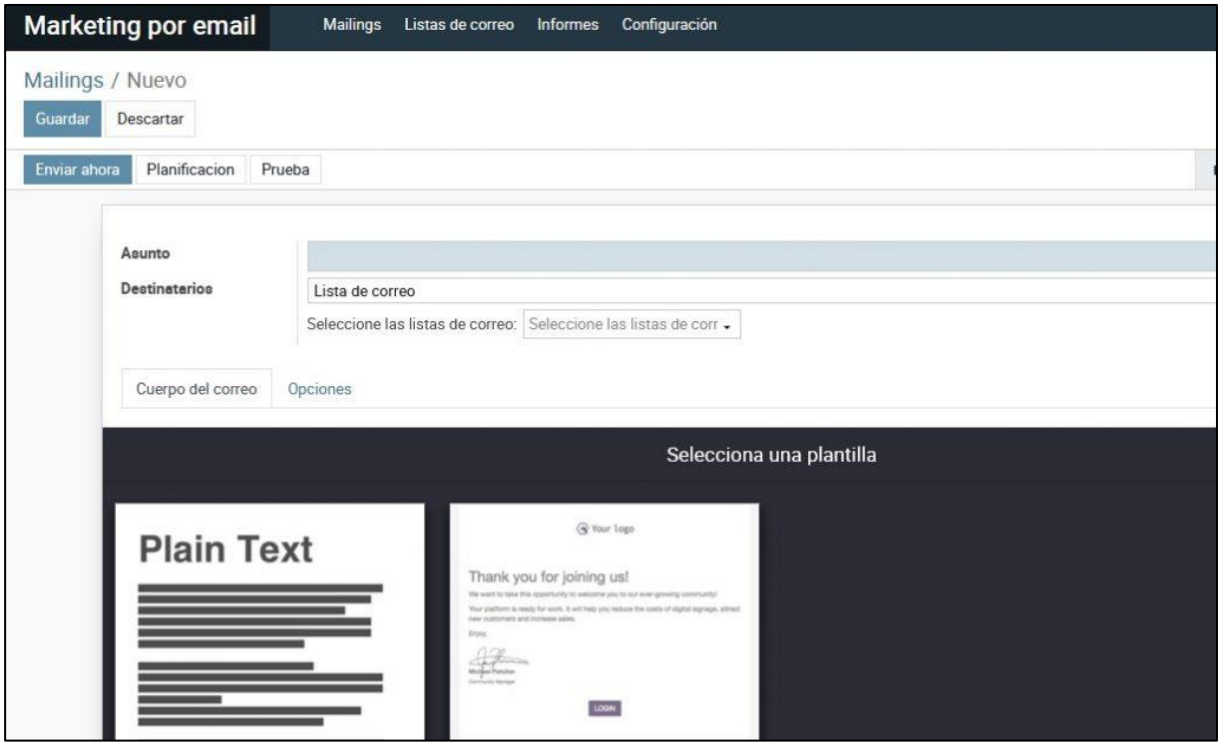


Figura 35. Plataforma de Odoo, marketing por email.
Fuente: (iTecan, 2021)

Características de correo masivo Odoo

Las características de Odoo posibilitan la filtración de destinatarios de la campaña según criterios como país, fecha, puesto en la empresa, entre otros. Esta orientación tiene como objetivo garantizar que solo las personas clave reciban la información compartida, optimizando la relevancia y personalización de los mensajes dirigidos. (Mit Mut, 2021)

Existe una versión gratuita de Odoo, conocida como la versión Community. Sin embargo, presenta ciertas restricciones y no todos pueden acceder a su implementación debido a ciertas limitaciones.

La siguiente figura muestra una captura de pantalla de los precios de Odoo:

Figura 36. Plan y precios de Odoo.
Fuente: (Odoo, 2023)

A continuación, se presenta una tabla comparativa entre MailChimp, Odoo y AWeber en función de algunas características clave:

Característica	**MailChimp**	**Odoo**	**AWeber**
Facilidad de Uso	Fácil de usar con una interfaz intuitiva.	Interfaz de usuario amigable y personalizable.	Interfaz sencilla para crear y enviar correos.
Plantillas de Correo	Ofrece una amplia variedad de plantillas.	Permite personalizar plantillas de correo.	Ofrece plantillas y opciones de diseño.
Automatización	Potentes herramientas de automatización.	Automatización completa de marketing.	Automatización de correos electrónicos.
Segmentación de Listas	Permite segmentar listas de suscriptores.	Ofrece opciones de segmentación avanzada.	Posibilidad de segmentar listas.
Informes y Análisis	Proporciona informes detallados de campañas.	Ofrece informes y análisis de campañas.	Informes básicos de seguimiento.
Integraciones	Amplia gama de integraciones disponibles.	Integración con otras aplicaciones de Odoo.	Integraciones disponibles.
Precios	Ofrece planes gratuitos y de pago.	Varias ediciones de pago disponibles.	Ofrece planes de pago.
Soporte Técnico	Ofrece soporte técnico por chat y correo.	Dependiendo de la edición, puede variar.	Soporte técnico disponible.
Personalización	Personalización avanzada de correos.	Personalización de plantillas y flujos.	Personalización de correos y formularios.

Tabla 3. Comparativa entre plataformas de correos masivos investigados.
Fuente: las autoras.

Se ha optado por utilizar MailChimp como la plataforma de correo electrónico masivo, por una serie de razones que subrayan su idoneidad para nuestras necesidades. MailChimp brinda una interfaz intuitiva y fácil de usar que permite crear y enviar campañas de correo electrónico efectivas de manera rápida y sencilla. Además, su capacidad de automatización permite personalizar y programar mensajes para llegar a los estudiantes en el momento adecuado y socializar fácilmente las credenciales (los váuchers) para acceder a la red Wifi de la Institución. También se valoró su capacidad de seguimiento y análisis que permite medir el rendimiento de las campañas y tomar decisiones basadas en datos. Con una amplia gama de plantillas y herramientas de diseño, MailChimp permite crear correos electrónicos visualmente atractivos y profesionales. En resumen, MailChimp es una elección sólida para llevar a cabo el proyecto y la difusión de los váuchers por correo electrónico de manera efectiva y eficiente.

5.14. NAS

(Fernández Y. , Servidores NAS: qué son, cómo funcionan y qué puedes hacer con uno, 2023)

Un NAS, que significa "Network Attached Storage" en inglés (Almacenamiento Conectado a la Red en español), es un dispositivo de almacenamiento de datos diseñado para servir archivos y datos a través de una red. Funciona como un servidor de archivos dedicado que permite a múltiples usuarios y dispositivos acceder, compartir y respaldar datos de manera centralizada en una red local o a través de Internet.

Algunas características comunes de un NAS incluyen:

1. **Almacenamiento de Datos**: Un NAS contiene uno o varios discos duros (o incluso unidades de estado sólido) para almacenar archivos y datos. La capacidad de

almacenamiento puede variar significativamente según el modelo y las necesidades del usuario.

2. **Conectividad de Red**: Un NAS se conecta a una red local mediante Ethernet, lo que permite a los usuarios acceder a los datos almacenados en él desde computadoras, dispositivos móviles u otros dispositivos en la misma red.
3. **Sistema Operativo Especializado**: La mayoría de los NAS ejecutan un sistema operativo especializado diseñado para gestionar el almacenamiento y proporcionar funciones de servidor de archivos, seguridad y administración.
4. **Acceso Remoto**: Muchos NAS ofrecen la posibilidad de acceder a los datos de forma remota a través de Internet, lo que permite a los usuarios acceder a sus archivos desde cualquier lugar con una conexión a Internet segura.
5. **Copias de Seguridad**: Los NAS a menudo incluyen capacidades de copia de seguridad automáticas y programadas para proteger los datos almacenados.
6. **Compartición de Archivos y Colaboración**: Facilitan la compartición de archivos y la colaboración en equipo, ya que varios usuarios pueden acceder y trabajar en los mismos archivos de forma simultánea.
7. **Transmisión de Medios**: Algunos NAS incluyen aplicaciones para transmitir contenido multimedia, como música y video, a dispositivos compatibles, como televisores inteligentes y reproductores multimedia.
8. **Almacenamiento Redundante**: Muchos NAS admiten configuraciones de almacenamiento redundante (por ejemplo, RAID) para proteger los datos contra fallos de disco.

Los NAS son muy versátiles y se utilizan en una variedad de entornos, desde hogares y pequeñas empresas hasta empresas de tamaño mediano y grande. Ofrecen una solución de

almacenamiento centralizada que simplifica la gestión de datos y mejora la colaboración y el acceso a archivos en una red.

5.14.1. Synology

(Synology, s.f.)

Synology es una empresa taiwanesa que se especializa en el desarrollo y fabricación de dispositivos NAS (Network Attached Storage) y soluciones relacionadas con el almacenamiento de datos y la gestión de servidores. Fundada en 2000, Synology ha ganado reconocimiento internacional por sus productos de alta calidad y su software intuitivo.

Los dispositivos NAS de Synology son servidores de almacenamiento en red diseñados para uso doméstico, empresarial y empresarial. Estos dispositivos permiten a los usuarios almacenar, compartir y gestionar datos de manera centralizada en una red local. Algunas de las características y funcionalidades comunes de los NAS Synology incluyen:

1. *Almacenamiento Centralizado*: Los NAS Synology ofrecen una capacidad de almacenamiento significativa y permiten a los usuarios almacenar y respaldar archivos, documentos, fotos, videos y otros datos de manera centralizada.
2. *Acceso Remoto*: Los usuarios pueden acceder a sus datos almacenados en un NAS Synology desde cualquier lugar con una conexión a Internet segura utilizando aplicaciones y servicios proporcionados por Synology.
3. *Gestión de Archivos*: Synology proporciona software de gestión de archivos que facilita la organización y búsqueda de archivos, así como la capacidad de compartir archivos y carpetas con otros usuarios.

4. *Seguridad y Protección de Datos*: Los NAS Synology ofrecen funciones de seguridad avanzada, incluido el cifrado de datos, copias de seguridad automáticas y funciones antivirus.
5. *Transmisión Multimedia*: Muchos NAS Synology incluyen aplicaciones para transmitir contenido multimedia, lo que los convierte en soluciones de entretenimiento en el hogar.
6. *Aplicaciones de Negocios*: Synology también ofrece una variedad de aplicaciones empresariales, como soluciones de correo electrónico, servidores de archivos, aplicaciones de colaboración y más.
7. *Escalabilidad*: Los NAS Synology suelen ser escalables, lo que significa que los usuarios pueden agregar unidades de disco adicionales para aumentar la capacidad de almacenamiento según sea necesario.
8. *Comunidad Activa*: Synology cuenta con una comunidad activa de usuarios y desarrolladores que contribuyen con aplicaciones y mejoras para los dispositivos.

Synology se ha ganado una sólida reputación por su enfoque en la facilidad de uso, la seguridad y la fiabilidad de sus productos. Sus dispositivos NAS se utilizan en una variedad de entornos, desde hogares y pequeñas empresas hasta empresas de tamaño mediano y grande que requieren soluciones de almacenamiento robustas y versátiles.

5.14.2. TerraMaster

(TerraMaster, s.f.)

Es una marca que se especializa en la fabricación de dispositivos NAS (Network Attached Storage) y soluciones de almacenamiento en red. Los NAS TerraMaster son servidores de almacenamiento diseñados para ayudar a los usuarios a almacenar, administrar y compartir datos de manera centralizada en una red local o a través de Internet. Estos dispositivos se

utilizan en una variedad de entornos, desde hogares y pequeñas empresas hasta entornos empresariales y de servidores.

Las características y funcionalidades de los dispositivos TerraMaster NAS incluyen:

1. *Almacenamiento Centralizado*: Los NAS TerraMaster proporcionan una capacidad de almacenamiento significativa, permitiendo a los usuarios almacenar una amplia variedad de datos, incluyendo documentos, fotos, videos, archivos de música y más.
2. *Acceso Remoto*: Los usuarios pueden acceder a sus datos almacenados en un NAS TerraMaster desde cualquier lugar con una conexión a Internet mediante aplicaciones y servicios proporcionados por TerraMaster.
3. *Gestión de Archivos*: TerraMaster ofrece software de gestión de archivos que facilita la organización y búsqueda de datos, así como la capacidad de compartir archivos y carpetas con otros usuarios.
4. *Seguridad y Protección de Datos*: Los NAS TerraMaster ofrecen funciones de seguridad avanzada, como el cifrado de datos, copias de seguridad automáticas y protección contra malware.
5. *Transmisión Multimedia*: Muchos modelos de TerraMaster incluyen aplicaciones para transmitir contenido multimedia, convirtiéndolos en soluciones de entretenimiento en el hogar.
6. *Escalabilidad*: Los NAS TerraMaster suelen ser escalables, lo que significa que los usuarios pueden agregar unidades de disco adicionales para aumentar la capacidad de almacenamiento según sea necesario.
7. *Aplicaciones de Negocios*: Además de ser utilizados en entornos domésticos, los NAS TerraMaster también se pueden configurar para servir como servidores de archivos,

servidores de impresión, servidores de correo electrónico y más en entornos empresariales.

8. *Comunidad y Soporte*: TerraMaster cuenta con una comunidad activa de usuarios y ofrece soporte técnico para ayudar a los usuarios a configurar y mantener sus dispositivos.

En resumen, TerraMaster NAS es una solución de almacenamiento en red versátil que ofrece una variedad de características y capacidades para satisfacer las necesidades de diferentes usuarios y entornos. Estos dispositivos son conocidos por su facilidad de uso y su relación calidad-precio competitiva en el mercado de los NAS.

5.14.3. Proyecto de Titulación de Galarza Vecilla Héctor Andrés

(Galarza Vecilla, 2023)

En junio del año 2023, como proyecto de titulación para alcanzar el título en tecnólogo en Desarrollo de Software, el ahora tecnólogo Héctor Andrés Galarza Vecilla presentó su proyecto titulado “Implementación de un servidor NAS para el almacenamiento y respaldo de la información generada en el edificio matriz del Instituto Superior Tecnológico Sudamericano Quito”.

Este proyecto, aunque funcionaba, presentaba una interfaz poco agradable, los servicios eran complicados de utilizar, no presentaba muchas opciones y fue implementado en un computador con pocos recursos. Razones por las cuales las autoras prefirieron no utilizarlo e implementar un NAS eficiente, intuitivo en su manejo y con suficientes servicios.

5.14.4. TrueNAS

(Wikipedia contributors, s.f.)

TrueNAS es una plataforma de almacenamiento de datos de código abierto desarrollada por iXsystems. TrueNAS se basa en el sistema operativo FreeBSD y está diseñada para proporcionar soluciones de almacenamiento de alto rendimiento, confiabilidad y escalabilidad para una variedad de aplicaciones y entornos, desde pequeñas empresas hasta grandes centros de datos empresariales.

Las características y funcionalidades clave de TrueNAS incluyen:

1. *Almacenamiento en Red*: TrueNAS es un sistema de almacenamiento en red que admite protocolos de acceso compartido como SMB/CIFS (para entornos Windows), NFS (para sistemas Unix y Linux) y AFP (para entornos Mac).
2. *ZFS como Sistema de Archivos*: TrueNAS utiliza el sistema de archivos ZFS (Zettabyte File System) de código abierto, conocido por su integridad de datos, capacidad de almacenamiento eficiente y características avanzadas de administración de almacenamiento.
3. *Capacidades de Escalabilidad*: TrueNAS es escalable, lo que significa que los usuarios pueden agregar unidades de disco adicionales y ampliar la capacidad de almacenamiento según sea necesario. También es compatible con configuraciones de clústeres y alta disponibilidad.
4. *Cifrado y Seguridad*: TrueNAS ofrece opciones de cifrado de datos para proteger la confidencialidad de los datos almacenados. También incluye funciones de seguridad como la autenticación de usuarios y la administración de permisos.

5. *Servicios Integrados*: Además del almacenamiento de datos, TrueNAS incluye servicios integrados como servidores de archivos, servidores de correo electrónico, servicios de virtualización, copias de seguridad y más.
6. *Gestión Centralizada*: TrueNAS proporciona una interfaz de administración web intuitiva para la configuración y supervisión del sistema.
7. *Soporte Empresarial*: iXsystems ofrece servicios de soporte técnico y mantenimiento para entornos empresariales que utilizan TrueNAS.

TrueNAS se utiliza en una variedad de entornos, desde pequeñas empresas que necesitan un almacenamiento confiable hasta organizaciones empresariales y proveedores de servicios en la nube que requieren soluciones de almacenamiento de alto rendimiento y alta disponibilidad. Además, TrueNAS es una opción popular para la virtualización y la administración de cargas de trabajo de servidores.

Es importante destacar que TrueNAS es una plataforma de código abierto, lo que significa que su código fuente está disponible para su revisión y modificación por parte de la comunidad, lo que contribuye a la transparencia y la personalización de la solución de almacenamiento.

A continuación, se presenta una tabla comparativa entre Synology, TerraMaster y TrueNAS en función de algunas características clave:

Característica	**Synology**	**TerraMaster**	**TrueNAS**
Sistema Operativo	DSM (DiskStation Manager)	TOS (TerraMaster Operating System)	FreeBSD (basado en FreeBSD)
Arquitectura	Hardware y software propietario	Hardware y software propietario	Software de código abierto basado en FreeBSD (TrueNAS CORE)
Almacenamiento en Red	Soporta múltiples protocolos como SMB, NFS, FTP, HTTP, etc.	Soporta múltiples protocolos como SMB, NFS, FTP, HTTP, etc.	Soporta múltiples protocolos como SMB, NFS, FTP, HTTP, etc.
Escalabilidad	Escalabilidad limitada en algunos modelos. Modelos de gama alta ofrecen más opciones.	Escalabilidad limitada en algunos modelos. Modelos de gama alta ofrecen más opciones.	Escalabilidad escalable y alta disponibilidad con clústeres.
ZFS	No utiliza ZFS por defecto. Puede instalar ZFS manualmente.	No utiliza ZFS por defecto. Puede instalar ZFS manualmente.	Utiliza ZFS como sistema de archivos predeterminados.
Capacidad de Cifrado	Soporta cifrado de datos.	Soporta cifrado de datos.	Soporta cifrado de datos.
Soporte Técnico	Ofrece soporte técnico.	Ofrece soporte técnico.	Ofrece soporte técnico. Comunidad activa de código abierto para TrueNAS CORE.
Aplicaciones	Ofrece paquetes de aplicaciones y servicios en su tienda.	Ofrece aplicaciones y servicios adicionales a través de su App Store.	Ofrece servicios integrados como servidores de archivos, correo electrónico, virtualización, etc.

Tabla 4. Comparativa entre plataformas NAS investigadas.
Fuente: las autoras.

Se ha decidido trabajar con Synology como la solución de almacenamiento en red debido a varias razones clave que destacan su excelencia. Synology ofrece una plataforma sólida y confiable respaldada por su sistema operativo DiskStation Manager (DSM), que es conocido por su facilidad de uso y su amplia gama de aplicaciones y servicios disponibles en su tienda. Además, Synology es altamente escalable, lo que permite crecer con las necesidades sin problemas. Su capacidad de cifrado de datos y su soporte técnico sólido también son aspectos cruciales para garantizar la seguridad y el funcionamiento continuo de nuestros datos y servicios. En general, Synology se presenta como una elección versátil y robusta para nuestros requerimientos de almacenamiento y gestión de datos.

6. Desarrollo del Proyecto

El desarrollo e implementación del proyecto se basa en una serie de pasos estratégicos que constituyen la base de su ejecución exitosa. La prioridad se centra en la utilización de dispositivos tecnológicos existentes y el análisis de las instalaciones donde se implementa el proyecto.

6.1. Infraestructura de la red informática del edificio matriz

Para cumplir con el objetivo de evaluar y optimizar la infraestructura actual de red de computadoras del edificio matriz del Instituto Superior Tecnológico Sudamericano de Quito (INTESUD), se realizó un diagnóstico detallado del estado de la red. Este análisis crítico permitió identificar las capacidades, limitaciones y posibles mejoras que facilitarían la integración del portal cautivo y la reconfiguración eficiente de la infraestructura de red, así como el uso de los puntos de acceso Wifi (hotspots).

A través de un proceso riguroso, se revisaron las configuraciones de hardware y software, los esquemas de direccionamiento IP, el cableado estructurado existente, la ubicación de los Access Point que brindan Wifi, así como las políticas de seguridad y los procedimientos de acceso en vigencia.

Con el propósito de proporcionar una visualización clara de la infraestructura actual, se adjuntan gráficos que ilustran la topología de la red LAN del edificio matriz antes de la intervención. Estos gráficos ofrecen una representación esquemática breve de todos los componentes de red, incluyendo enrutadores, switches, puntos de acceso, dispositivos de usuario y conexiones de red cableadas e inalámbricas. Asimismo, detallan la distribución física

y lógica de la red, mostrando cómo los dispositivos están interconectados y cómo fluye el tráfico de datos bajo la configuración preexistente.

El siguiente paso consistirá en usar esta representación gráfica para planificar la reconfiguración y redistribución de los puntos de red, dando paso a la creación de un diseño de red más robusto, escalable y seguro. Este rediseño buscaría no solo satisfacer las necesidades actuales sino también anticiparse a futuros requerimientos, garantizando que la nueva infraestructura soporte de manera efectiva la autenticación de usuarios y el manejo del tráfico de la red de acuerdo con las mejores prácticas y estándares de la industria.

La siguiente figura es una representación general de la red y del servicio de internet con la que contaba el edificio matriz del INTESUD al momento de iniciar con el proyecto:

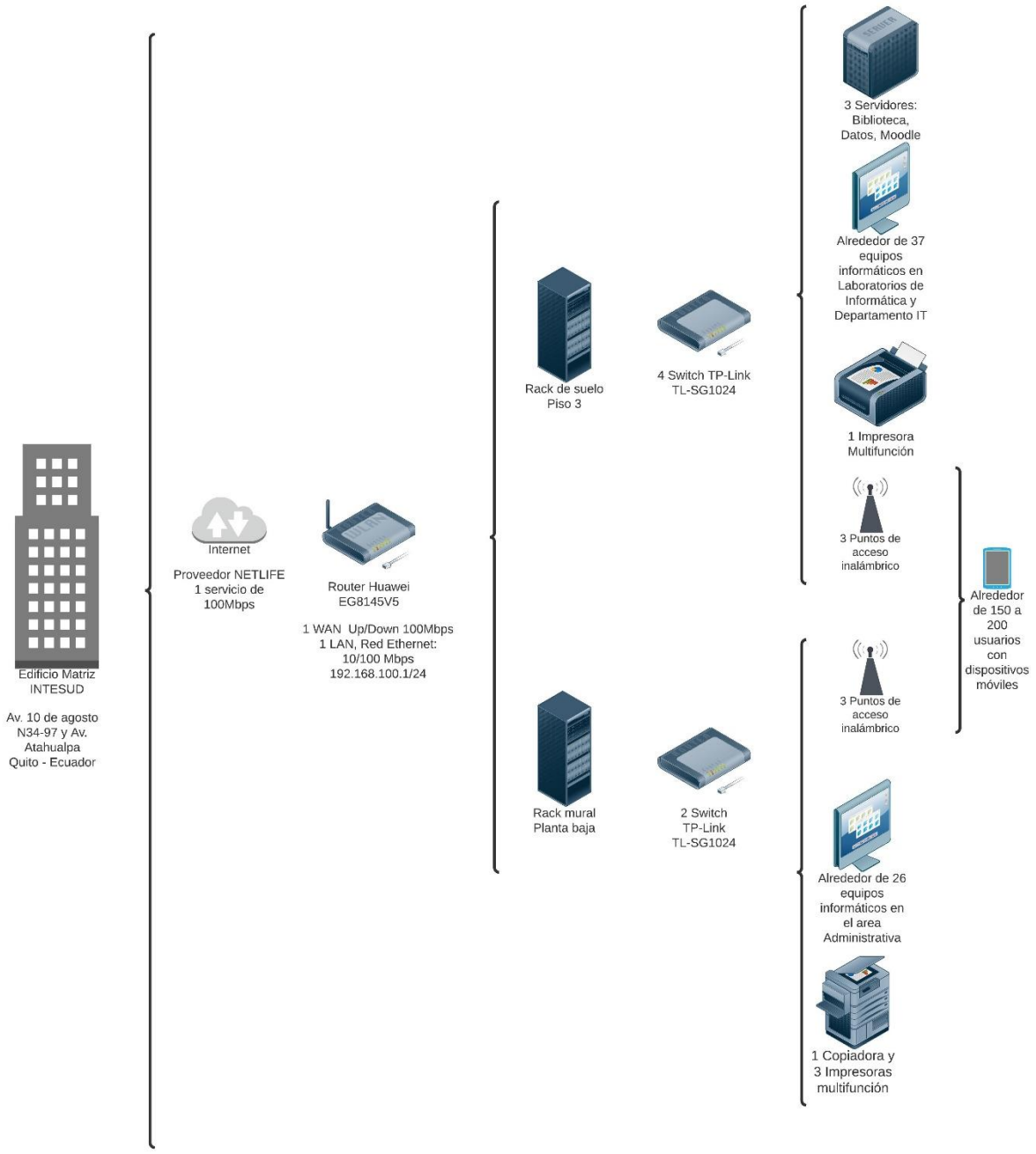


Figura 37. Representación general de la red informática del edificio matriz INTESUD. Fuente: Las autoras.

La gráfica anterior ofrece una perspectiva general de la red LAN del edificio matriz del Instituto Superior Tecnológico Sudamericano Quito (INTESUD). La infraestructura de red se centra en un servicio de Internet provisto por el proveedor MetLife, con una capacidad de 100 Mbps. Este servicio se canaliza a través de un router Huawei EG8145V5, que gestiona una única LAN con una tasa de transferencia de 10/100/1000 Mbps y opera bajo la subred 192.168.100.1/24.

La red está estructurada en dos localizaciones físicas distintas dentro del edificio: un rack de suelo en el tercer piso y un rack mural en la planta baja. Ambos están equipados con switches de 24 puertos TP-Link TL-SG1024, los cuales distribuyen la conectividad a varios dispositivos y áreas.

En el tercer piso, el rack de suelo, ubicado en la oficina de la Coordinación de la Escuela de Desarrollo de Software y Departamento de las Tecnologías de la Información, consta de cuatro switch a los cuales se conecta tres servidores que proporcionan diversos servicios, incluyendo bases de datos y la vieja plataforma Moodle, esenciales para la gestión de la información. Además, hay alrededor de 37 equipos informáticos ubicados en los laboratorios de informática y la oficina de las Tecnologías de la Información (TI), así como una impresora multifunción. Cuatro puntos de acceso inalámbrico desde aquí son distribuidos a los pisos 1, 2, 3 y 4, cuya misión es expandir la cobertura Wifi por piso del edificio matriz, atendiendo a aproximadamente a 150 usuarios con dispositivos móviles.

En la planta baja, el rack de mural, ubicado en un cuarto a lado del área de coordinaciones de Escuela, alberga dos switches que facilitan la conexión de red a aproximadamente 26 equipos informáticos en la zona administrativa, además de una copiadora y tres impresoras

multifunción. Similar al tercer piso, tres puntos de acceso inalámbrico ofrecen conectividad Wifi en esta área incluido el Mezanine ofreciendo wifi alrededor de 26 usuarios.

La siguiente figura representa la configuración de red antes de la implementación del portal cautivo y la optimización de la infraestructura de red. La disposición de red de ese momento, aunque capaz de satisfacer las necesidades básicas de conectividad, no estaba optimizada para el alto tráfico, conexiones simultáneas que superen las 254 conexiones y la gestión de acceso segura que requiere una institución educativa moderna.

Teniendo en cuenta todo lo anterior, la siguiente figura presenta de forma breve y compactada el esquema de red del edificio matriz del Instituto, que como ya se mencionó líneas atrás, muestra una estructura que, si bien estaba funcionalmente operativa, carecía de una organización lógica y cohesiva. Se puede apreciar que la red se origina en un punto centralizado, el router MetLife, que se encarga de distribuir la conexión a Internet a múltiples switches a lo largo de la edificación.

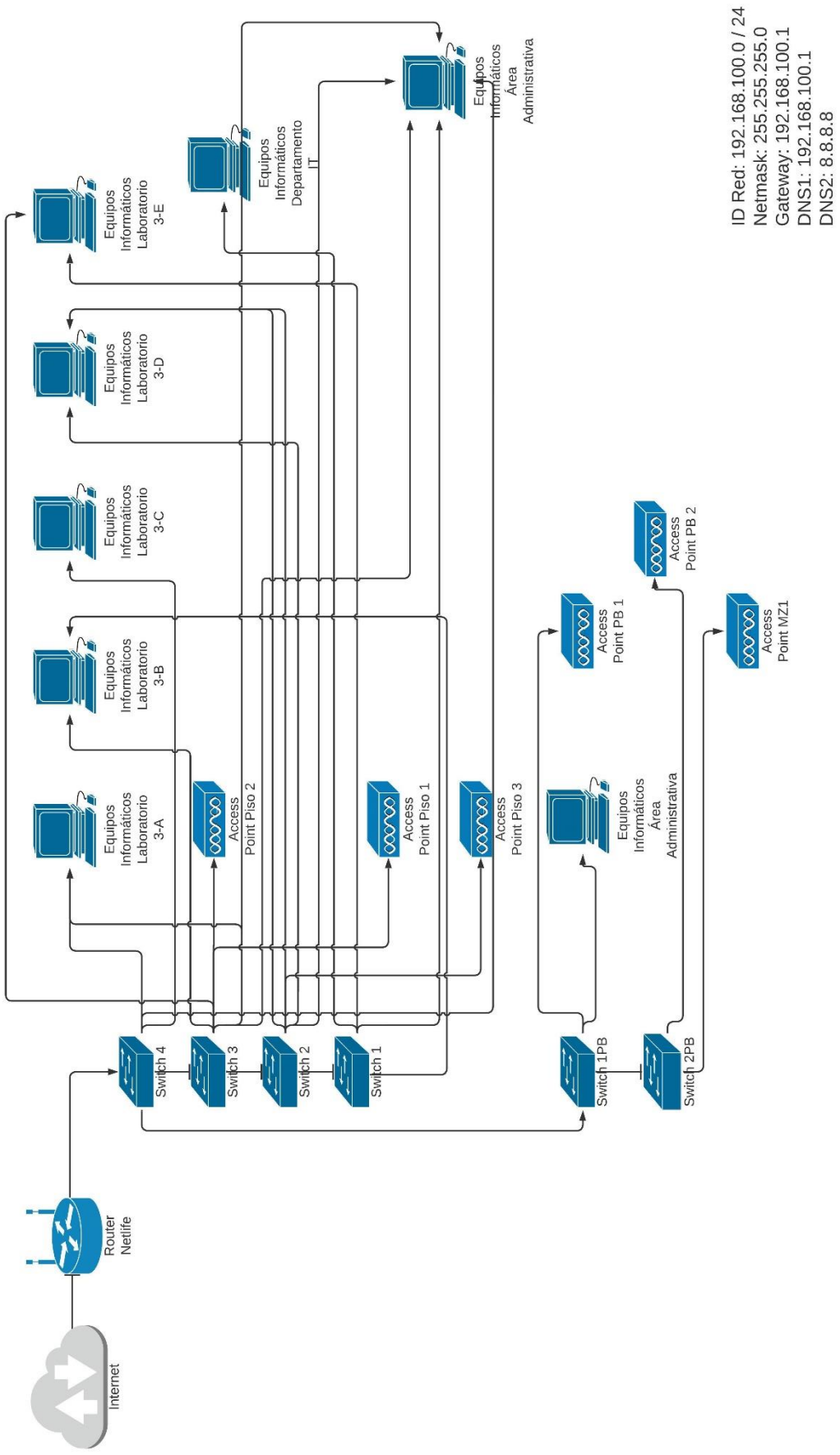


Figura 38. Esquema de red original del edificio matriz del INTESUD.
Fuente: Las autoras.

En el gráfico se observan seis switches numerados, estos conmutadores están conectados en cascada y desde aquí se distribuyen los puntos de red a los distintos pisos y áreas del edificio, incluyendo espacios como los laboratorios informáticos y el área administrativa. Los puntos de acceso inalámbrico, indicados como Access Point, están ubicados en cada piso, conectándose a distintos switches, lo que indica que no había una planificación de red óptima.

Se destaca una práctica de cableado y conexión que no sigue un patrón de organización racional. Por ejemplo, los equipos del Laboratorio Informático 3-D deberían estar conectados a un switch específico y en puertos contiguos para facilitar la gestión y el mantenimiento de la red. Sin embargo, en la realidad, estos se encontraban repartidos aleatoriamente a través de diferentes switches y puertos. Esta falta de estructura sistemática se repite a lo largo de todo el edificio, lo que puede conducir a una serie de complicaciones técnicas como la dificultad en la localización de fallas, la ineficiencia en la administración de la red y el aumento en el tiempo de respuesta para resolver problemas.

El desorden visible en la asignación de conexiones a los switches y la distribución aleatoria de los puertos utilizados, reflejan una implementación que no se alinea con las mejores prácticas en la administración de redes. Este enfoque fragmentado puede resultar en una red con puntos de falla difíciles de diagnosticar, una gestión de tráfico subóptima, y un incremento en el riesgo de problemas de seguridad debido a la complejidad adicional que supone el seguimiento de dispositivos y usuarios en la red.

La intención de presentar la imagen anterior era la de subrayar la necesidad imperante de reestructurar la topología de red existente. Un rediseño buscaría establecer un esquema más ordenado y eficiente, donde cada área o laboratorio esté claramente mapeado a switches

específicos y puertos consecutivos, facilitando así la escalabilidad, la seguridad, el mantenimiento y la resolución de problemas. Este paso es crucial para la implementación exitosa del portal cautivo y para garantizar una red robusta y confiable para la comunidad institucional.

A continuación, se presenta la tabla de los puntos de red registrados en el edificio matriz por las autoras, trabajo que se desarrolló debido a que se conoce que nunca fueron entregados por el contratista en un documento formal, es decir, la Institución al momento de realizar este trabajo, no contaba con la documentación y registro de la infraestructura de red. Al menos se contaba con los puntos de red debidamente identificados en los patch cords, patch panels de los racks y en los puntos de red de pared ubicados en todo el edificio.

TABLAS DE TOMAS DE INTERNET																				
PISO 4	**CÓDIGOS**																		CONEXIÓN	Nº
SIN Access Point	D601																		Switch 1	1
PISO 3	**CÓDIGOS**																			
IT	D554	D555	D556																Switch 1, 2	3
Aula 3A	D501	D502	D503	D504	D505	D506	D507	D508	D509										Switch 1,3,4	9
Aula 3B	D510	D511	D512	D513	D514	D515	D516	D517	D518										Switch 2,4	9
Aula 3C	D520	D521	D522	D523	D524	D525													Switch 1,3	6
Aula 3D	D526	D527	D528	D529	D530	D531	D532	D533	D534	D535	D536	D537	D538	D539	D540	D541	D542	D543	Switch 3,4	18
Aula 3E	D544	D545	D546	D547	D548	D549	D550	D551	D552	D553									Switch 2,3	10
Access Point	D557																			1
DVR	DVR01	DVR02																		2
PISO 2	**CÓDIGOS**																			
Access Point	D401																		Switch 1	1
PISO 1	**CÓDIGOS**																			
Access Point	D301																		Switch 3	1
MEZANINE	**CÓDIGOS**																			
Access Point - Gerencia	D205																		Switch 4	1
Gerencia	D204																		Switch 4	1
Dirección Académica	D206	D207																	Switch 3	2
Sala de Reuniones	D202	D203																	Switch 4	2
PLANTA BAJA	**CÓDIGOS**																			
Marketing	D136	D137	D138																Switch 1PB	3
Biblioteca	D103	D104	D105	D107	D109	D118	D139	D140	D141										Switch 1	9
Secretaría	D110	D112	D113	D114	D115														Switch 1PB	5
Acreditación	D117	D118																	Switch 1PB	2
Recursos Humanos	D119																		Switch 1PB	1
Financiero	D142	D143	D144	D145															Switch 3	4
Coordinaciones	D120	D121	D122	D123	D124	D125	D126	D127	D128										Switch 1PB	9
Profesores	D129	D130	D131	D132	D133	D134													Switch 1PB	6
AdminRed	D111																		Switch	1
Administración	D116																		Switch 2PB	1
Administración	D135																		Switch 2PB	1
Repetidor	D132																		Switch	2

Tabla 5. Puntos de red del edificio matriz y su nomenclatura.
Fuente: Las autoras.

Con ayuda de la tabla anterior se pudo trabajar en el rack principal del tercer piso y reestructurar la topología de red existente al reconectar los puntos de red de forma ordenada y eficiente en los conmutadores. De esta manera ahora cada área y laboratorio está claramente mapeado a switches específicos y puertos consecutivos, facilitando así la escalabilidad, la seguridad, el mantenimiento y la resolución de problemas. Este paso era crucial para la implementación exitosa del portal cautivo y para garantizar una red robusta y confiable para la comunidad institucional.

TABLAS DE TOMAS DE INTERNET																			
PISO 4		**CÓDIGOS**																	
Switch Portal Cautivo	**Puerto**	**8**																	
Access Point		D601																	
PISO 3		**CÓDIGOS**																	
Switch 2	**Puerto**	**7**	**3**	**SW1-7**															
IT		D554	D555	D556															
Switch 4	**Puerto**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**									
Aula 3A		D501	D502	D503	D504	D505	D506	D507	D508	D509									
Switch 4	**Puerto**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**									
Aula 3B		D510	D511	D512	D513	D514	D515	D516	D517	D518									
Switch 5	**Puerto**	**1**	**2**	**3**	**4**	**5**	**6**												
Aula 3C		D520	D521	D522	D523	D524	D525												
Switch 3	**Puerto**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
Aula 3D		D526	D527	D528	D529	D530	D531	D532	D533	D534	D535	D536	D537	D538	D539	D540	D541	D542	D543
Switch 5	**Puerto**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**								
Aula 3E		D544	D545	D546	D547	D548	D549	D550	D551	D552	D553								
Switch Portal Cautivo	**Puerto**	**7**																	
Access Point		D557																	
Switch 1	**Puerto**	**6**	**8**																
DVR		DVR01	DVR02																
PISO 2		**CÓDIGOS**																	
Switch Portal Cautivo	**Puerto**	**5**																	
Access Point		D401																	
PISO 1		**CÓDIGOS**																	
Switch Portal Cautivo	**Puerto**	**3**																	
Access Point		D301																	
MEZANINE		**CÓDIGOS**																	
Switch 1	**Puerto**	**9**																	
Access Point - Gerencia		D205																	
Switch 2	**Puerto**	**2**																	
Gerencia		D204																	
Switch 2	**Puerto**	**19**	**18**																
Dirección Académica		D206	D207																
Switch 2	**Puerto**	**15**	**22**																
Sala de Reuniones		D202	D203																
PLANTA BAJA		**CÓDIGOS**																	
Marketing		D136	D137	D138															
Switch 2	**Puerto**	**20**	**8**	**11**	**9**														
Biblioteca		D103	D104	D105	D107	D109	D118	D139	D140	D141									
Switch 2	**Puerto**	**14**																	
Secretaría		D110	D112	D113	D114	D115													
Acreditación		D117	D118																
Recursos Humanos		D119																	
Financiero		D142	D143	D144	D145														
Coordinaciones		D120	D121	D122	D123	D124	D125	D126	D127	D128									
Profesores		D129	D130	D131	D132	D133	D134												
Switch 1	**Puerto**	**10**																	
Access Point		D111																	
Administración		D116																	
Administración		D135																	
Repetidor		D132																	

Tabla 6. Puntos de red del edificio matriz y su reorganización.
Fuente: Las autoras.

La siguiente figura muestra el trabajo realizado y la nueva distribución de puntos de red, es decir, el nuevo esquema de red del edificio, en donde se aumentó un conmutador más, se “peinó” adecuadamente los patch cord en el rack principal ubicado en el tercer piso, se agrupó adecuadamente los switches y los puntos de red en función de áreas, se agregó un nuevo enrutador con capacidad de manejar VLAN y como se mencionó líneas atrás, todo esto es para lograr una infraestructura de red organizada, escalable y adecuada:

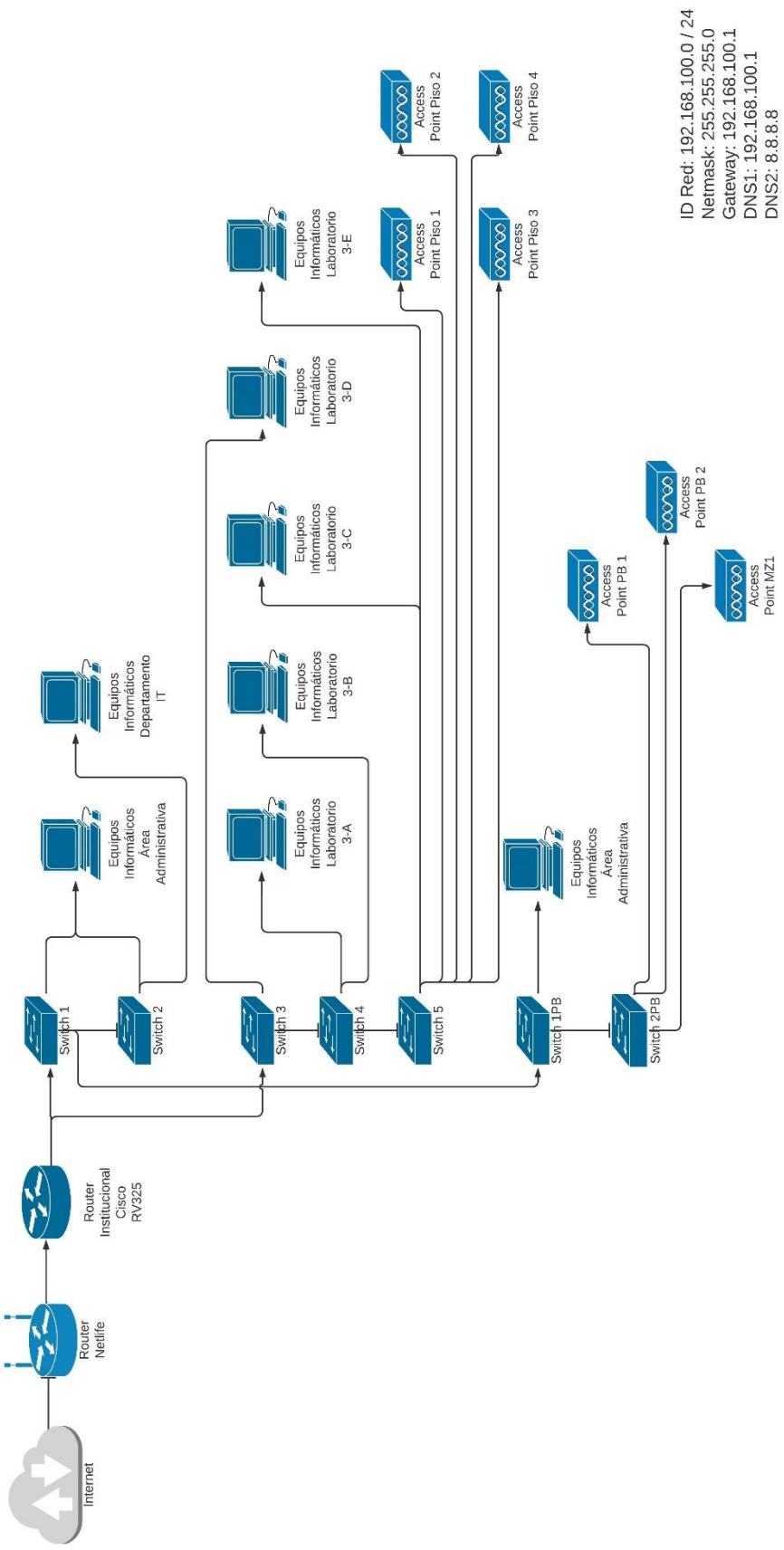


Figura 39. Esquema de red organizada y reconfigurada del edificio matriz del INTESUD. Fuente: Las autoras.

La situación inicial de la red LAN clase C con la subred 192.168.100.0/24 en el edificio matriz del Instituto Superior Tecnológico Sudamericano Quito (INTESUD) planteaba un escenario crítico en términos de escalabilidad y administración de recursos de red, particularmente debido a la limitada cantidad de direcciones IP disponibles que este tipo de red puede ofrecer. Con una máscara de subred /24, la red puede soportar hasta 254 direcciones IP asignables, lo cual es insuficiente al considerar el número potencial de dispositivos concurrentes.

Con aproximadamente 85 equipos informáticos fijos y la posibilidad de que hasta 180 personas lleven uno o más dispositivos móviles que requieren conexión, la demanda excede con creces las direcciones IP disponibles en el rango DHCP (200 arriendos). Este déficit de direcciones llevó a una serie de problemas operativos, tales como la incapacidad de conectar nuevos dispositivos, conflictos de direcciones IP y una sobrecarga general del servidor DHCP.

Además, el tener una única red LAN para todo el tráfico de datos aumenta el riesgo de congestión, lo que puede traducirse en una disminución significativa de la calidad del servicio de Internet. Con muchos dispositivos compartiendo la misma red, el ancho de banda disponible se distribuye entre todos los usuarios, lo que potencialmente podría conducir a velocidades de conexión más lentas, latencia más alta y una disminución general en la eficiencia de la transmisión de datos.

Para cumplir con el objetivo de diseñar y configurar una red de área local virtual (VLAN) en los equipos existentes para segmentar el tráfico de la red y mejorar la seguridad y eficiencia de la red interna, se analizó que separar la red en dos VLAN distintas, una dedicada exclusivamente para el área Administrativa y otra para los Laboratorios y Access Points, puede

mitigar significativamente estos problemas. La segmentación de red a través de VLAN permite una administración más eficiente del ancho de banda y de las direcciones IP, al distribuir la carga entre dos subredes diferentes y potencialmente reducir el tráfico de broadcast. Además, permite aplicar políticas de seguridad más específicas y adaptadas a las necesidades de cada segmento de la red, mejorando la seguridad y el rendimiento general.

Con esta separación, el área Administrativa podría manejar sus operaciones de red de manera más aislada y segura, mientras que los Laboratorios y Access Points disfrutarían de una red más flexible y dinámica, capaz de adaptarse mejor a los patrones de uso de los estudiantes y del personal docente. Esta mejora en la gestión de la red no solo aumenta la cantidad de direcciones IP disponibles para los dispositivos, sino que también optimiza el uso del ancho de banda, ya que cada VLAN puede tener asignado un ancho de banda específico acorde a sus necesidades, garantizando así una mejor experiencia de usuario y un servicio de Internet más estable y confiable.

La siguiente imagen muestra una rediseñada infraestructura de red en el Instituto Superior Tecnológico Sudamericano Quito (INTESUD), en la que se han creado dos VLAN distintas para segmentar y optimizar el tráfico de la red en el edificio matriz.:

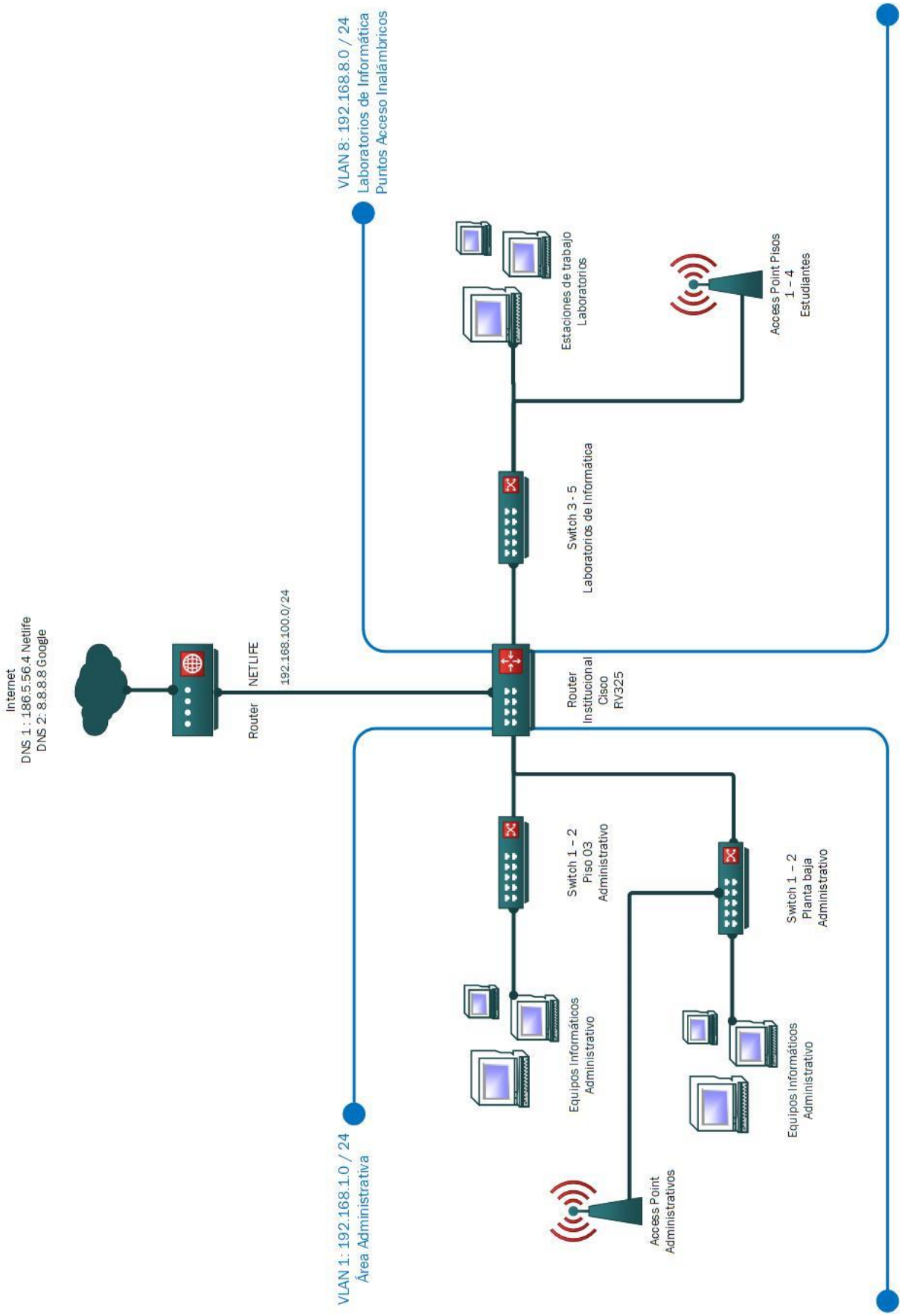


Figura 40. Esquema de red rediseñada con VLAN del edificio matriz del INTESUD.
Fuente: Las autoras.

La imagen anterior muestra la VLAN 1, con la subred 192.168.1.0/24, está designada para el Área Administrativa. Esta VLAN engloba los equipos informáticos administrativos, tanto en el piso 3 como en la planta baja, así como los Access Points administrativos. Esta segmentación asegura que los dispositivos dentro de la administración tengan una red dedicada que permite una comunicación segura y eficiente, reduciendo la posibilidad de congestión y mejorando el rendimiento de la red para las operaciones administrativas críticas.

Por otro lado, la VLAN 8, con la subred 192.168.8.0/24, se ha establecido para los Laboratorios de Informática y los puntos de acceso inalámbrico utilizados por los estudiantes, ubicados en los pisos 1 a 4. Esta separación facilita la gestión del tráfico generado por los estudiantes y los dispositivos utilizados en los laboratorios, permitiendo un uso más eficiente del ancho de banda y proporcionando una conexión más estable para fines educativos y de investigación.

Cada VLAN, al estar configurada en subredes separadas, puede operar de manera independiente, lo cual permite al INTESUD gestionar mejor las direcciones IP y asegurar que haya un suministro adecuado para todos los dispositivos en la red. Esta estructura facilita el control de tráfico, la aplicación de políticas de seguridad diferenciadas y mejora la calidad del servicio al proporcionar ancho de banda según las necesidades específicas de cada grupo de usuarios.

El router central institucional, Cisco RV325, actúa como el corazón de esta configuración, manejando el enrutamiento entre las VLAN y el acceso a Internet, proporcionado por MetLife con un servicio de 100/1000 Mbps y utilizando servidores DNS tanto de MetLife como de Google para la resolución de nombres. La implementación de esta arquitectura de red VLAN

no solo optimiza los recursos de red existentes, sino que también escala adecuadamente para satisfacer la creciente demanda de conectividad dentro del instituto.

Ya determinado las VLAN y las subredes con las que se dividirá el edificio matriz se procede a la configuración del Router Cisco RV325, se aclara que las autoras no configuraron ningún Access Point debido a que esto ya fue realizado por el Departamento IT de la institución, configurando en cada Access Point el SSID por piso, por ejemplo “INTESUD_P02”, y la contraseña institucional del wifi que es “*yosoydelintesud*”; por lo tanto, no se detalla ninguna configuración de los Access Point.

En la siguiente imagen se evidencia las configuraciones realizadas en el router institucional Cisco RV325, en dónde se observa las dos VLAN, con identificación (Id.) 1 y 8, así como la configuración de los servicios de DHCP para cada una de ellas con un rango de 150 IPv4 dinámicas arrendables, 100 IPv4 fijas o estáticas y 4 IPv4 reservadas, para un total de 254 IPv4 por VLAN.

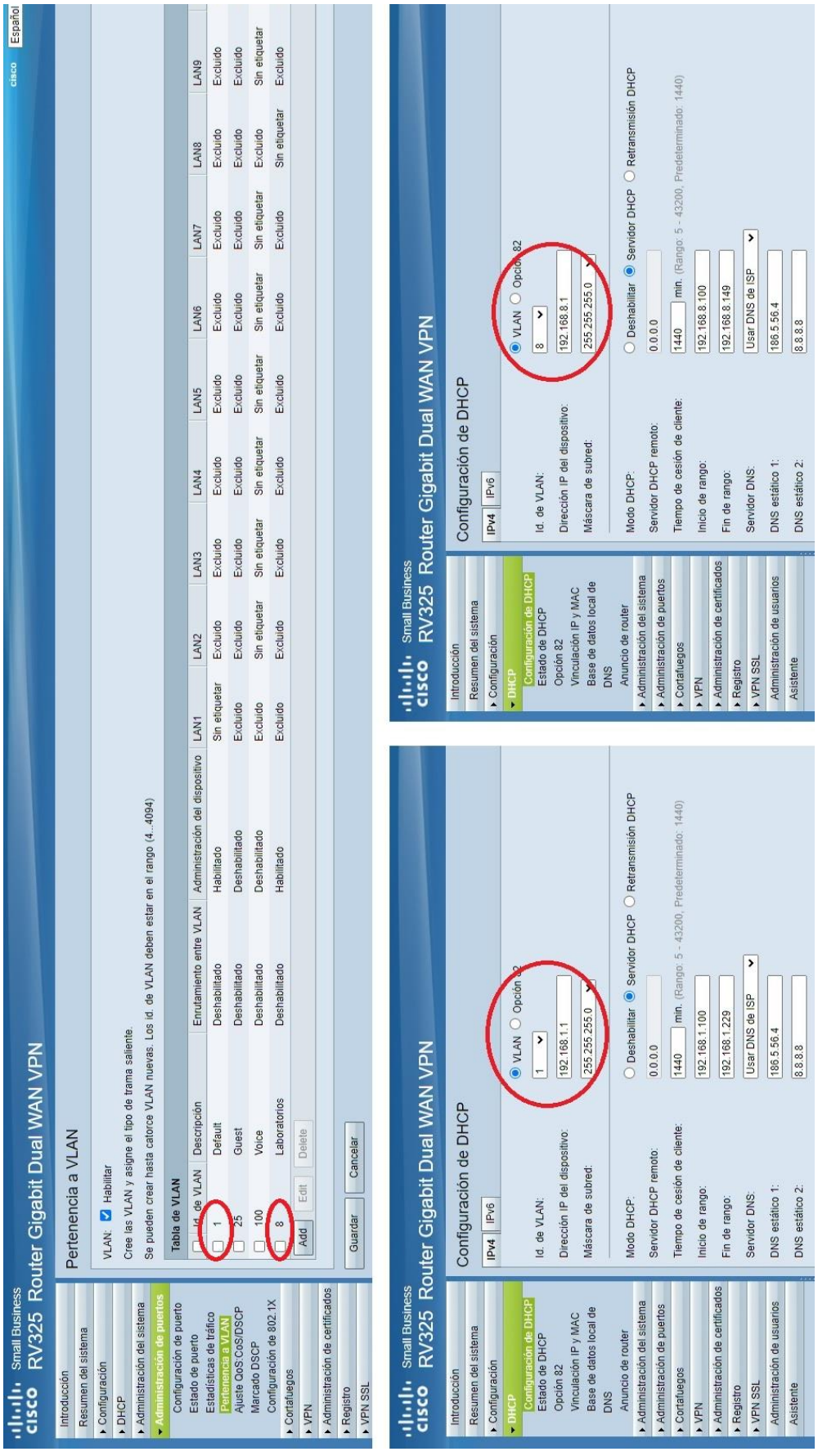


Figura 41. Configuración del Router Cisco RV325.
Fuente: Las autoras.

La siguiente imagen muestra la infraestructura de red del INTESUD con la integración del servidor de portal cautivo en la VLAN 8, que está diseñada para manejar el tráfico de los estudiantes y profesores que se conectan a través de los puntos de acceso inalámbricos distribuidos en los pisos 1 al 4 del edificio.

La VLAN 8, con la subred 192.168.8.0/24, se ha configurado específicamente para separar el tráfico de datos de la red administrativa y ofrecer a los usuarios de esta VLAN una conexión a Internet a través del portal cautivo. Este portal cautivo está alojado en un servidor que utiliza pfSense, un software de firewall y router de código abierto, que brinda funcionalidades avanzadas de seguridad y gestión de tráfico.

El servidor de portal cautivo tiene una dirección IP estática 192.168.7.1, con una máscara de subred 255.255.255.0, y está configurado para ser el gateway y el servidor DNS para los usuarios que se conectan a través de él. Esto significa que todo el tráfico de Internet de los estudiantes y profesores que accedan a la red a través de los puntos de acceso inalámbricos será gestionado y filtrado por el portal cautivo, proporcionando una capa adicional de seguridad y control sobre quién y cómo se utiliza la red.

La red del portal cautivo, identificada con la subred 192.168.7.0/24, está dedicada exclusivamente al tráfico que pasa a través del portal cautivo, lo que simplifica la administración de la red y mejora la seguridad, ya que todo el tráfico puede ser monitoreado y controlado centralmente. Los estudiantes y profesores se autentican en el portal antes de obtener acceso a Internet, lo que permite una gestión eficiente de los usuarios y proporciona estadísticas sobre el uso de la red.

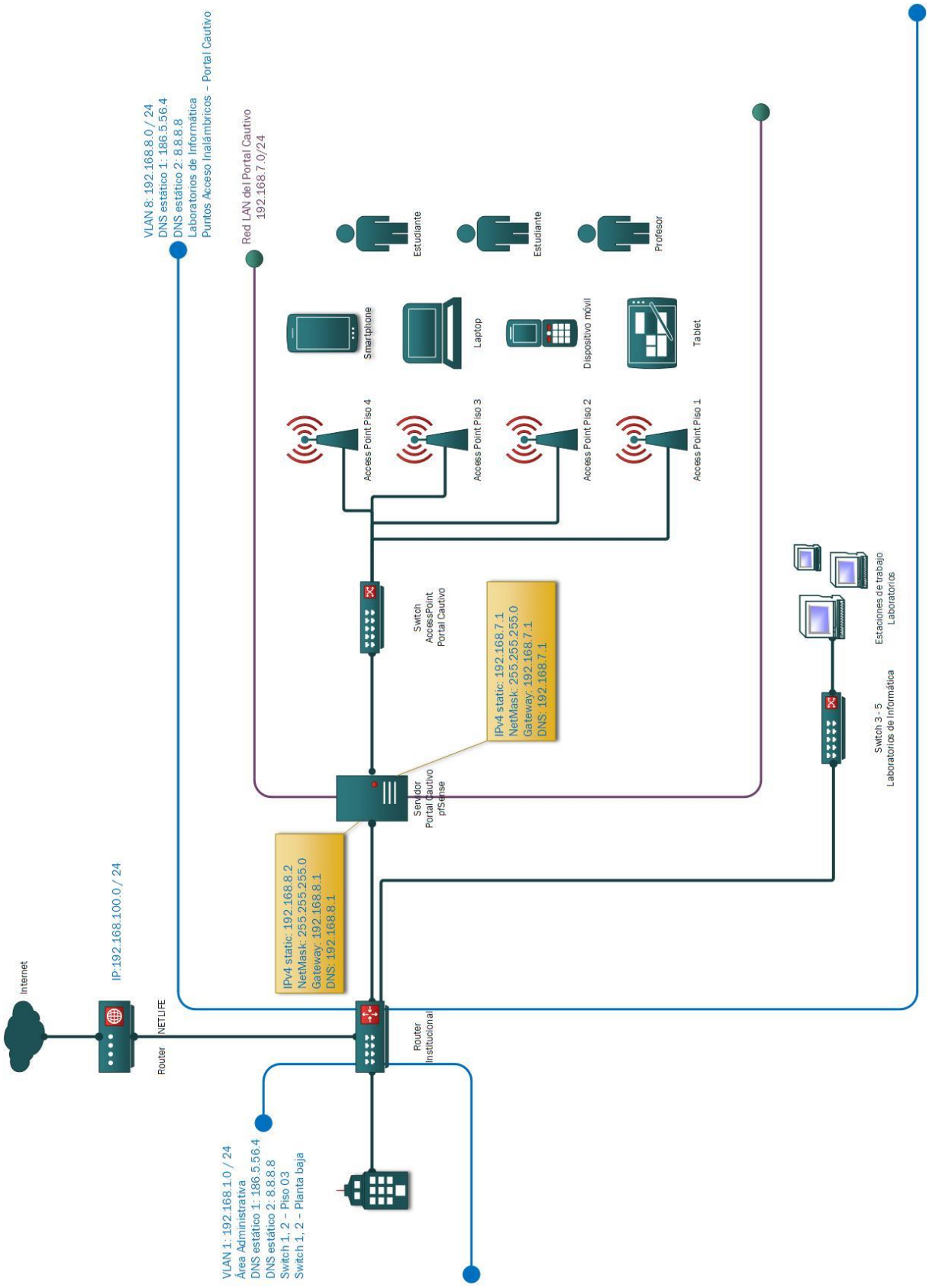


Figura 42. Infraestructura de red con Portal Cautivo del edificio matriz del INTESUD.
Fuente: Las autoras.

Como se puede observar en la siguiente imagen se muestra las características y direcciones IP del servidor Portal Cautivo pfSense, y sus respectivas conexiones con su red WAN (que corresponde a la VLAN 8 de la Institución) y su red LAN, a las que pertenecen los Access Point.

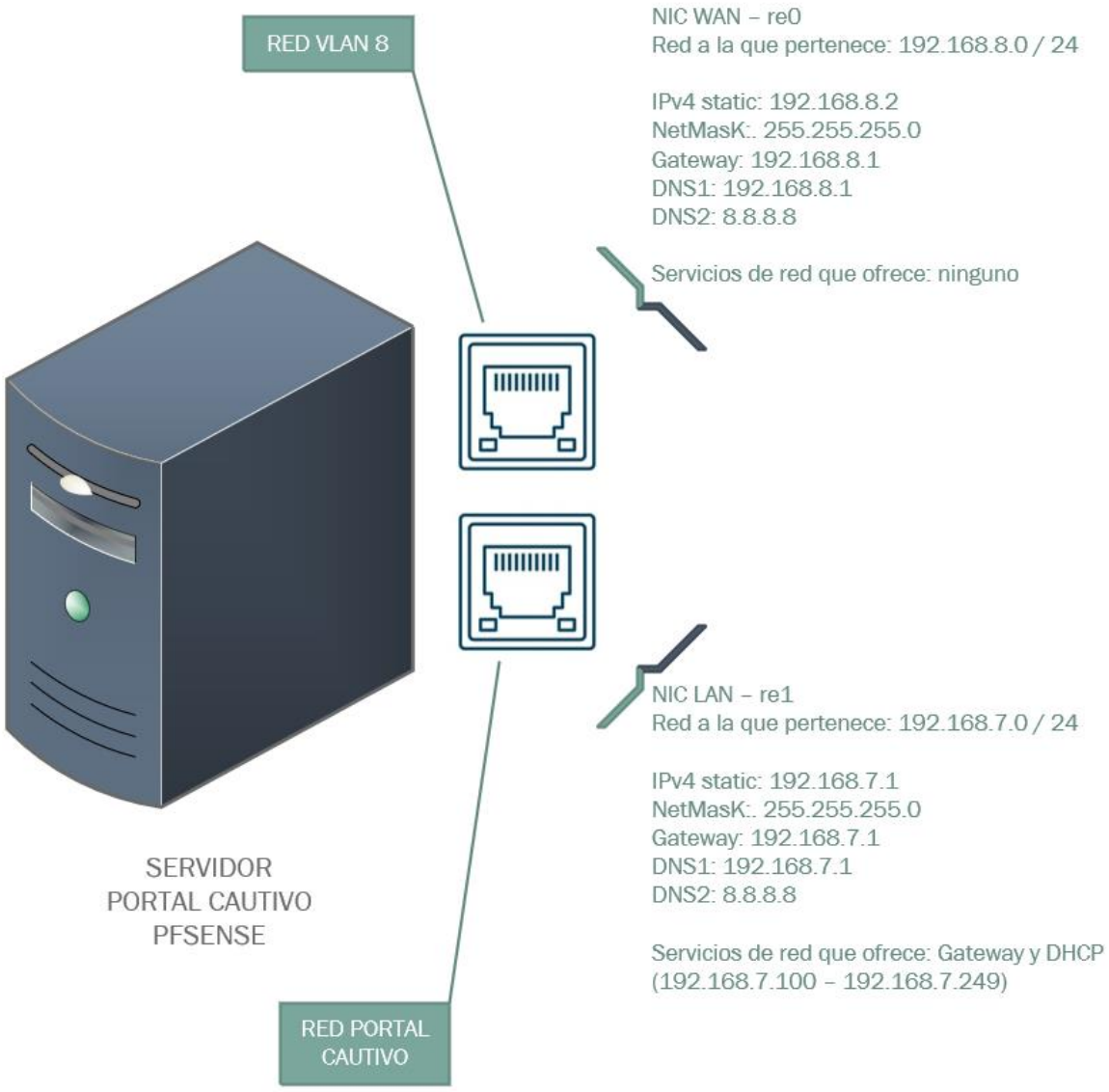


Figura 43. Diagrama conexiones de red del servidor Portal Cautivo pfSense.
Fuente: Las autoras.

La implementación de este sistema ayuda a asegurar que solo los usuarios autorizados tengan acceso a la red, previene el acceso no autorizado y mejora la experiencia del usuario al ayudar a evitar la congestión de la red. Además, al tener un control más estricto sobre las conexiones a la red, el instituto puede garantizar un uso más eficiente del ancho de banda, asignando recursos de red de manera más efectiva y mejorando así la calidad del servicio para todos los usuarios.

6.2. Portal Cautivo pfSense

Para cumplir con el objetivo de seleccionar, instalar y configurar el software apropiado para gestionar el portal cautivo, en el punto "5.12.4. Comparación de pfSense vs otros portales *cautivos*", de este mismo trabajo, se explica que la selección de pfSense como la solución de Portal Cautivo, está fundamentada por ser un software libre y con la capacidad de manejar váuchers. Además, pfSense permite implementar un Portal Cautivo altamente personalizable, lo que significa que se puede ofrecer a los usuarios una experiencia de inicio de sesión segura y fluida en la red Wifi de la institución.

La función de manejo de váuchers es excepcional, permitiendo generar y administrar fácilmente códigos de acceso temporales e inclusive si fuera necesario de pago para algunos usuarios. Esto es esencial para el entorno del edificio matriz, ya que brinda un control completo sobre quién accede a la red y cuándo. En combinación con sus sólidas capacidades de firewall y enrutamiento, gratuidad, pfSense se destaca como la elección perfecta para la red haciéndola segura y brindando un acceso gestionado de manera eficiente a la comunidad institucional.

Tras la explicación anterior y la infraestructura de red establecida, se procedió a instalar pfSense en el servidor que se tenía disponible y que fue facilitado por el Departamento IT de la institución. Este cumple con los requisitos recomendados:

- Procesador: mínimo 500 MHz, se tiene de 1.5GHz.
- Memoria RAM: mínimo 1 GB de RAM, se tiene de 4GB.
- Disco duro: al menos 8 GB de espacio libre, se tiene de 512GB.
- Tarjetas de interfaz de red (NIC): Funciona con dos NIC, se cuenta con cuatro.

Es importante destacar que pfSense se presenta como un sistema operativo de código abierto basado en FreeBSD, diseñado para funcionar como portal cautivo.

Posterior, se configuran las direcciones IP de las tarjetas de red LAN y WAN como de detalló en la figura anterior.

Instalado y configurado pfSense y su servicio de portal cautivo, se puede acceder a la página de inicio de sesión por defecto con usuario general y sin contraseña. Se busca utilizar váuchers para el acceso con un inicio de sesión rápido y seguro.

De manera estándar se permitirá acceder a internet al hacer clic directamente en el botón *Login*. La siguiente figura muestra el diseño de la página principal de “login” (log in – ingreso) del portal cautivo:

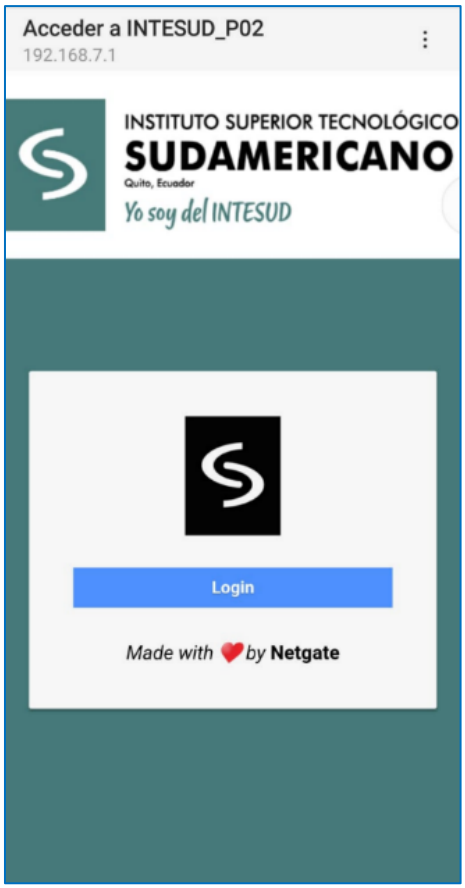


Figura 44. Pantalla de inicio de ingreso del Portal Cautivo.
Fuente: Las autoras.

6.2.1. Descarga de pfSense

A continuación, se presentan las figuras que muestran la página oficial de pfSense, desde donde se puede descargar la imagen ISO. También se describe el proceso para convertir una unidad USB en un dispositivo bootable, esencial para ejecutar el programa en el servidor donde se implementará.

Paso 1: Se descargar la imagen ISO de pfSense desde su página oficial, teniendo en cuenta las características que el hardware soporta, como se muestra en la siguiente figura:

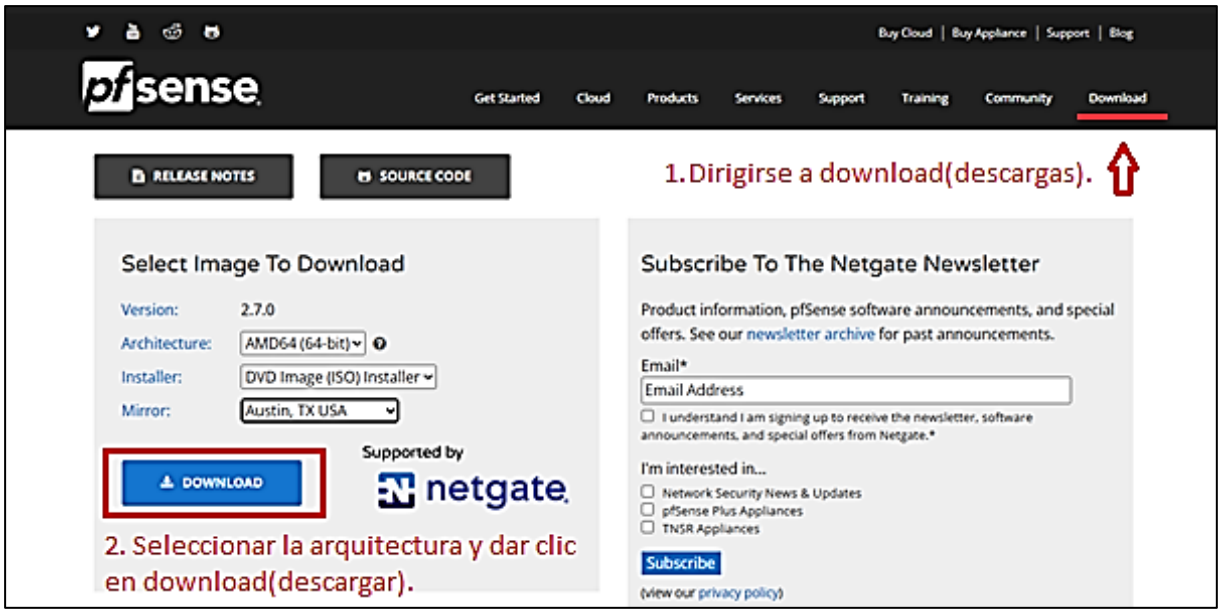


Figura 45. Descarga de la imagen ISO de pfSense.
Fuente: (Pfsense, s.f.)

Paso 2: Se utiliza el programa Rufus como una herramienta para convertir la una unidad de memoria USB en arrancable (bootable), como se muestra en la siguiente figura:

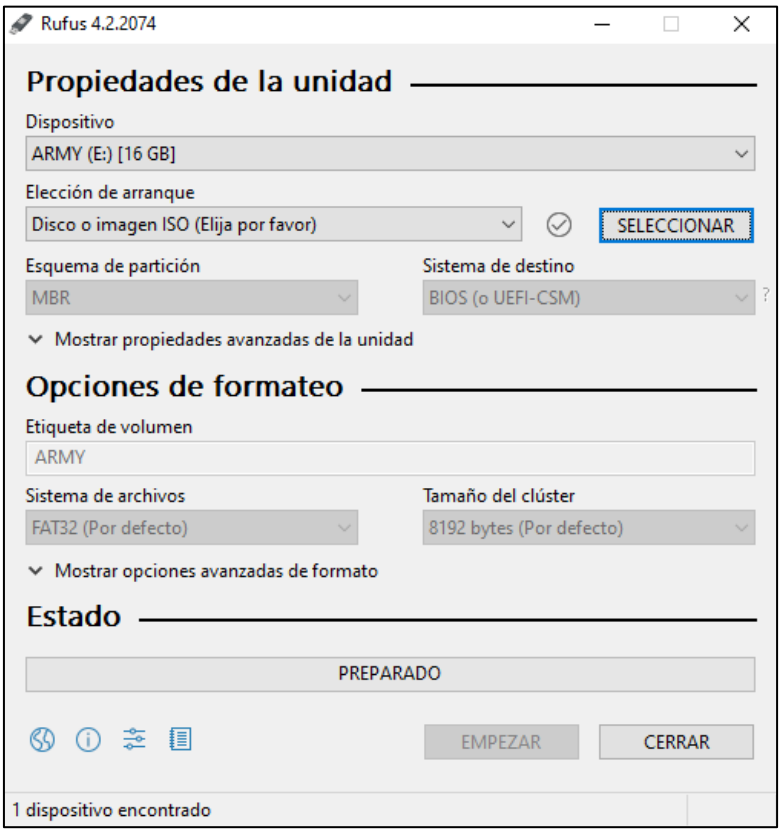


Figura 46. Programa para crear medios USB de arranque.
Fuente: (Rufus, s.f.)

Paso 3: Para arrancar desde la unidad USB booteable, se la conecta al servidor. Después, se configura la BIOS y se accede al *Boot Menu* para seleccionar la unidad USB correspondiente. De esta manera, se podrá continuar con la instalación, siguiendo el proceso que se muestra en la siguiente figura:

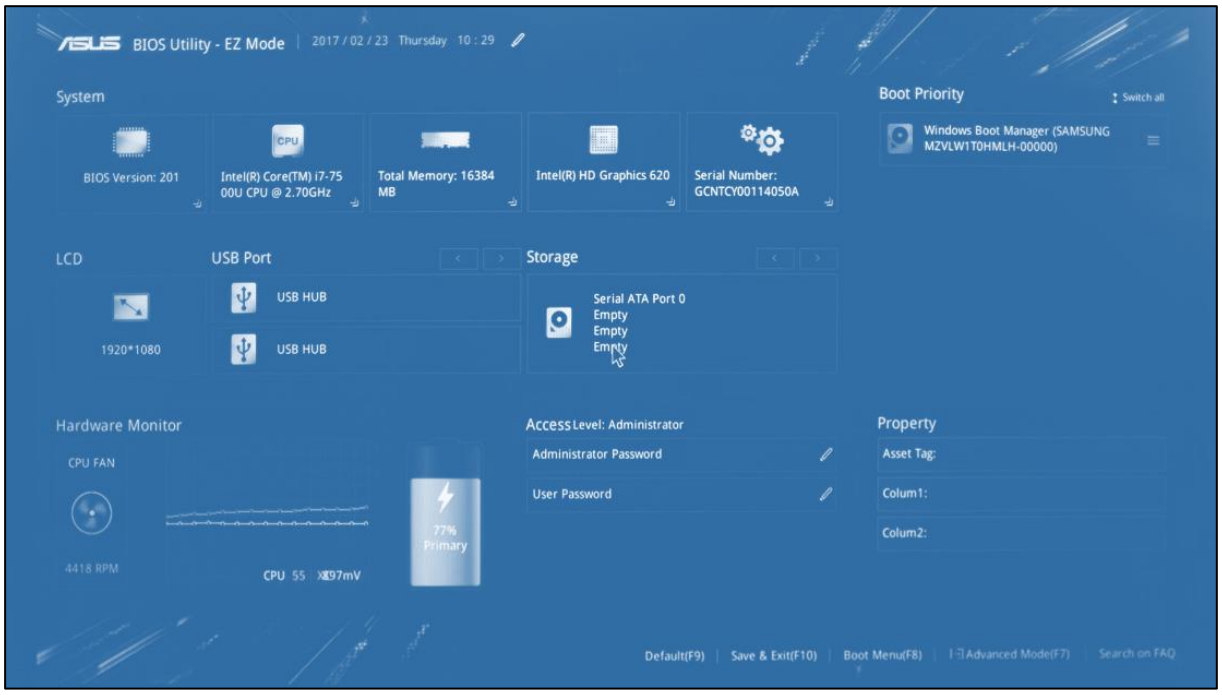


Figura 47. Configuración de la UEFI (o BIOS) para arrancar la PC por USB.
Fuente: (asus, s.f.)

Paso 4: Se inicia la instalación y configuración del software pfSense en el computador que sirve de servidor del Portal Cautivo. Durante el proceso de instalación, se presentan en pantalla las siguientes figuras, iniciando con el de "Aviso de derechos de autor y distribución", al cual se procederá a *aceptar*. Este paso se muestra detalladamente en la siguiente figura:

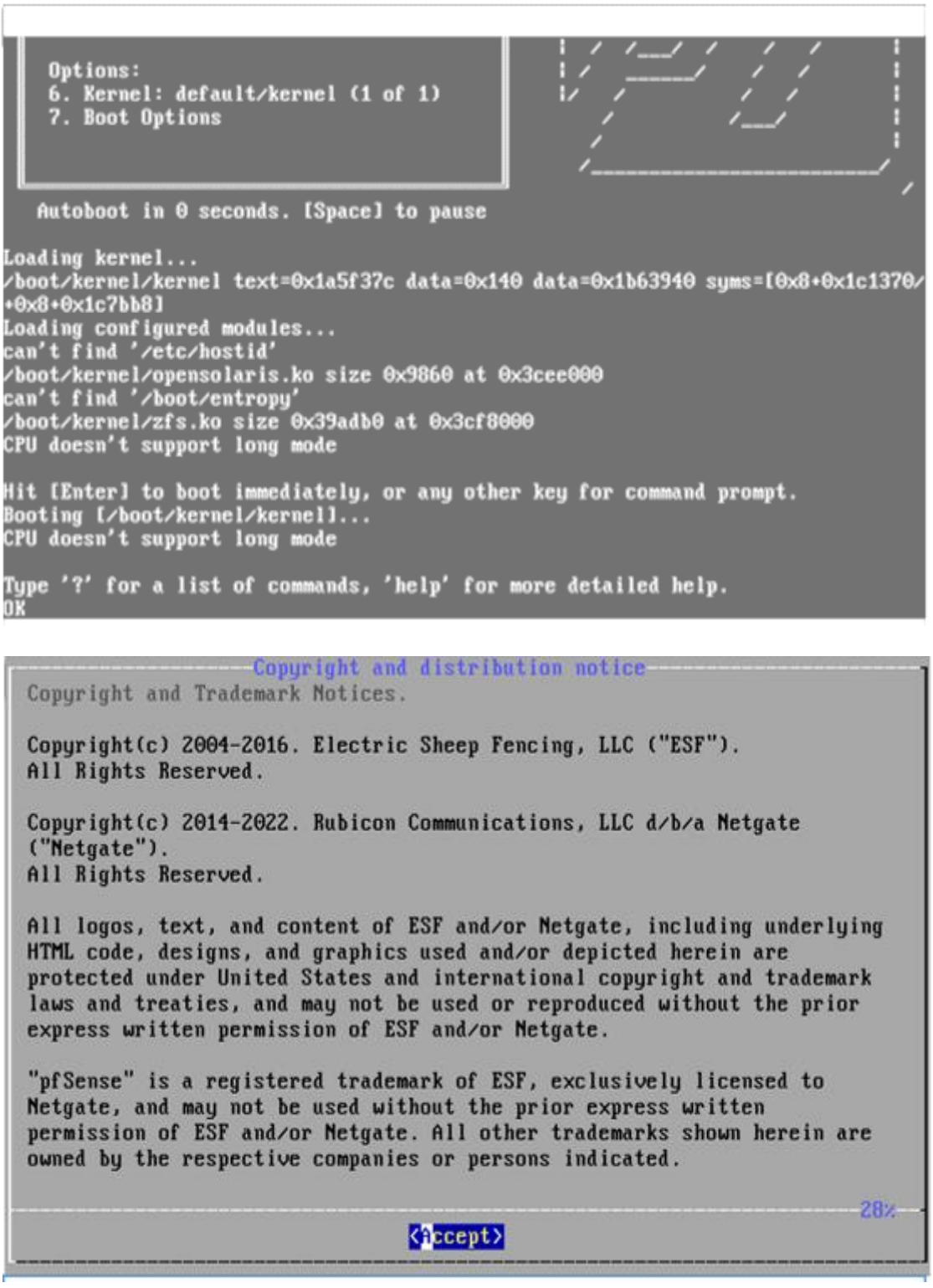


Figura 48. Instalación y configuración del programa pfSense, pantalla de inicio.
Fuente: Las autoras.

6.2.2. Instalación de pfSense

A continuación, se muestran una serie de figuras que explican el paso a paso de la configuración inicial. Cada figura va acompañada de una explicación detallada sobre los distintos controles y funciones que componen la configuración de pfSense.

Paso 1: Al usuario se le presenta una ventana en la cual se le solicita seleccionar el idioma del teclado que está utilizando. Sin embargo, en esta ocasión, decide mantener la configuración predeterminada, como se muestra en la figura:

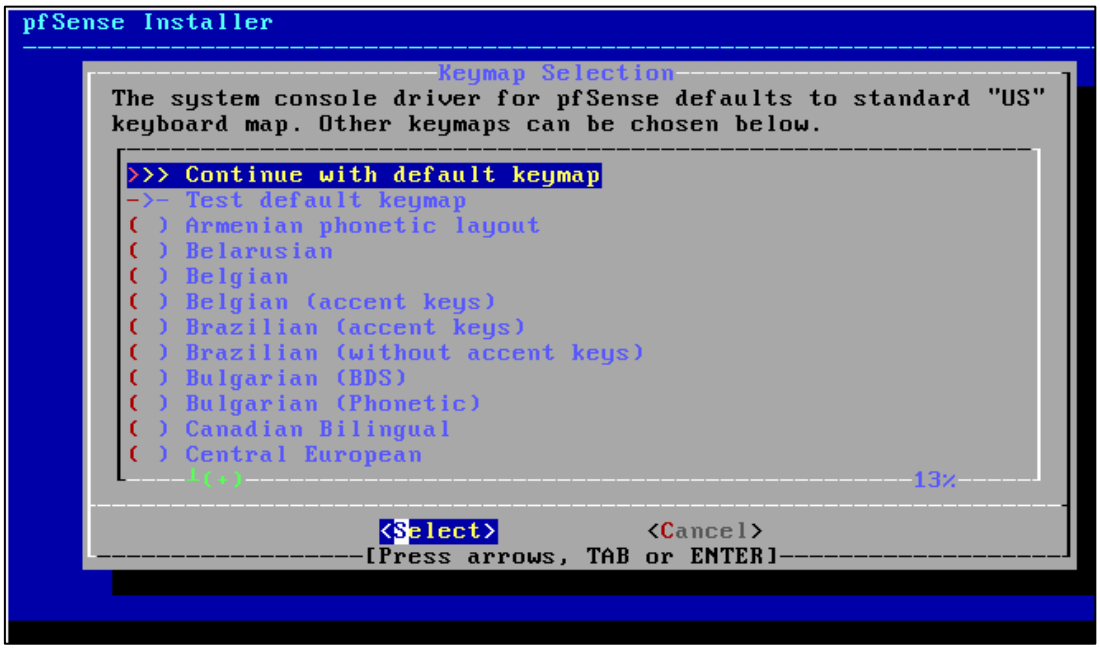


Figura 49. Instalación de pfSense, configuración de idioma de teclado.
Fuente: Las autoras

Paso 2: Se realiza la partición del disco y se elige la opción (UFS) BIOS. La elección entre (UFS) BIOS y (UFS) UEFI depende del tipo de computadora que se esté utilizando. En las computadoras antiguas, se opta por (UFS) BIOS; en las modernas, se prefiere (UFS) UEFI. Esta decisión se basa en las especificaciones de cada computadora, como se muestra en la figura 50.

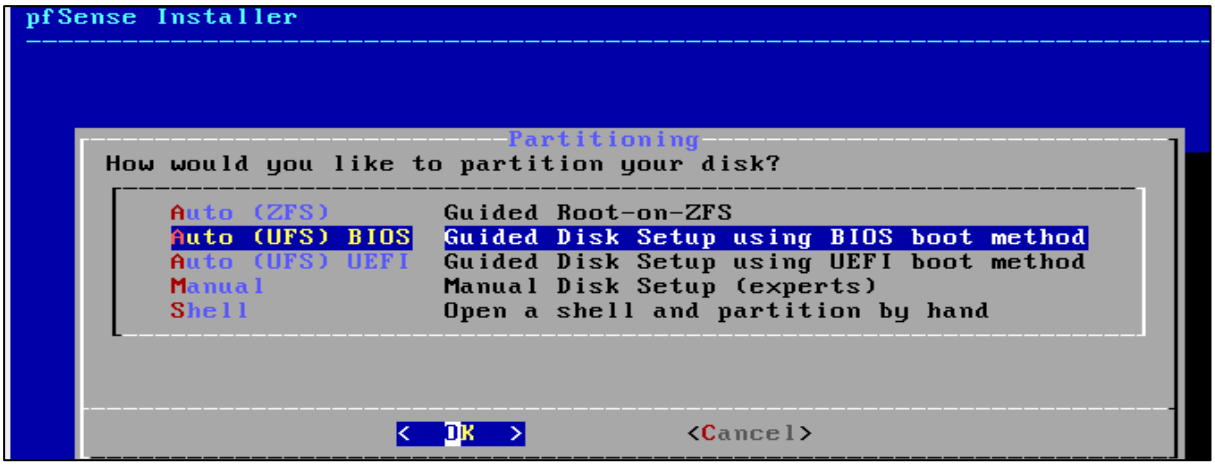


Figura 50. Instalación de pfSense, particiones de disco.
Fuente: Las autoras.

Paso 3: Se espera el proceso de instalación, como se muestra en la figura 51.

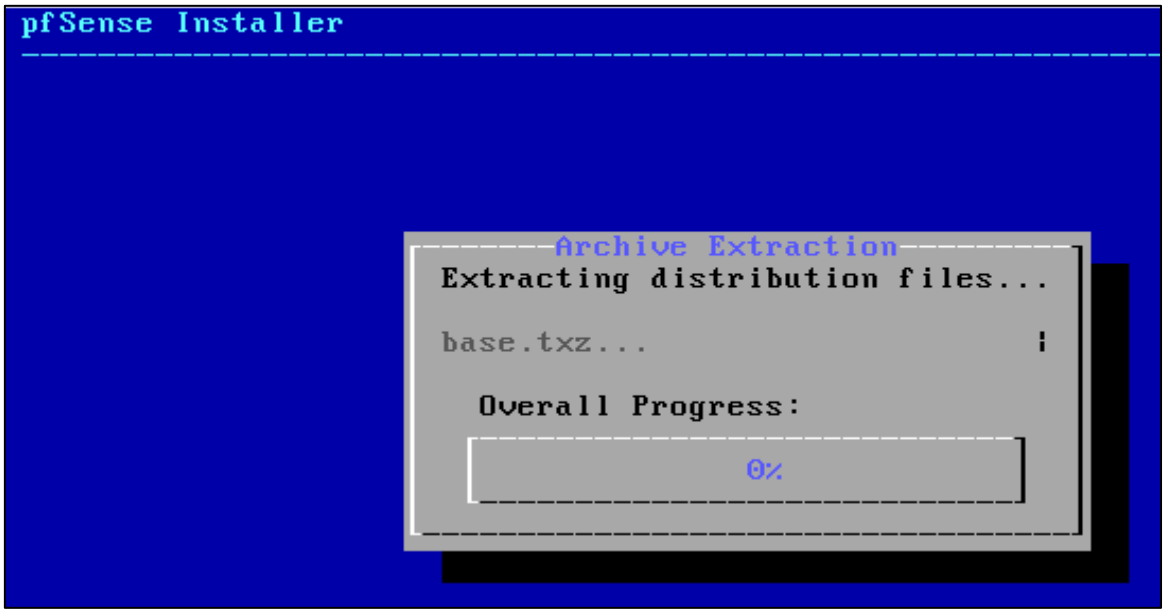


Figura 51. Instalación de pfSense, barra de progreso de la instalación.
Fuente: Las autoras.

Paso 4: En la pantalla, se presentará la opción de elegir una configuración avanzada, en este caso, se debe seleccionar “No”, tal como se muestra en la figura 52.

Figura 52. Instalación de pfSense, manual de configuración.
Fuente: Las autoras.

Paso 5: La instalación termina, informando al usuario que se debe reiniciar el sistema. Para realizar esta acción, se debe seleccionar la opción “Reboot” y retirar la unidad USB, según se muestra en la figura 53.

Figura 53. Instalación de pfSense, mensaje de instalación exitosa.
Fuente: Las autoras.

Paso 8: Para confirmar la correcta instalación de pfSense, se visualizará en pantalla la información concerniente a la WAN, LAN y otras opciones de configuración, tal como se muestra en la figura 54.

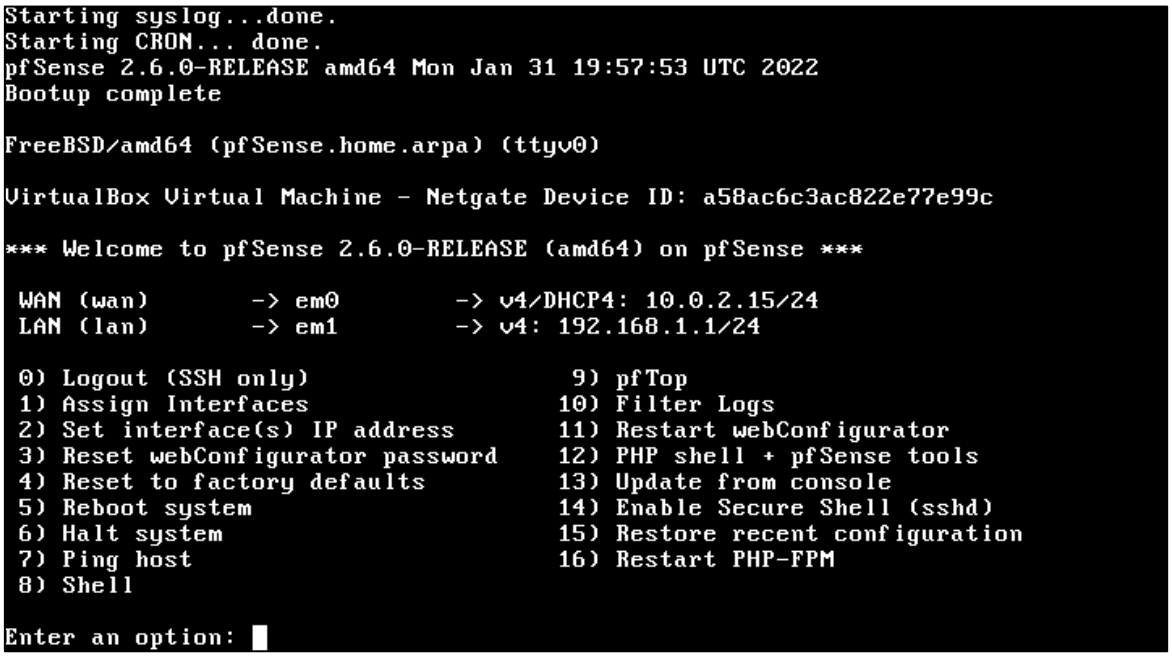


Figura 54. Terminal de configuración de pfSense en el servidor.
Fuente: Las autoras.

6.2.3. Configuración de pfSense

Una vez instalado en el servidor, el programa requerirá personalización y configuración del portal cautivo a través de una interfaz gráfica. En esta fase, se permitirá establecer la configuración de la dirección IP para habilitar la conexión y permitir una administración precisa de los datos de los estudiantes.

A continuación, se detallará los pasos de personalización:

Paso 1: Tras la instalación de pfSense, el usuario debe acceder a la página de inicio utilizando la IP 192.168.1.1. Puede que aparezca una advertencia de conexión “no privada” “debido a un certificado automático. Esta advertencia no afecta la privacidad. El usuario debe hacer clic en “Avanzado”, y así aparecerá la página principal de pfSense, como se muestra en la figura 55.

Figura 55. Configuración de pfSense, ingreso por PC cliente al modo gráfico de configuración, vía IP utilizando un navegador web.
Fuente: Las autoras.

Paso 2: En la siguiente figura, se observa la página de inicio de sesión, en la cual se utilizan las credenciales preestablecidas, es decir, “Admin” como nombre de usuario y “pfSense” como contraseña, como se muestra en la figura 56.

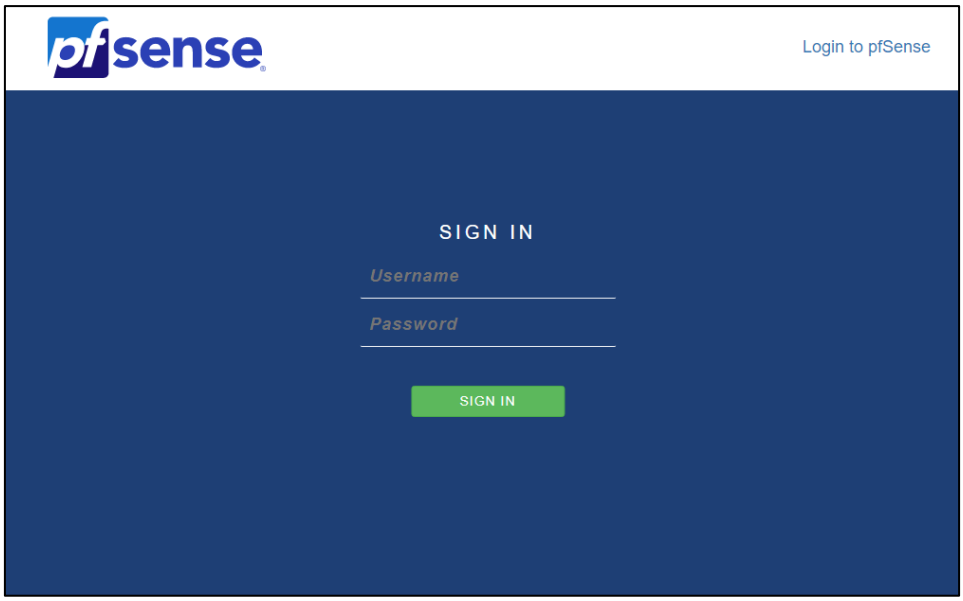


Figura 56. Configuración de pfSense, pantalla de ingreso al modo de configuración gráfica de pfSense. Fuente: Las autoras.

Paso 3: La página de bienvenida aparece en pantalla, luego se requiere hacer clic en el botón "Next". Esta acción permite personalizar varios aspectos según las necesidades, como cambiar la contraseña y el nombre de usuario, además de ajustar otros datos relevantes, tal como se muestra en la figura 57.

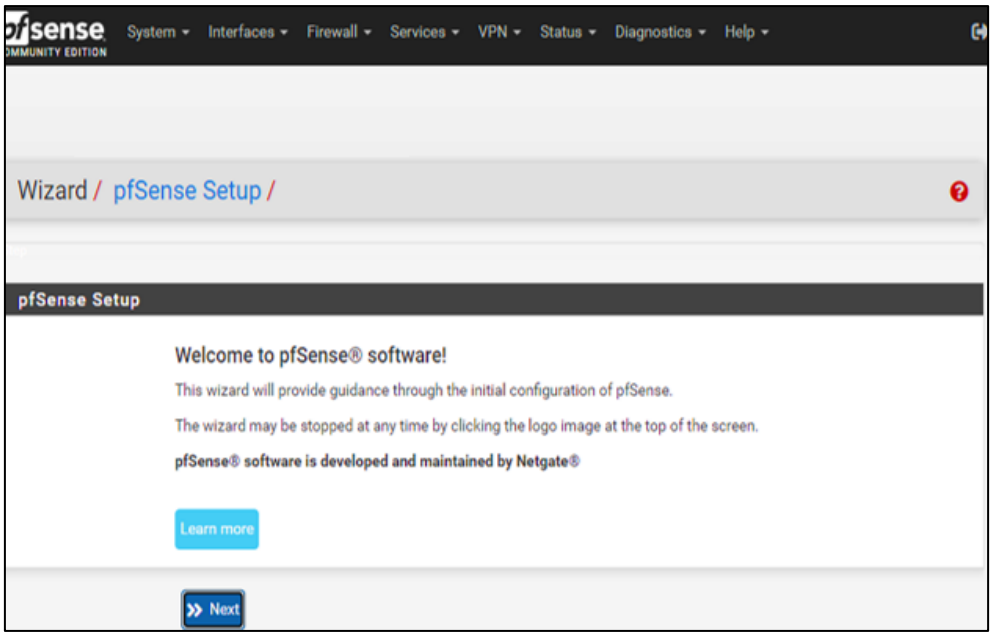


Figura 57. Configuración de pfSense, pantalla de inicio de bienvenida al dashboard de pfSense. Fuente: Las autoras.

Paso 5: El Dashboard servirá como la pantalla principal que desplegará todos los datos relevantes del servidor, incluyendo el nombre, credenciales web, detalles del sistema, BIOS, DNS, estado de la memoria y particiones del disco. También presentará una tabla gráfica para visualizar en tiempo real el consumo de datos de las redes LAN y WAN, permitiendo así la monitorización detallada de la actividad de la red.

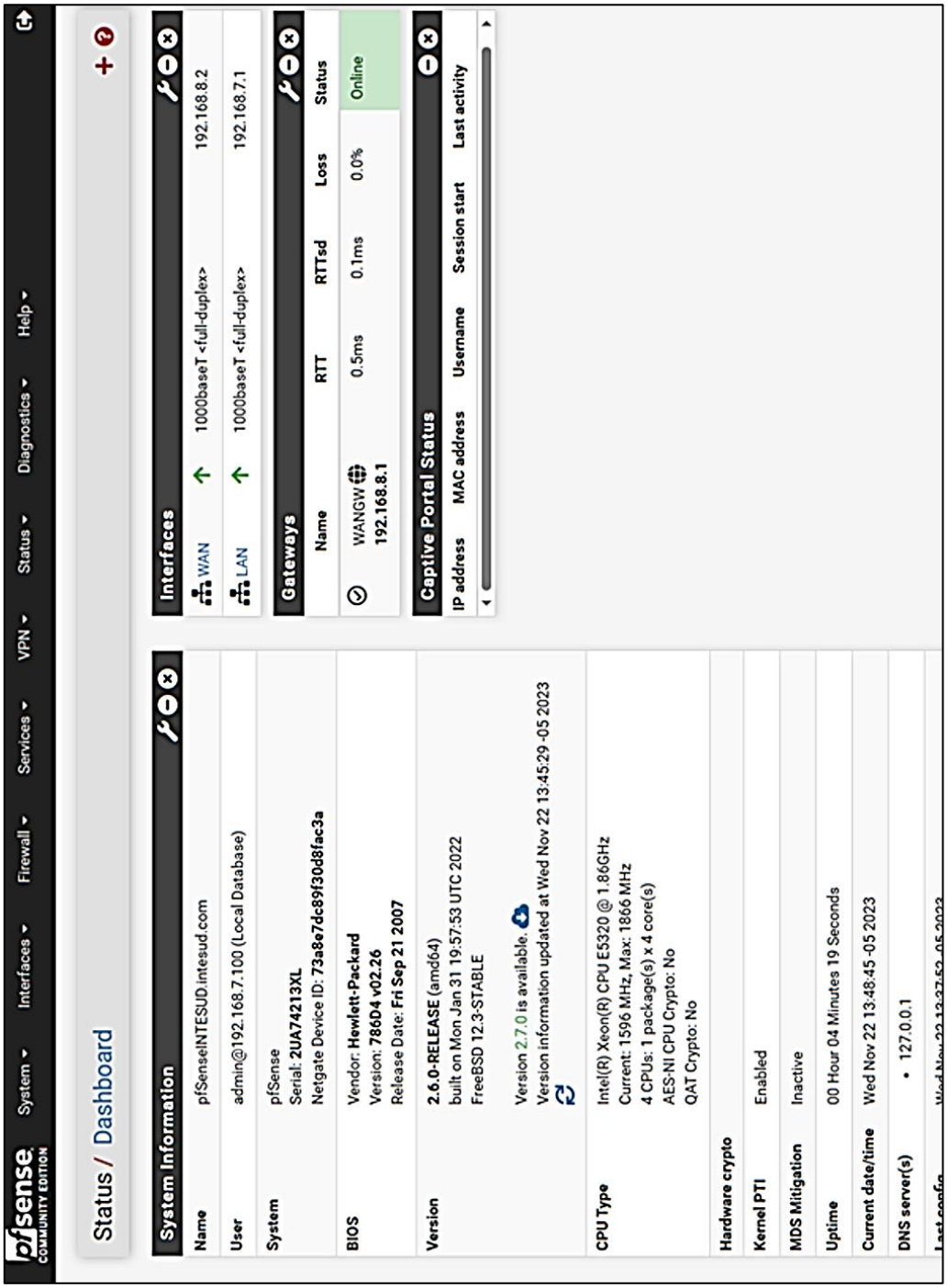


Figura 58. pfSense Dashboard.
Fuente: Las autoras

Paso 4: Se procede con el cambio del nombre del host a “PortalCautivoINTESUD” y la configuración del dominio para la red local. Es de suma importancia la inclusión de servidores DNS, tales como los proporcionados por Google con las direcciones “8.8.8.8” y “8.8.4.4”. En la configuración de la opción “DNS Resolution Behavior”, se establecerá el método de resolución de las solicitudes DNS. Para concluir, se empleará un servidor DNS local en la dirección 127.0.0.1, el cual guardará las solicitudes DNS en su caché interna. En caso de no hallar la información en la caché local, el servidor direccionará las solicitudes a servidores DNS remotos para su resolución, tal como se muestra en la figura 59.

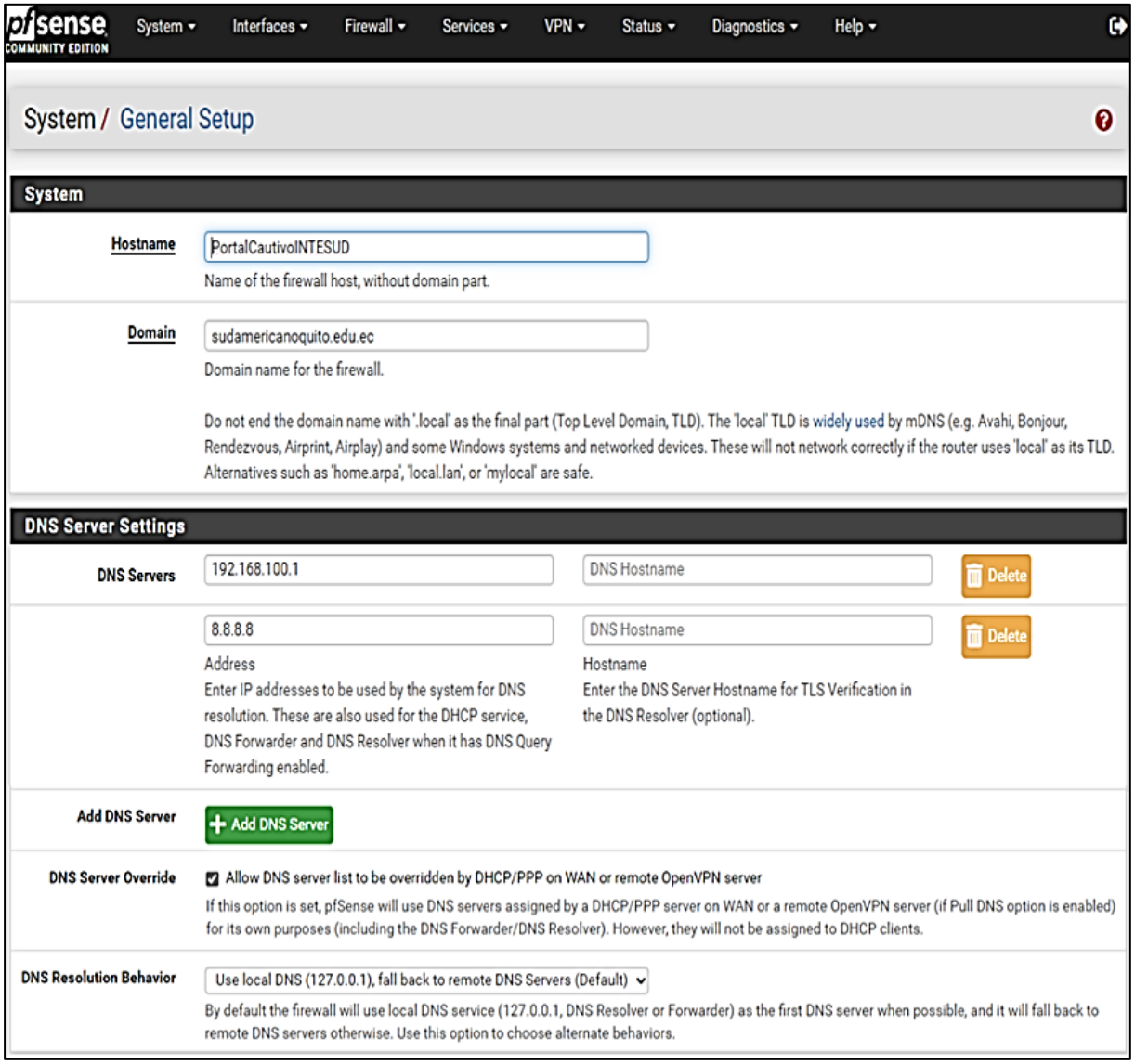


Figura 59. pfSense, pantalla de configuración general.
Fuente: Las autoras.

Paso 5: Se necesita realizar ajuste del horario basado en la ubicación geográfica. El resto de las configuraciones se las dejará por defecto, tal como se detalla en la figura 60.

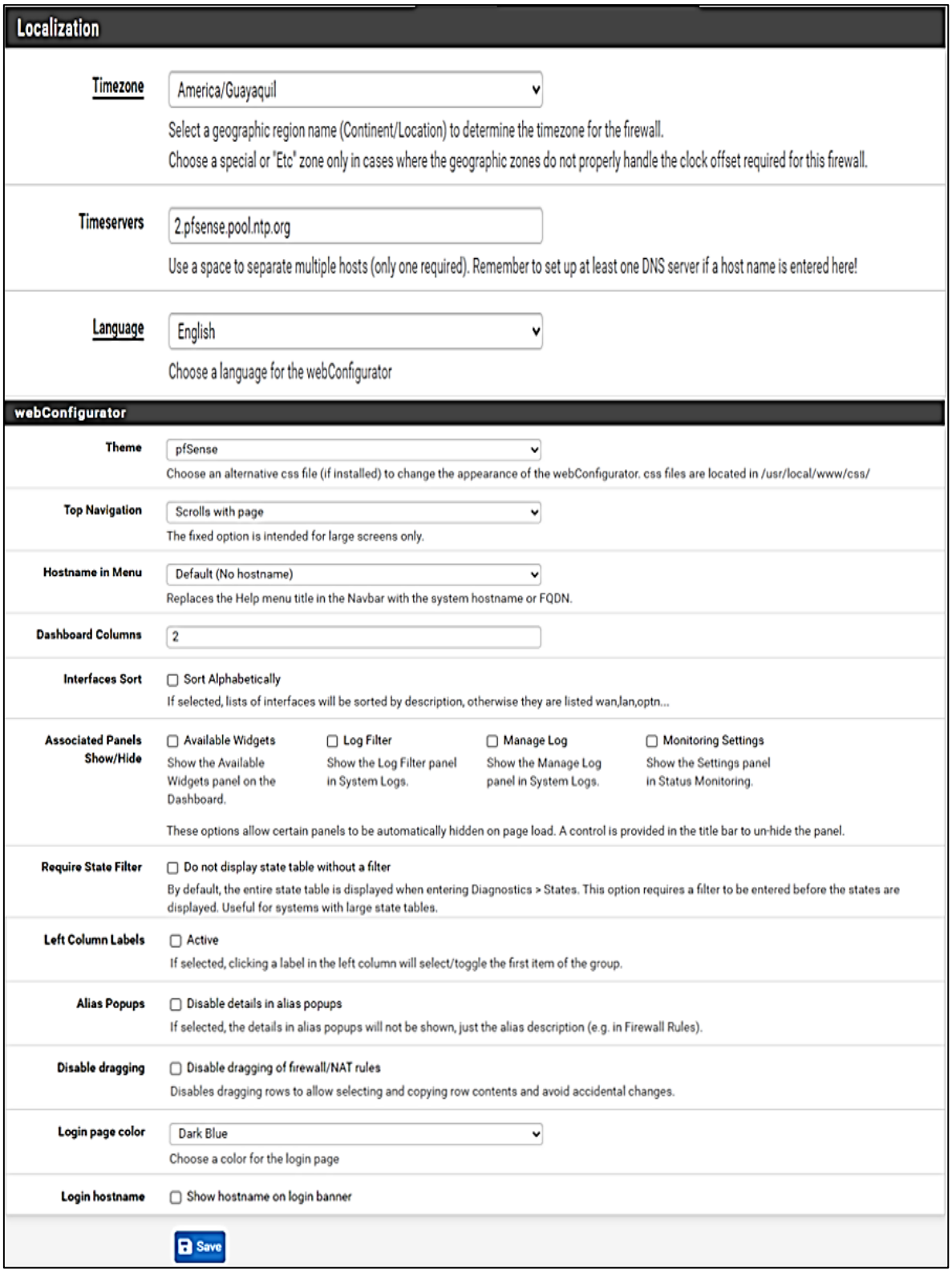


Figura 60. pfSense, configuración de la ubicación geográfica (localización del tiempo).
Fuente: Las autoras.

Paso 6: Las Autoridades de Certificación (CAS) son fundamentales en la autenticación segura de dispositivos y usuarios, garantizando la confidencialidad e integridad de las comunicaciones, por lo cual es necesario la creación de un certificado para el Portal Cautivo. Esto se refleja en la figura 61, se muestra el flujo de las certificaciones en un entorno de red.

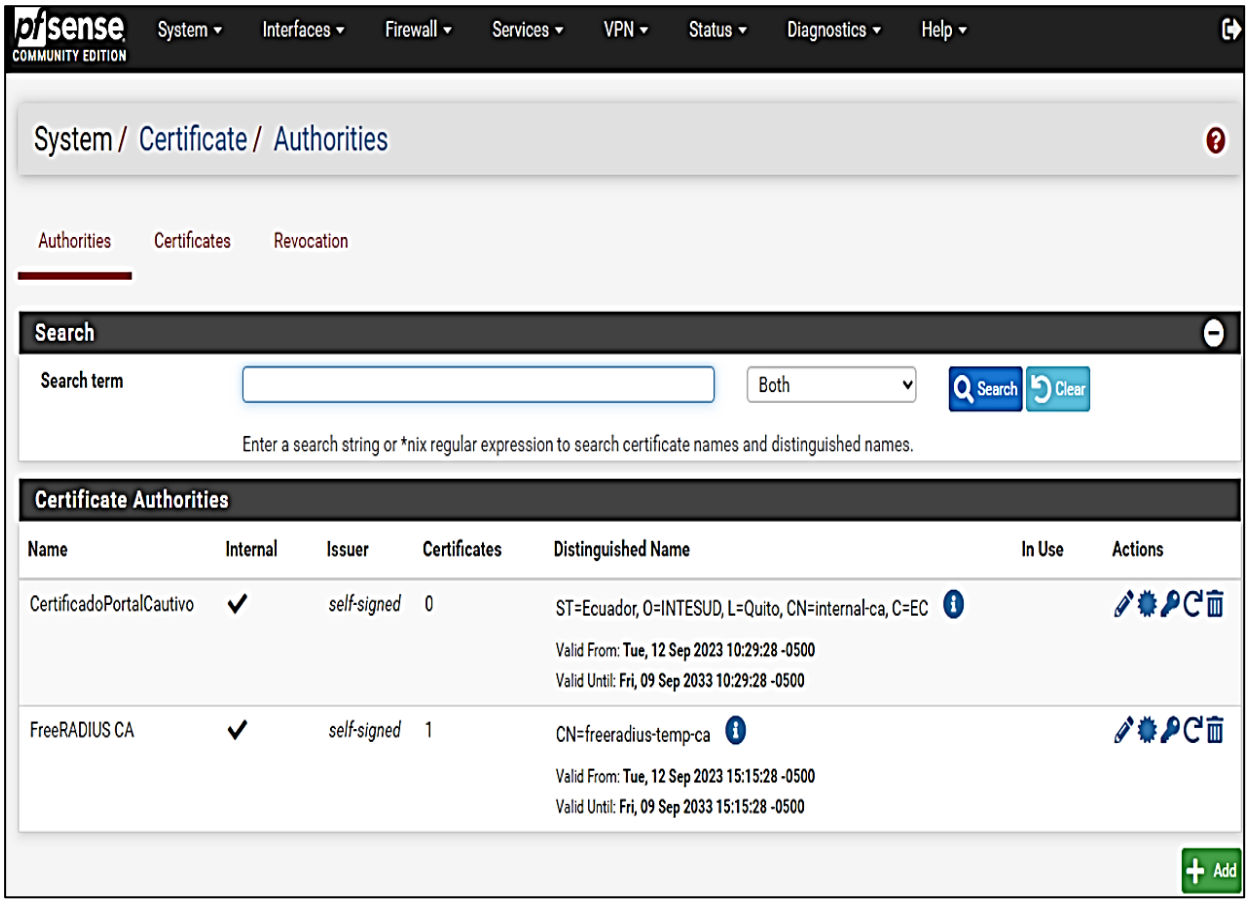


Figura 61. pfSense, configuración de certificados para la seguridad de red y protección.
Fuente: Las autoras.

Paso 7: Se deberá de establecer un nombre para el certificado y en "Method" se deja la opción de "Import an exiting Certificate Authority", la cual permite importar una autoridad de certificación existente y luego se deberá guardar los cambios, como se muestra en la figura 62.

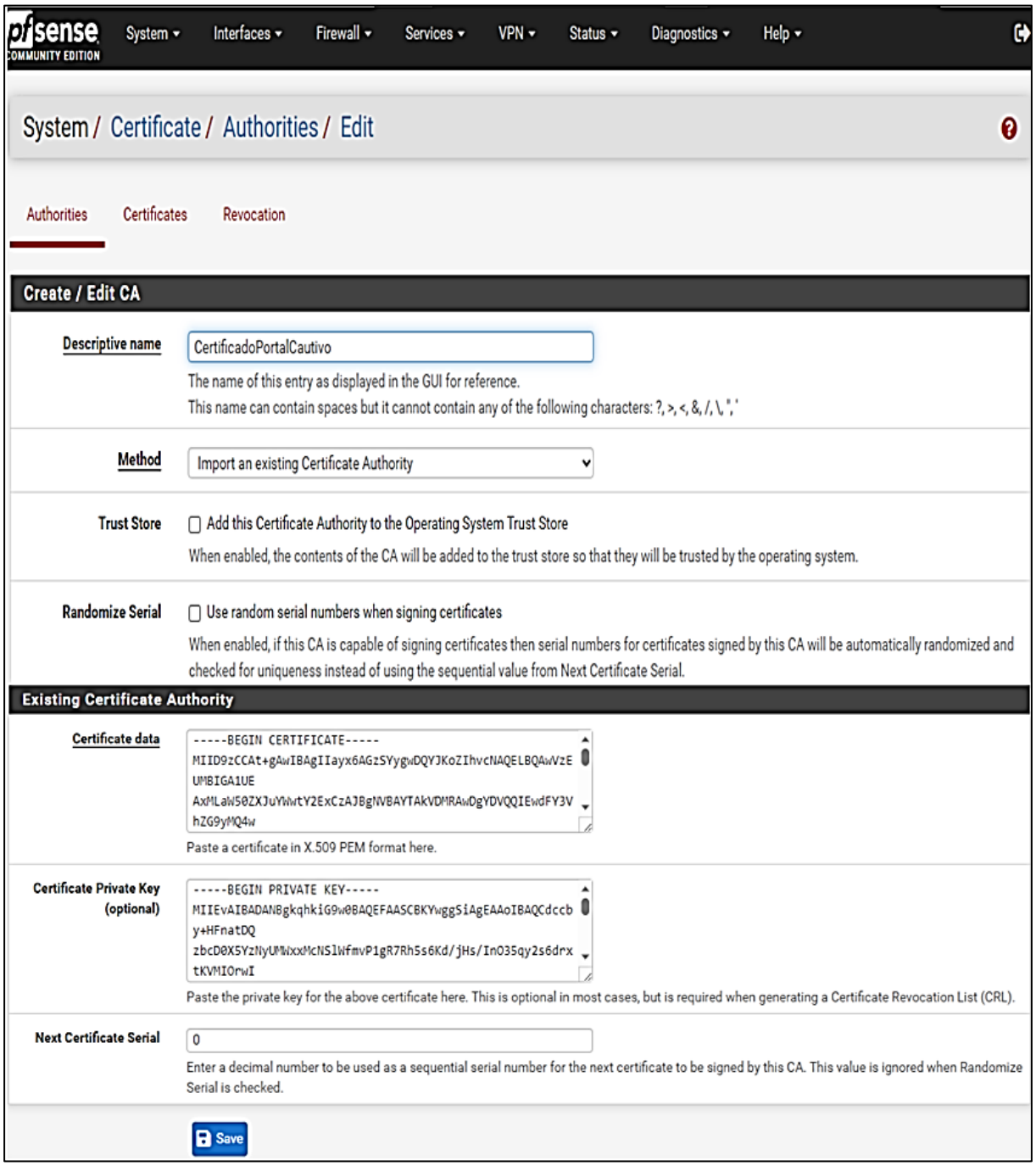
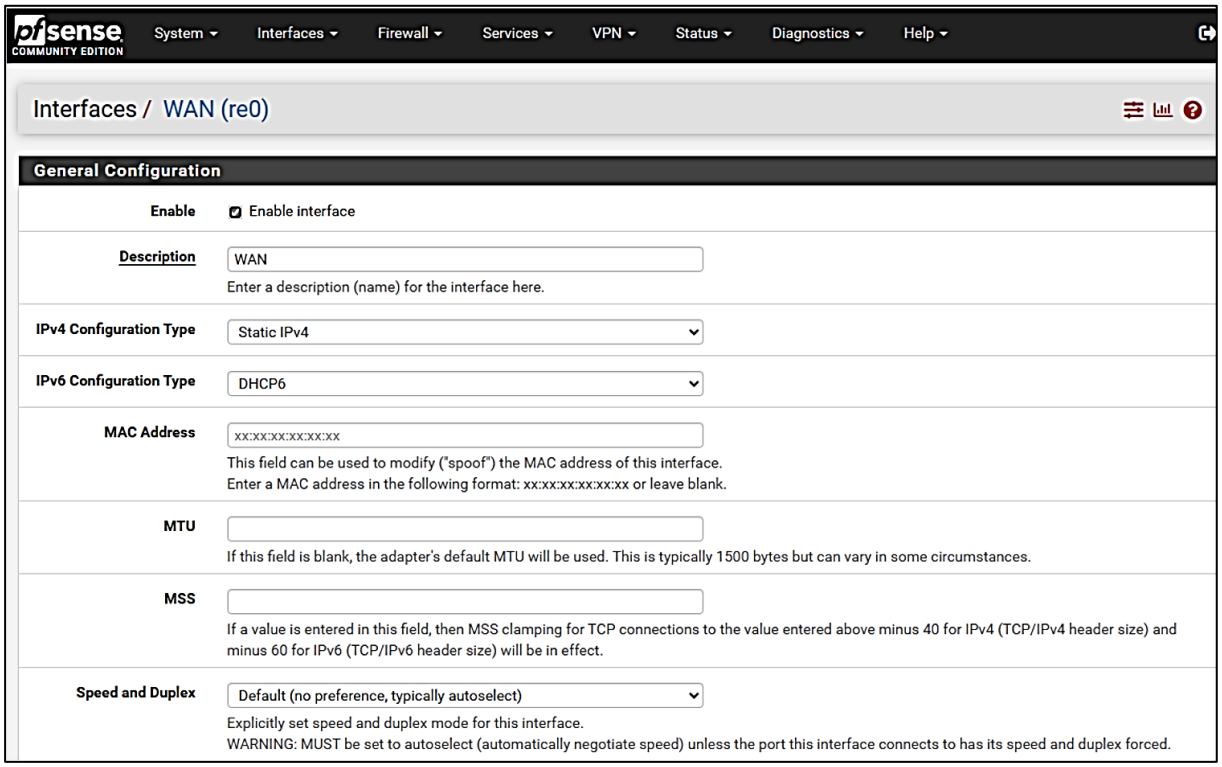


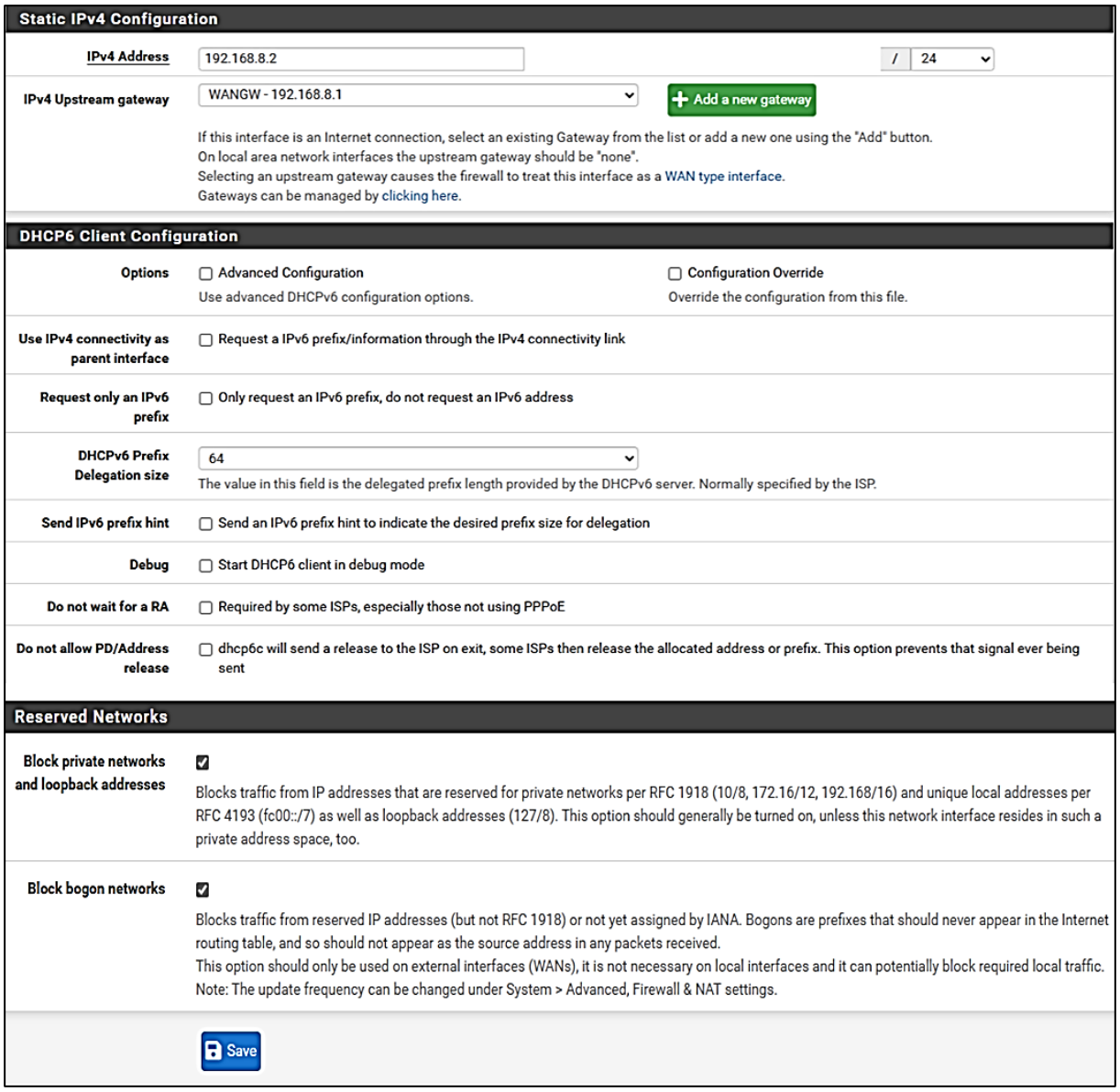
Figura 62. pfSense, configuración básica de certificados de los requisitos de seguridad.
Fuente: Las autoras.

Configuración de las tarjetas de red

Paso 8: Configuración de la interfaz WAN, para ello se debe activarla, establecer una descripción en este caso “WAN”, en configuración de IPv4, establecerla como estática y en el caso de IPv6 vamos de deshabilitarla por lo cual escogemos la opción “none”, como se muestra en la figura 63.



a)



b)

Figura 63. pfSense, configuración de la tarjeta de red WAN (re0).
Fuente: Las autoras.

Paso 9: Al igual que el paso anterior, durante la configuración de LAN, se deberá establecer una descripción en este caso “LAN”, habilitar IPv4, y en IPv6 elegir la opción “none”, tal como se muestra en la figura 64.

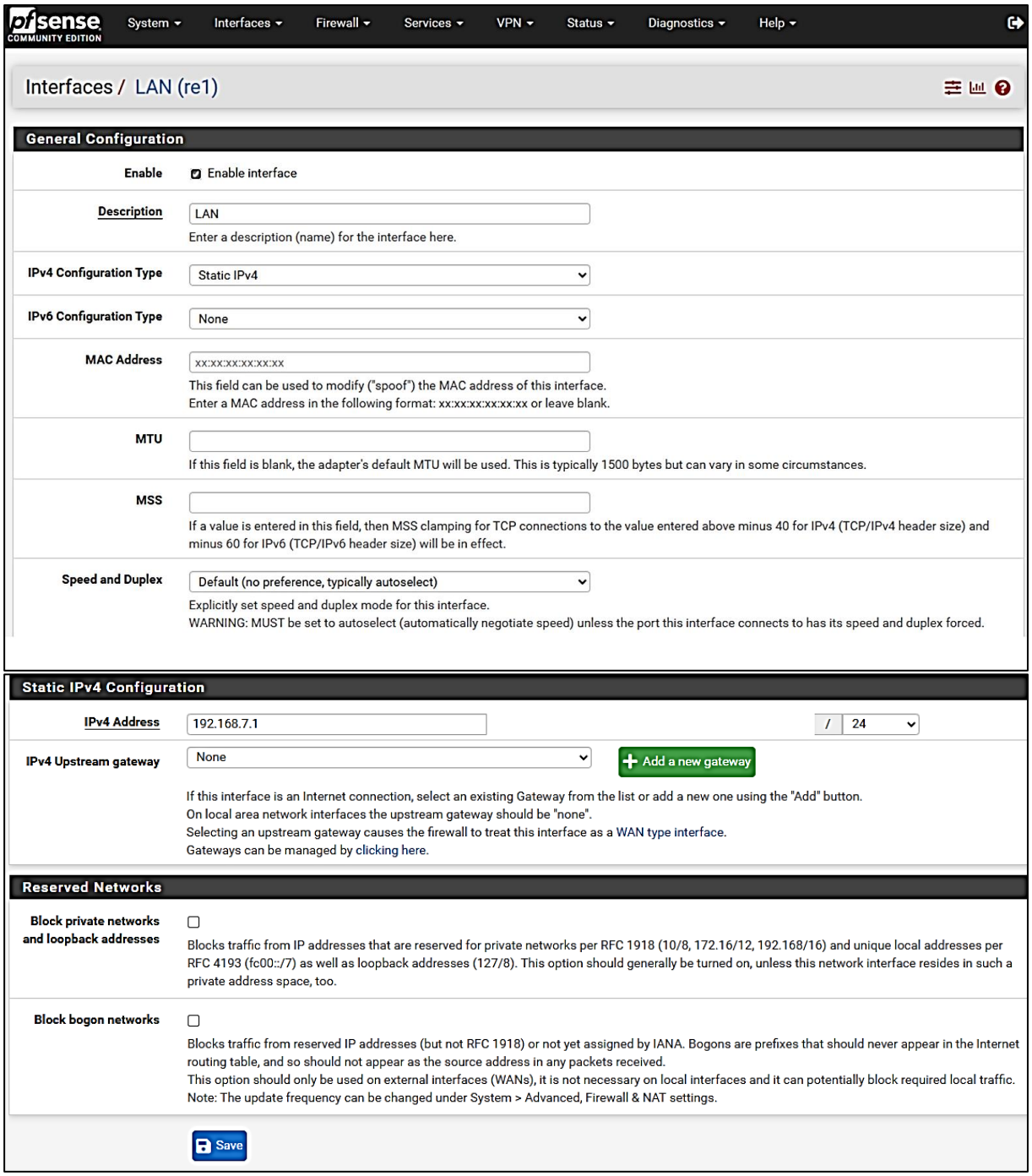


Figura 64. pfSense, configuración de la tarjeta de red LAN (re1).
Fuente: Las autoras.

Paso 10: En la configuración de la interfaz OPT1 (bge0), al igual que los dos pasos anteriores se la habilita, luego se establece la descripción “OPT1” y en IPv6 elegir la opción “none”, tal como se muestra en la siguiente figura:

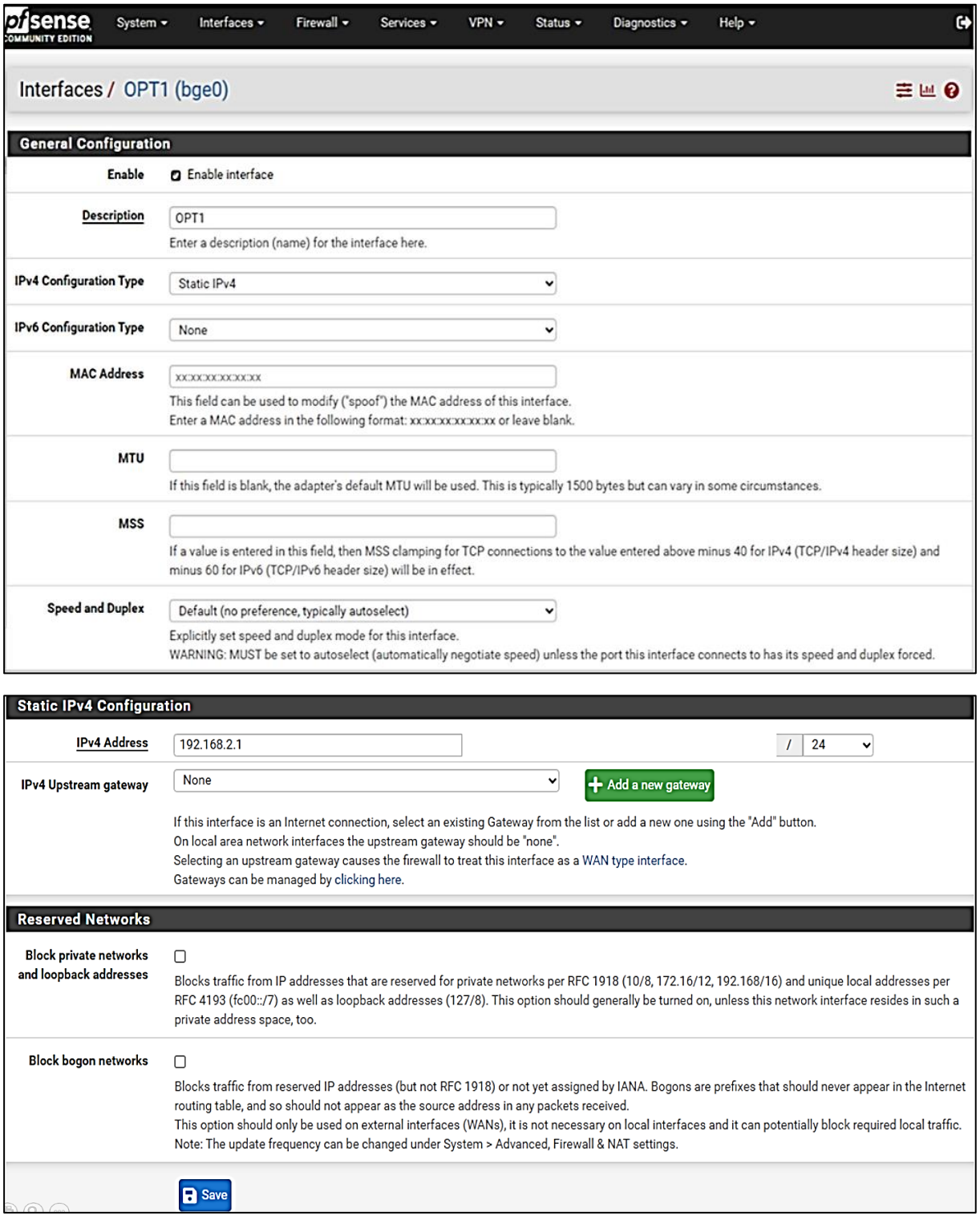
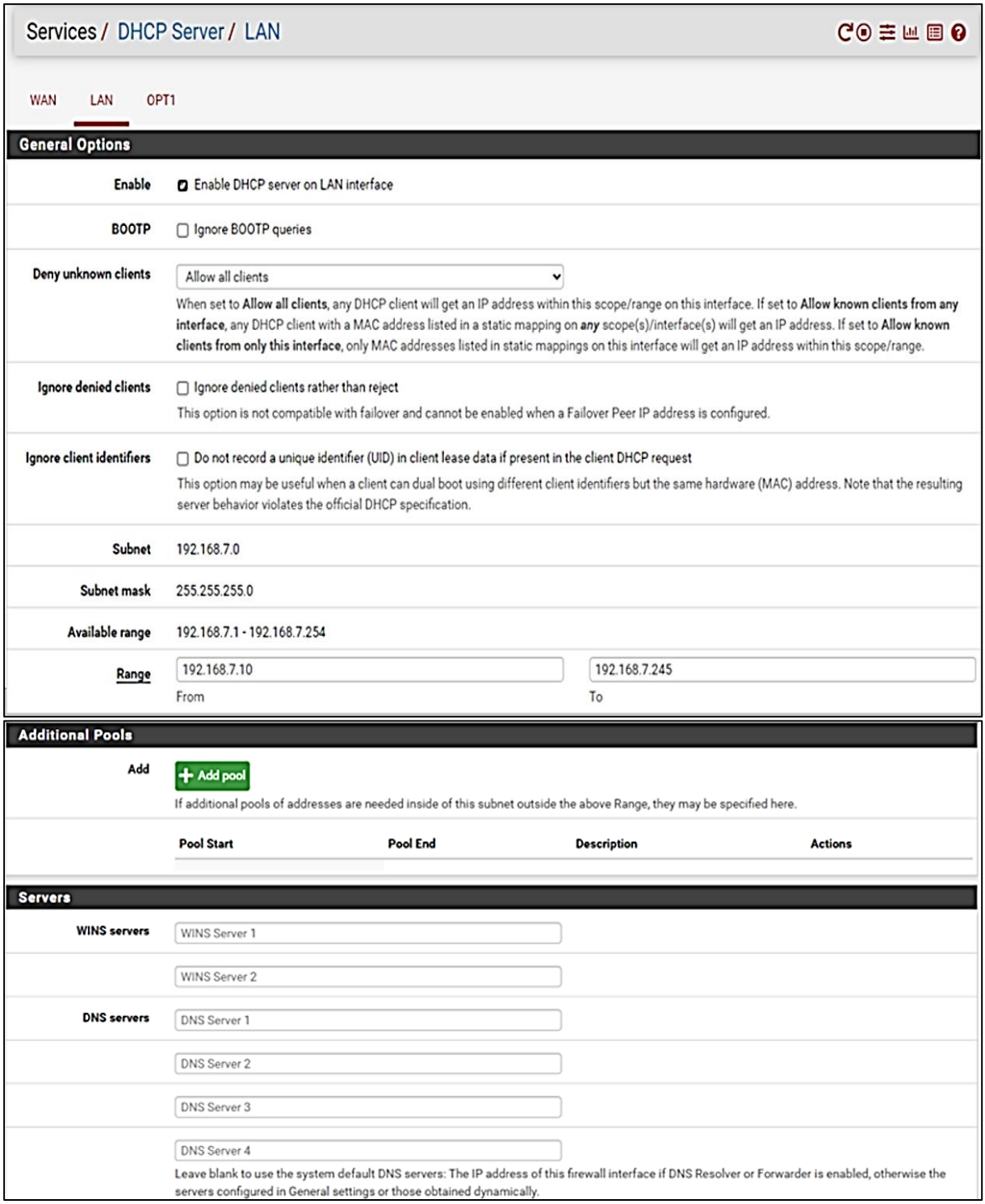


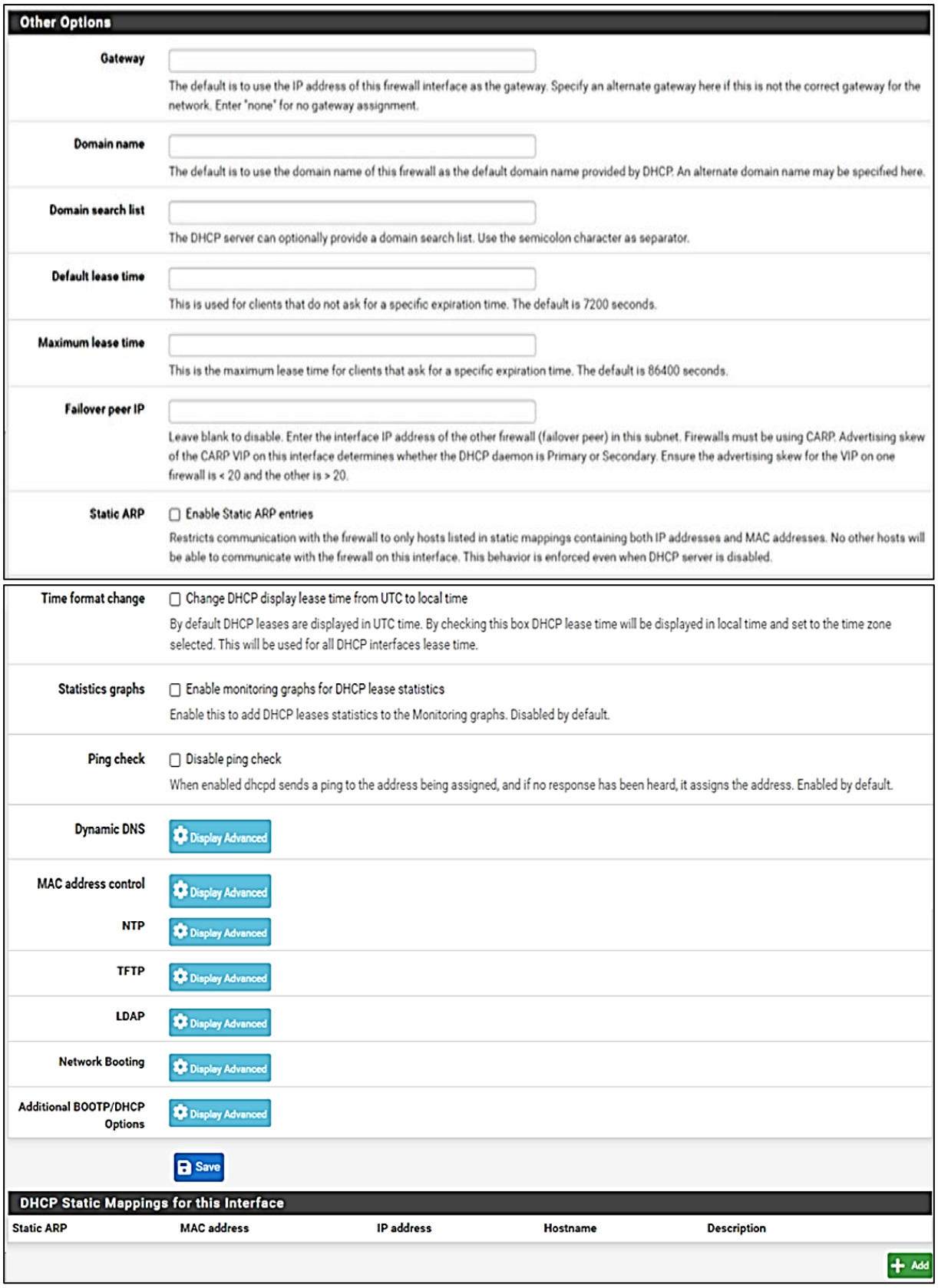
Figura 65. pfSense, configuración de la tarjeta OPT1 (bge0).
Fuente: Las autoras.

Configuración del servicio de DHCP para la LAN

Paso 11: Para configurar los servicios de servidor para ofrecer los servicios de **DHCP** a la LAN, únicamente se debe habilitar, luego se asigna el rango de direcciones IP, que van desde 192.168.7.10 hasta 192.168.7.245, tal como se muestra en la siguiente figura:



a)



b)

Figura 66. pfSense, configuración del servicio DHCP para la LAN.
Fuente: Las autoras.

Paso 12: Si se desea otra red operativa en OPT1 se realiza el mismo proceso habilitando el DHCP y por último dando un rango de IP que podrá ir, por ejemplo, desde la 192.168.2.100 hasta 192.168.2.200, por lo tanto, lo demás quedaría por defecto, como se muestra en la siguiente figura.

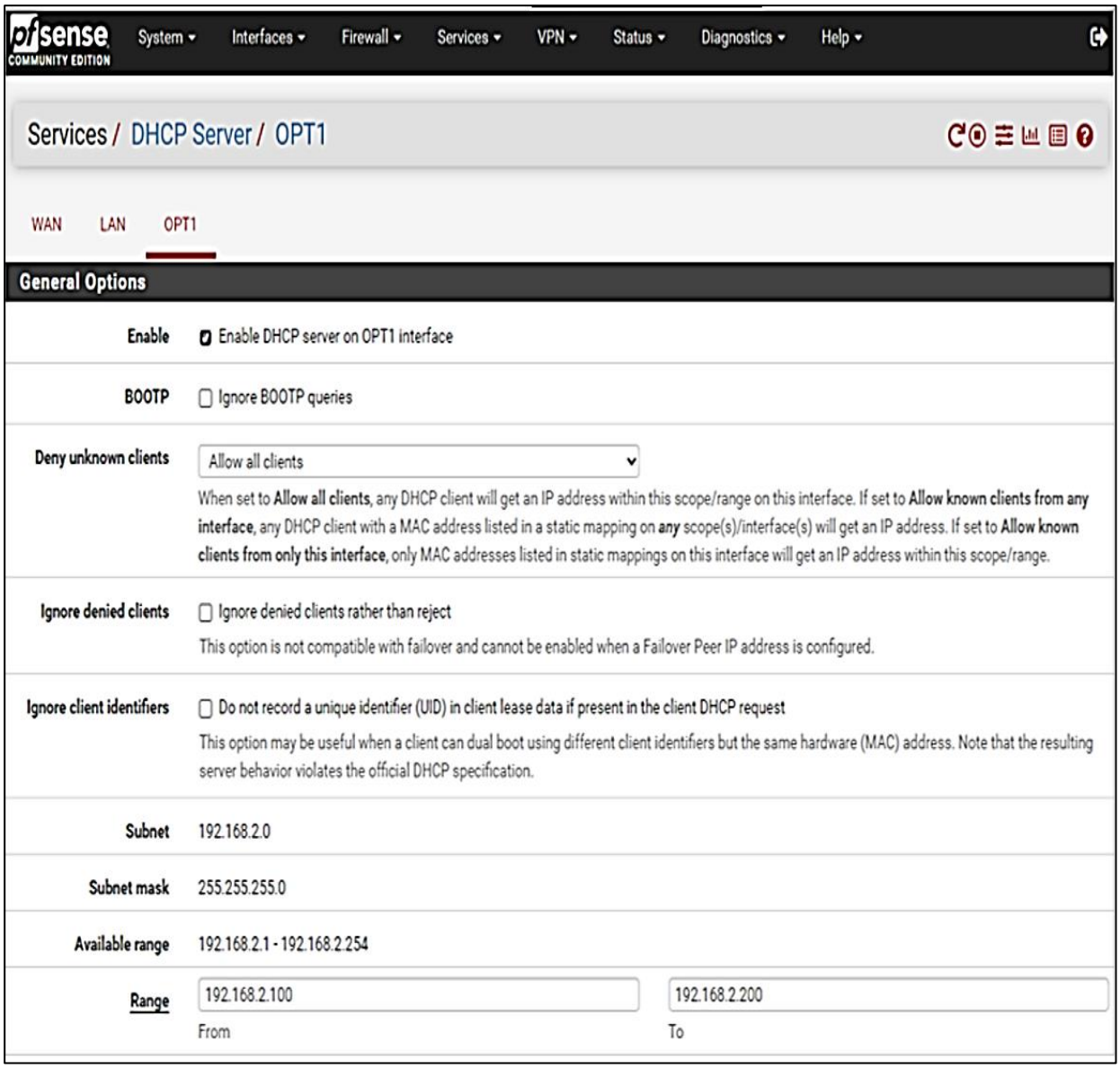


Figura 67. pfSense, configuración de DHCP server sobre OPT1.
Fuente: Las autoras.

Paso 13: En cuanto a las reglas firewall en WAN, se puede observar que existe ya una regla por defecto, por lo tanto, vamos a añadir una nueva, como se muestra en la siguiente figura:

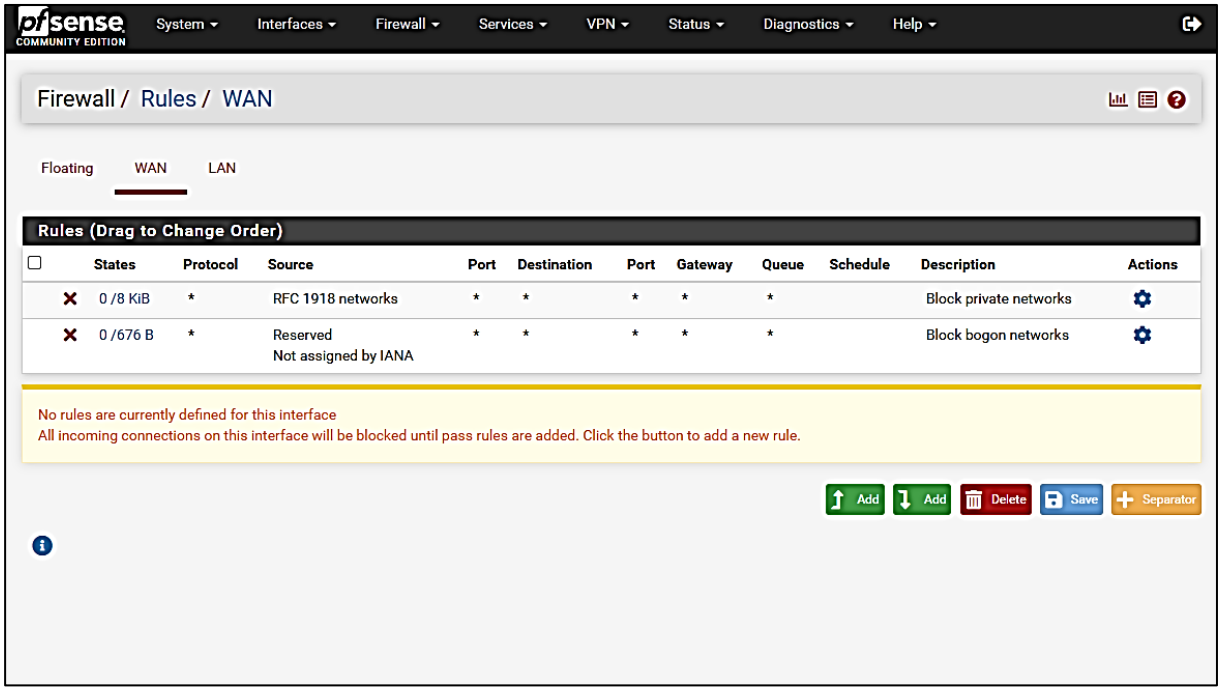


Figura 68. pfSense, reglas de Firewall por defecto para WAN.
Fuente: Las autoras.

Paso 14: Al añadir la nueva regla, se establece la acción “Pass”, luego se selecciona la interfaz que en este caso seria “WAN”, en la dirección de familia, escogemos la opción IPv4, por lo tanto, en protocolo vamos a elegir TCP, y en “Destination port range” que es el rango de nuestro puerto de destino, vamos a escoger de HTTPS (443) para HTTPS (443), como se muestra en la figura 69.

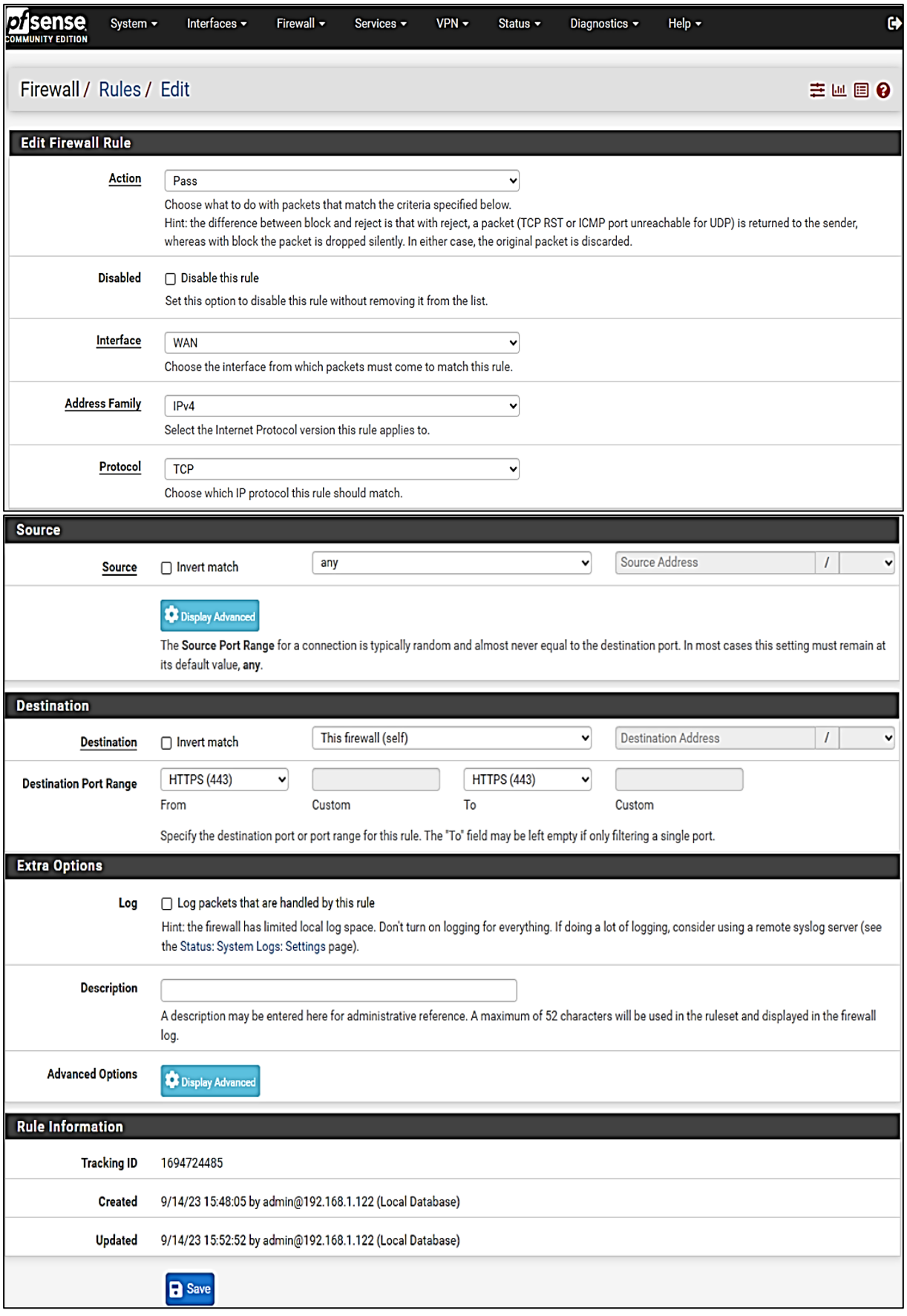


Figura 69. pfSense, edición de la regla general del Firewall para la interface WAN.
Fuente: Las autoras.

Configuración del Portal Cautivo

Paso 15: Para personalizar y configurar el **Portal Cautivo** en pfSense, el usuario debe dirigirse a 'Servicios' y seleccionar “Portal Cautivo”, como se muestra en la figura 70.

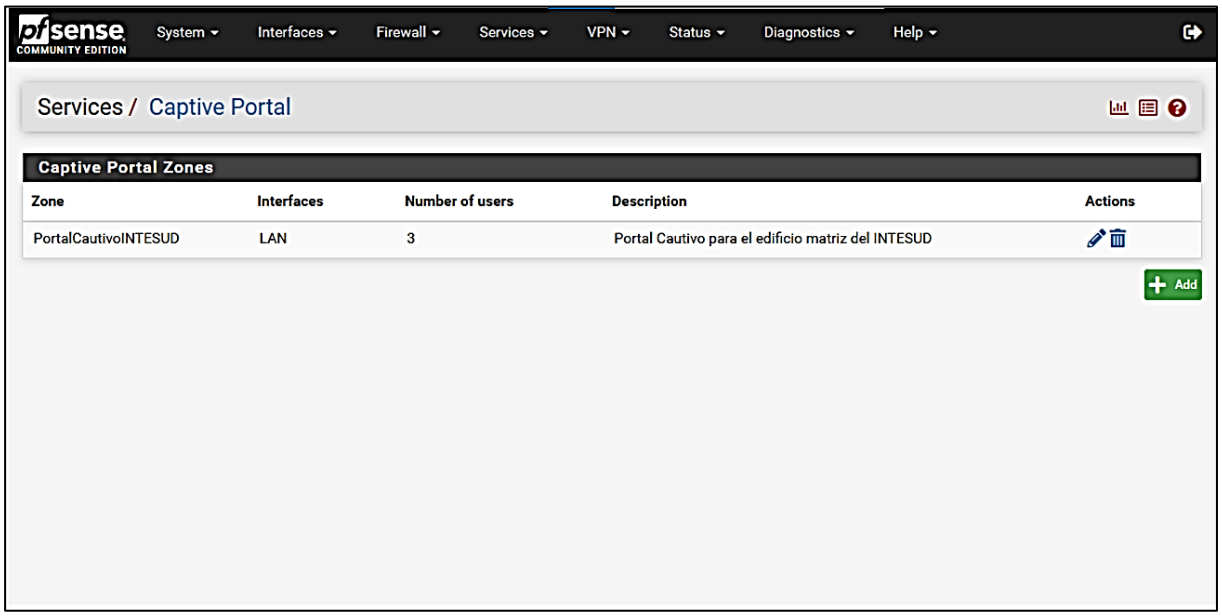
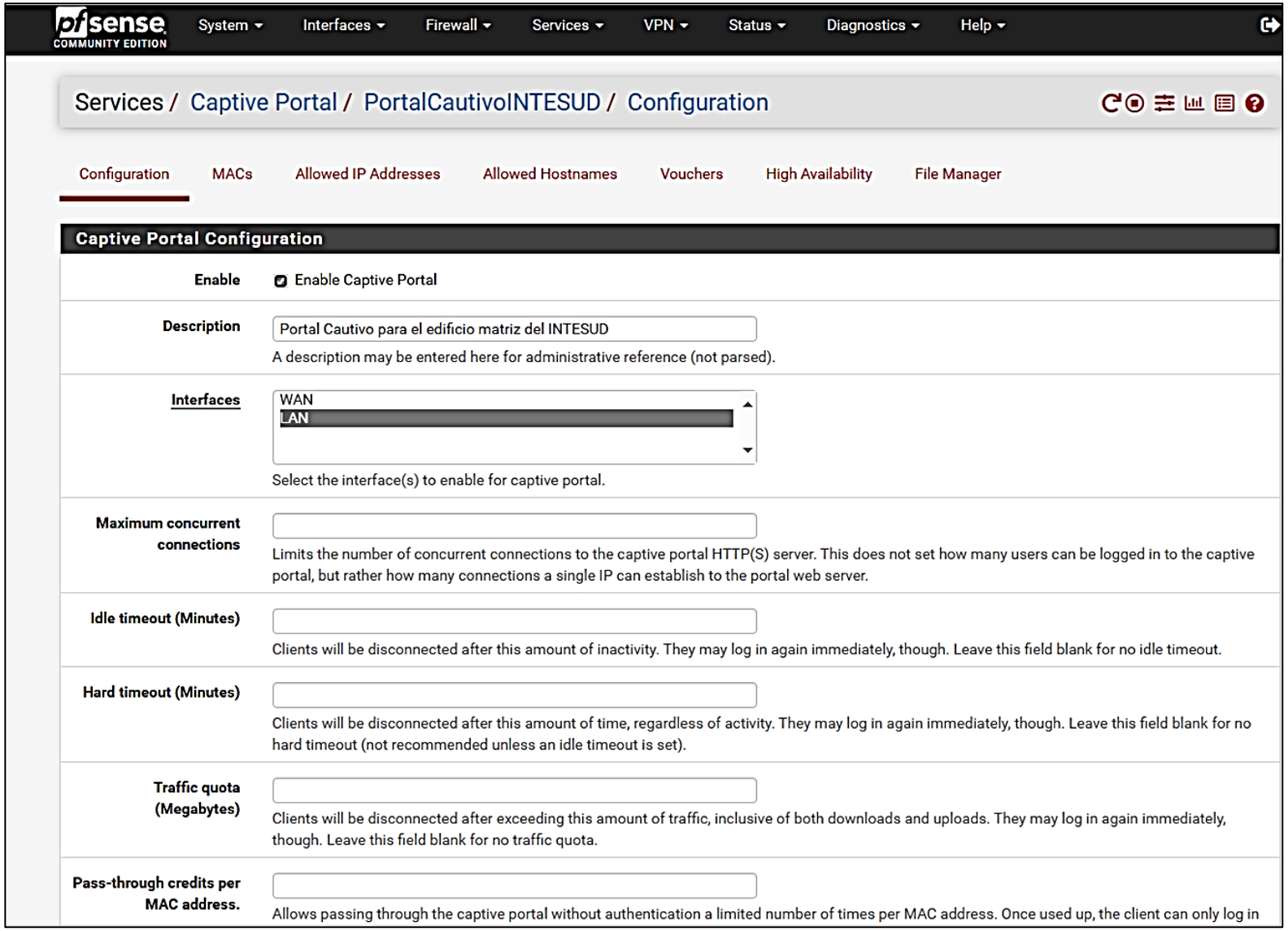


Figura 70. pfSense, configuración de la zona Portal Cautivo.
Fuente: Las autoras.

Paso 16: Una vez que se encuentre dentro de la opción, dar clic en “Add”. Va a pasar que se habilite la opción de portal cautivo, luego se signa una descripción, en interfaz se debe escoger “LAN”, vamos a escribir la dirección URL de la página de la institución en donde dice “After authentication Redirecction URL” para que luego de autenticarse el usuario le redirija a la página establecida y, por último, en cuanto a inicios de sesión de usuarios simultáneos “Concurrent user logins” vamos a elegir la opción de “last login”, según se muestra en las siguientes figuras:

(a)


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / Captive Portal / PortalCautivoINTESUD / Configuration
Configuration
MACs
Allowed IP Addresses
Allowed Hostnames
Vouchers
High Availability
File Manager
Captive Portal Configuration
Enable
Enable Captive Portal
Description
Portal Cautivo para el edificio matriz del INTESUD
A description may be entered here for administrative reference (not parsed).
Interfaces
WAN
LAN
Select the interface(s) to enable for captive portal.
Maximum concurrent connections
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.
Idle timeout (Minutes)
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout (Minutes)
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
Traffic quota (Megabytes)
Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.
Pass-through credits per MAC address.
Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in

b)

Figura 71. pfSense, configuración del Portal Cautivo.
Fuente: Las autoras.

Paso 17: Continuando con la configuración del paso anterior, ahora se debe habilitar la opción de cargar una plantilla personalizada, para la página de inicio de sesión del portal cautivo. Si es el caso de que el usuario desee utilizar una plantilla diseñada por pfSense, se debe deshabilitar la opción y cargar una imagen para el logo y una imagen de fondo. Además, se puede añadir términos y condiciones. Para el método de autenticación "Authentication

Method", seleccionamos la opción "None, don´t authenticate users", como se muestra en la figura 72.

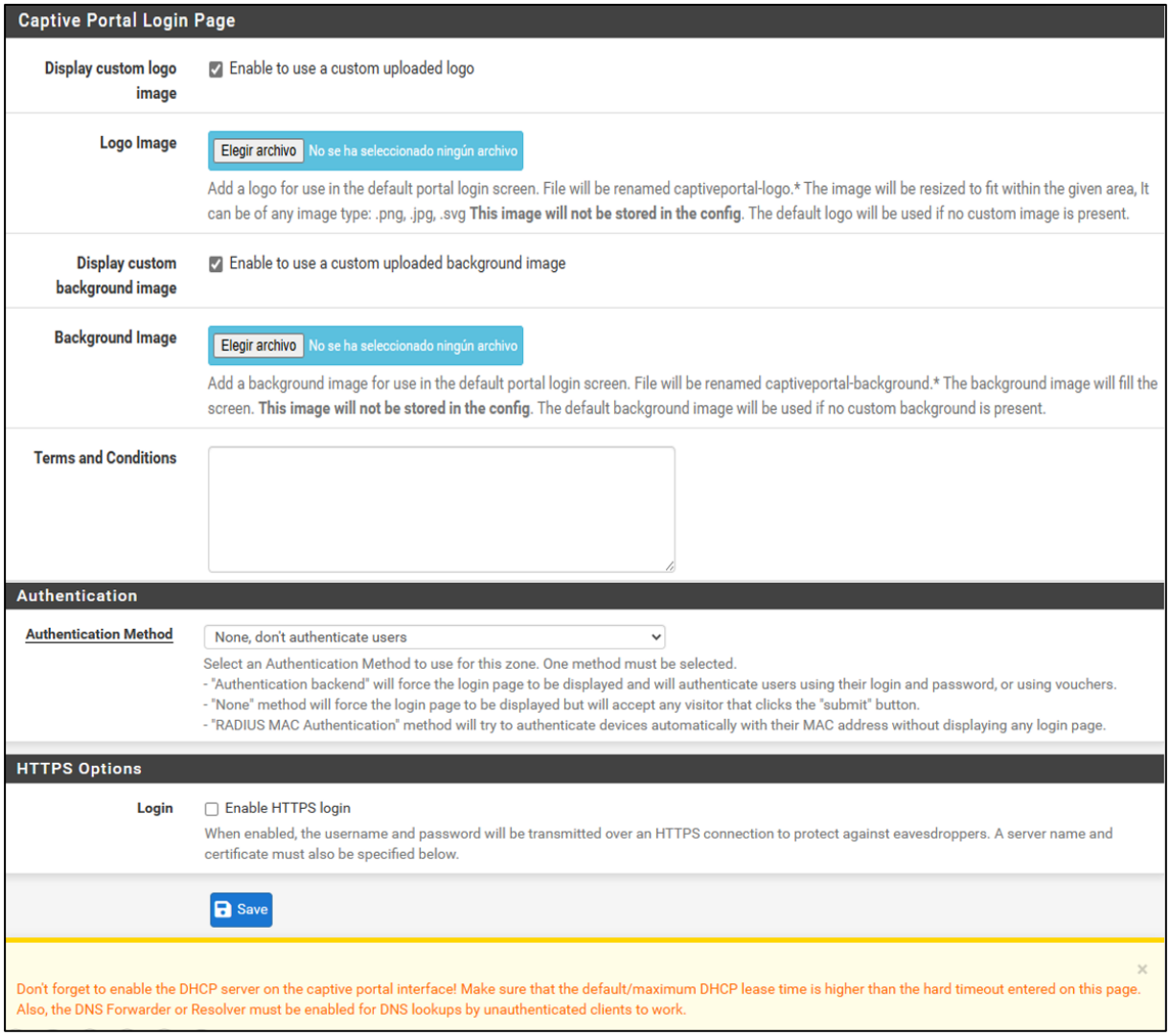


Figura 72. pfSense, configuración de personalización del logo del Portal Cautivo.
Fuente: Las autoras.

Paso 18: En el caso de escoger una plantilla personalizada por el usuario, es necesario que el logo se suba en "File Manager" que es el administrador de archivos y no en la plantilla de personalización, como se muestra en la siguiente figura:

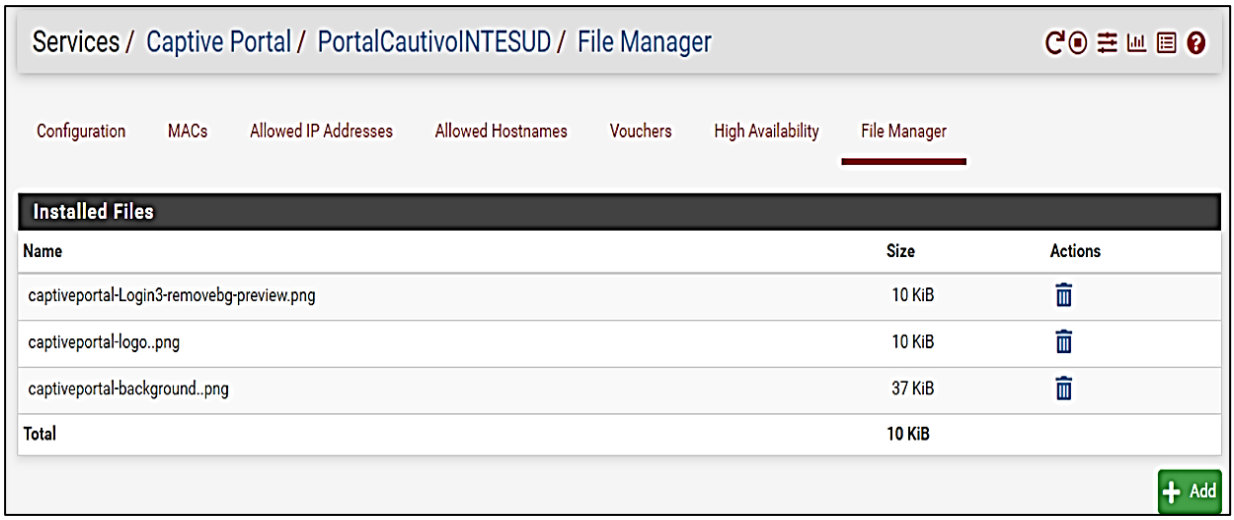
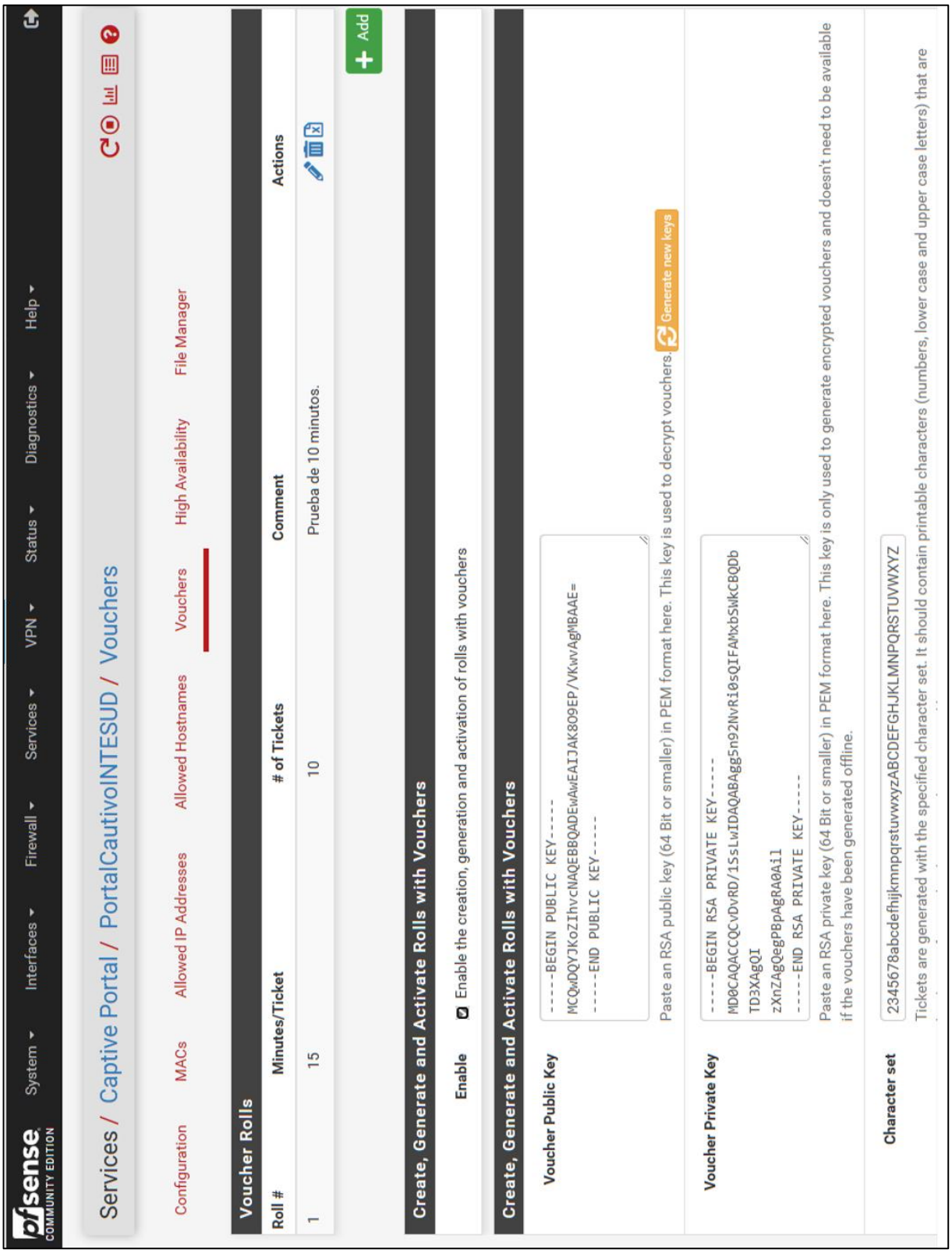


Figura 73. pfSense, administración de archivos del Portal Cautivo.
Fuente: Las autoras.

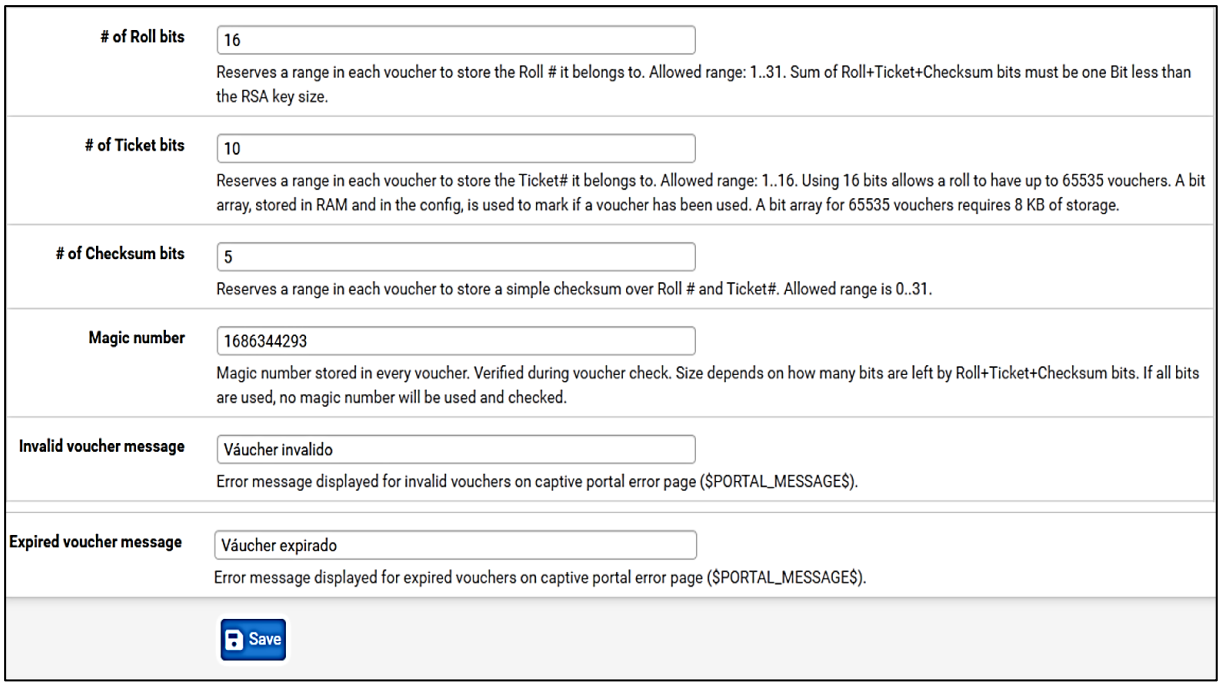
Configuración de los Váuchers

Para cumplir con el objetivo de desarrollar un sistema de distribución de váuchers que asegure un acceso restringido y monitoreado a la red Wifi, reservado para los miembros autorizados de la comunidad institucional, el siguiente paso número 19 de este proceso de configuración de pfSense evidencia el cumplimiento de este.

Paso 19: Para la creación de **váuchers**, se tiene el menú "Vouchers" en esta sección del servicio de Portal Cautivo. Una vez que se ingresa, se debe habilitar esta opción para luego dar clic en generar las claves necesarias. La configuración restante permanece en sus valores por defecto. Para configurar el tiempo límite, la cantidad y la descripción del váucher, se dirige a la sección de “Voucher Rolls” y se luego se debe guardar. Los váuchers se los pueden descargar en un archivo Excel o CSV, como se muestra en las siguientes figuras:


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / Captive Portal / PortalCautivoINTESUD / Vouchers
Configuration
MACs
Allowed IP Addresses
Allowed Hostnames
Vouchers
High Availability
File Manager
Voucher Rolls
Roll #
Minutes/Ticket
# of Tickets
Comment
Actions
1
15
10
Prueba de 10 minutos.
Add
Create, Generate and Activate Rolls with Vouchers
Enable
Enable the creation, generation and activation of rolls with vouchers
Create, Generate and Activate Rolls with Vouchers
Voucher Public Key
-----BEGIN PUBLIC KEY-----
MCQwDQYJKoZIhvcNAQEBBQADEwAwEAIJAK8O9EP/VKwvAgMBAAE=
-----END PUBLIC KEY-----
Paste an RSA public key (64 Bit or smaller) in PEM format here. This key is used to decrypt vouchers.
Generate new keys
Voucher Private Key
-----BEGIN RSA PRIVATE KEY-----
MD0CAQACCQCvDvRD/1SsLwIDAQABAgg5n92NvR10sQIFAMxbSwkCBQDb
TD3XAgQI
zXnZAgQegPBpAgRA0Ail
-----END RSA PRIVATE KEY-----
Paste an RSA private key (64 Bit or smaller) in PEM format here. This key is only used to generate encrypted vouchers and doesn't need to be available if the vouchers have been generated offline.
Character set
2345678abcdefhijkmnpqrstuvwxyzABCDEFGHJKLMNPQRSTUVWXYZ
Tickets are generated with the specified character set. It should contain printable characters (numbers, lower case and upper case letters) that are

a)



b)

Figura 74. pfSense, generador de váuchers.
Fuente: Las autoras.

En la configuración del portal cautivo, se presentan diversas alternativas para el manejo de inicios de sesión mediante váucher:

- **Deshabilitado**: No permite múltiples inicios de sesión simultáneos por váucher.
- **Múltiples**: No aplica restricciones en el número de inicios de sesión por váucher.
- **Último inicio de sesión**: Concede únicamente el acceso correspondiente al inicio de sesión más reciente por váucher. Los inicios de sesión previos son desconectados.
- **Primer inicio de sesión**: Concede exclusivamente el primer acceso por váucher. No se permiten más intentos de inicio de sesión con váucher mientras un usuario ya tiene una sesión activa.

La elección de 'Último inicio de sesión' se justifica por la necesidad de evitar el mal uso de las credenciales compartidas o el uso no autorizado de un mismo váucher por múltiples usuarios al mismo tiempo.

Paso 20: Se prueba el funcionamiento de la página principal del portal cautivo, y se obtiene la ventana de ingreso como se muestra en la siguiente figura:

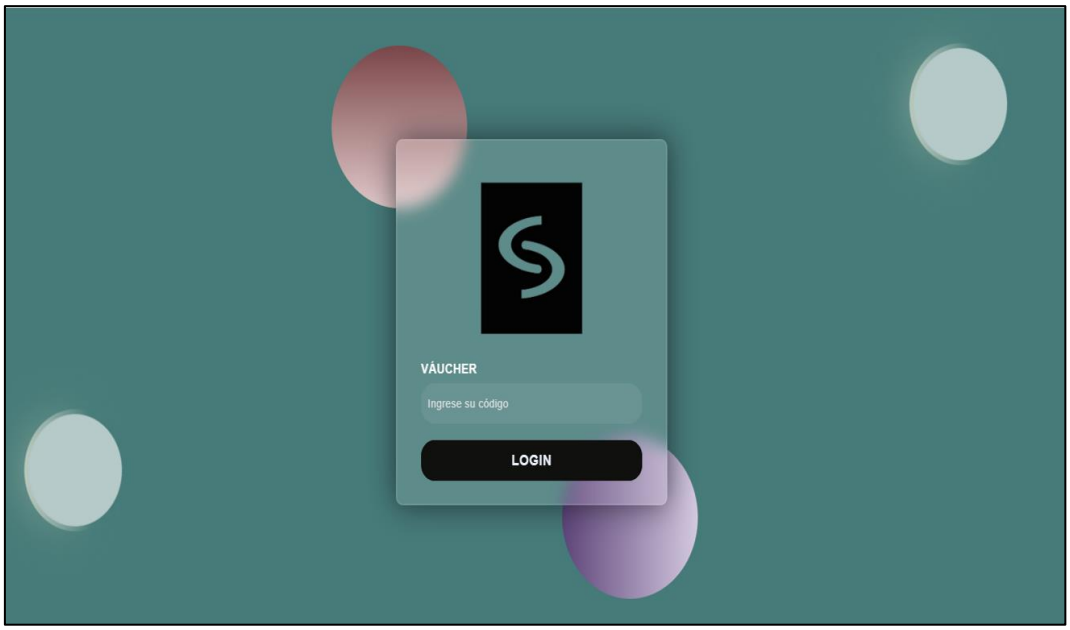


Figura 75. pfSense, página web de inicio de sesión del Portal Cautivo para un usuario.
Fuente: Las autoras.

Paso 21: Una vez ingresado el váucher, se redirige al usuario a la página de la Institución, como se muestra en la siguiente figura 76.

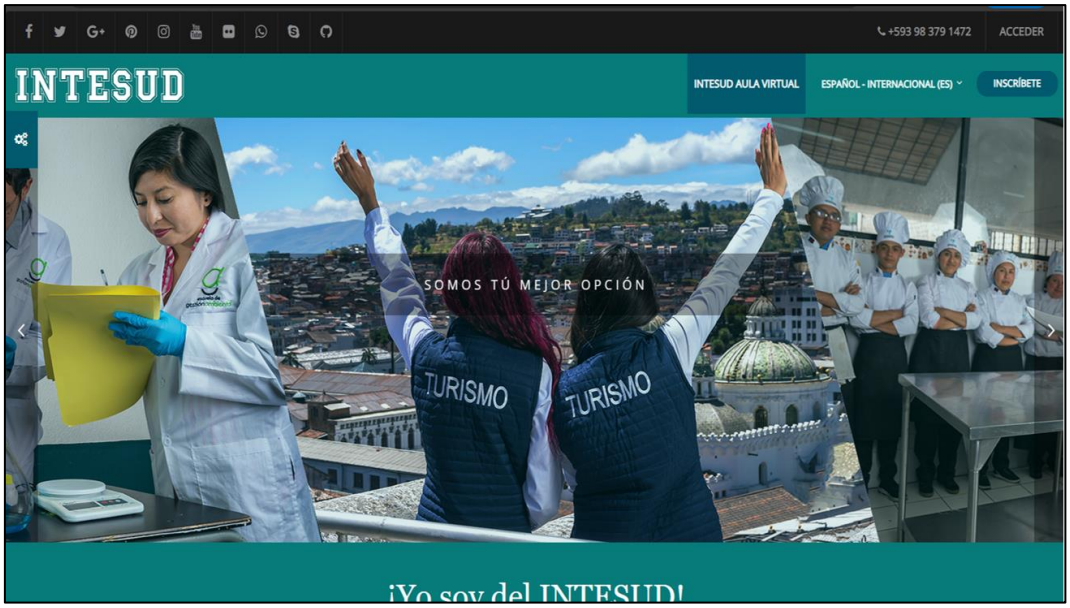


Figura 76. pfSense, redireccionamiento a la URL de inicio luego del ingreso exitoso por el Portal Cautivo.
Fuente: Las autoras.

Paso 22: Para revisar la bitácora de conexiones, se puede observar el estado de los usuarios conectados en la sección "Status" y luego en “Captive Portal”, como se muestra en la siguiente figura:

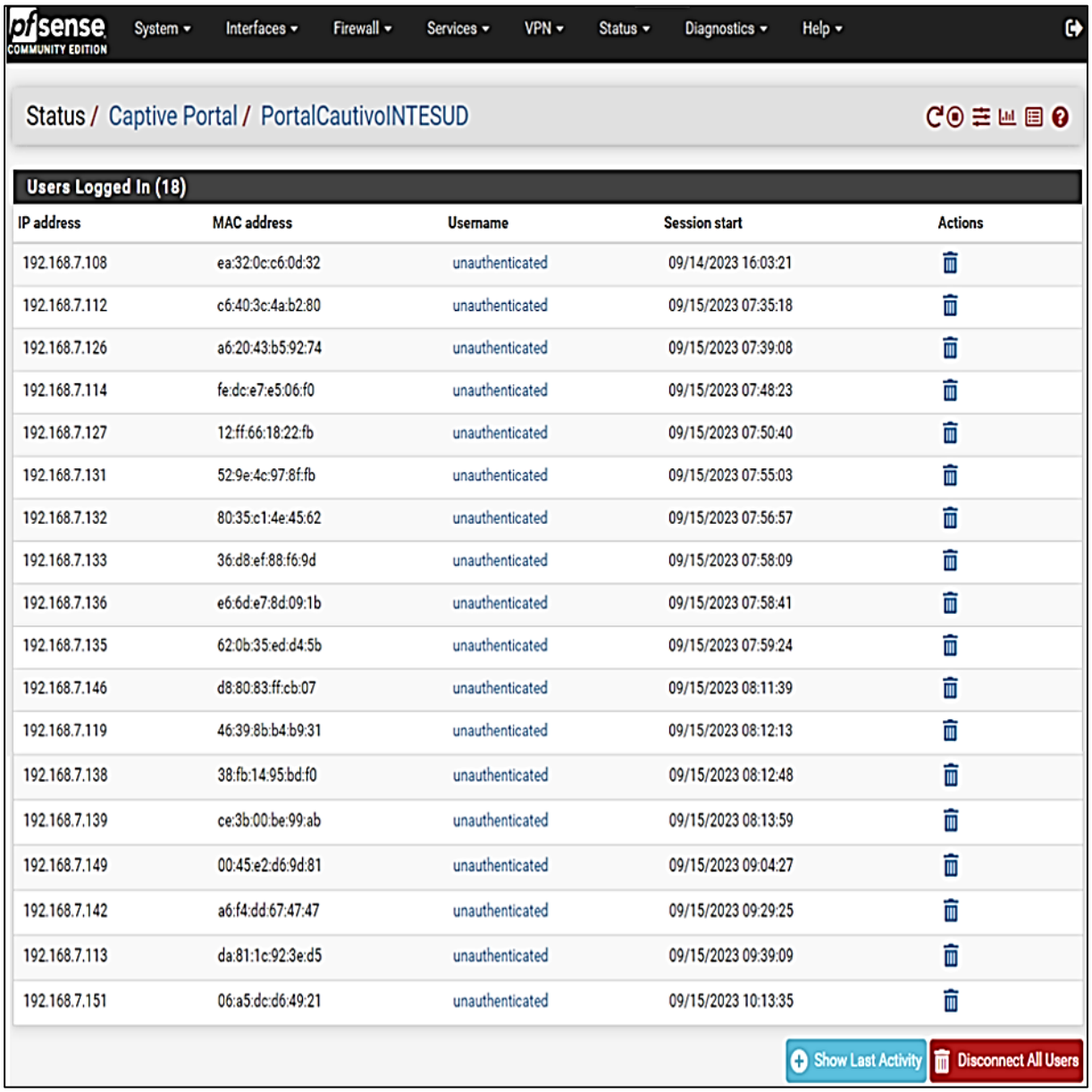


Figura 77. pfSense, registro total de usuarios del Portal Cautivo.
Fuente: Las autoras.

6.3. Correos masivos con MailChimp

Al momento de usar váuchers como un medio de autenticación estos deben ser socializados a los estudiantes de la sección diurna que asisten de manera presencial al edificio matriz de la Institución a recibir clase, para ello la mejor alternativa es el empleo de MailChimp como herramienta de correo masivo. Esta plataforma permite enviar de manera segura y confidencial los váuchers a los estudiantes.

MailChimp se destaca como una herramienta de alto nivel que proporciona la capacidad de enviar correos masivos a listas de contactos con una presentación profesional. A continuación, se presentan las siguientes figuras que describen la utilización y personalización de MailChimp para los propósitos de este proyecto:

Paso 1: Se accede al navegador de preferencia y se realiza la búsqueda de MailChimp, como se muestra en la siguiente figura:

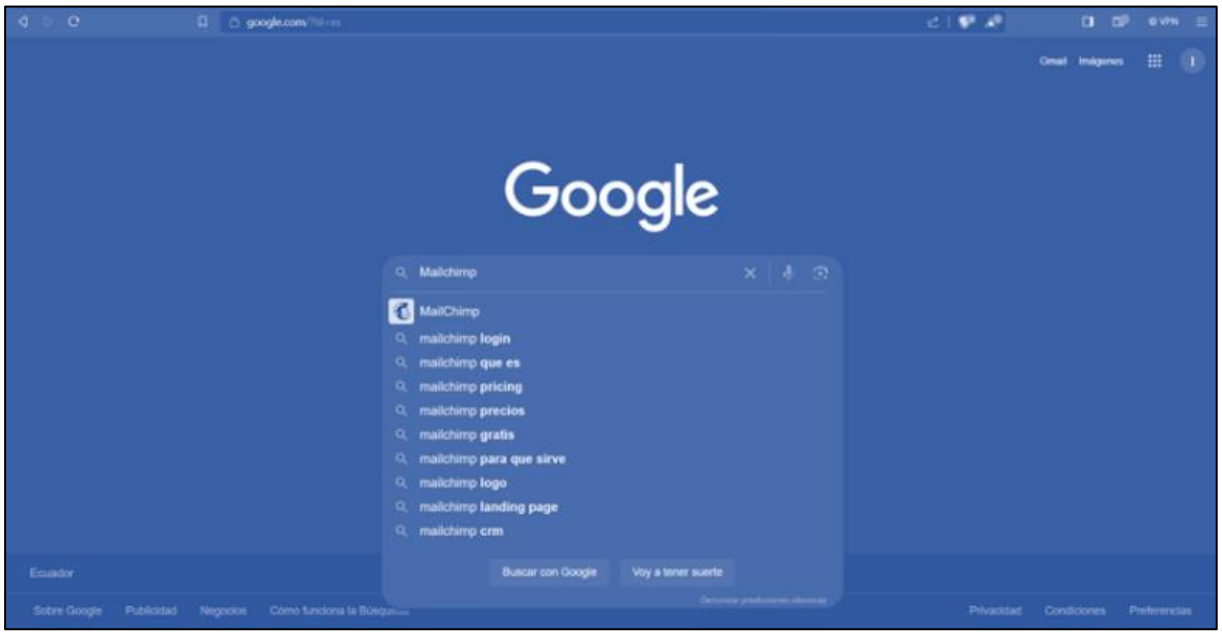


Figura 78. Búsqueda de MailChimp en un buscador de Internet.
Fuente: Las autoras.

Paso 2: Se escoge la opción "MailChimp: Plataforma de marketing por correo electrónico”, como se muestra en la figura 79.

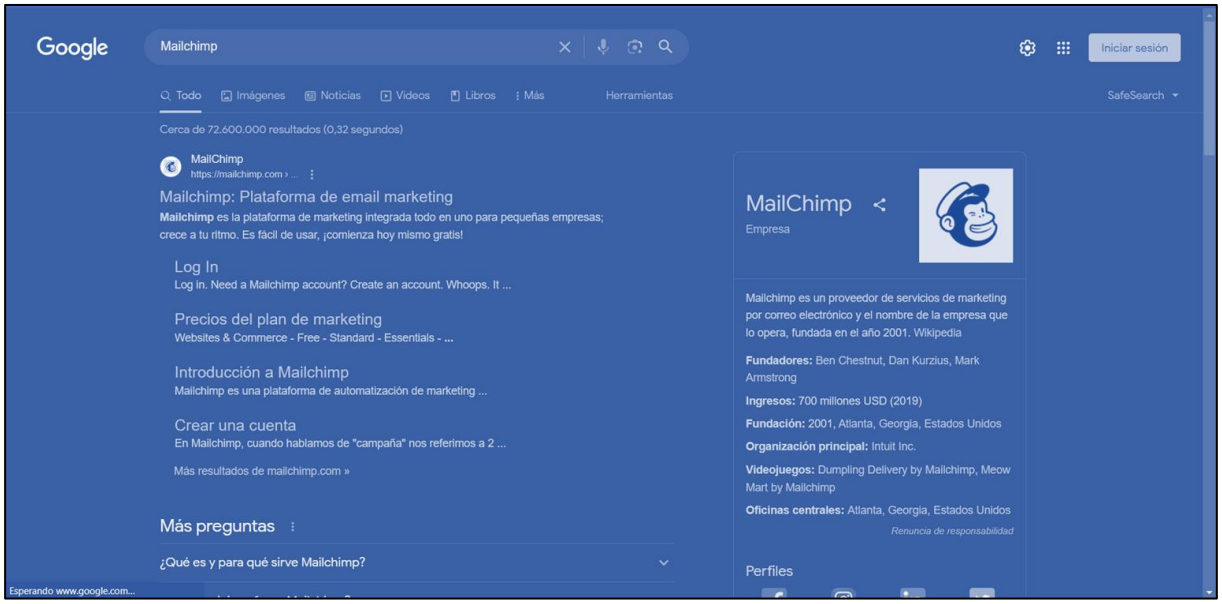


Figura 79. Resultado de búsqueda de MailChimp, Plataforma de marketing.
Fuente: Las autoras.

Paso 3: Ya en la página, se abrirá una ventana que contiene información detallada sobre la plataforma de MailChimp, por lo que se procede a hacer clic en "Registrarse" para crear una cuenta, como se muestra en la figura 80.

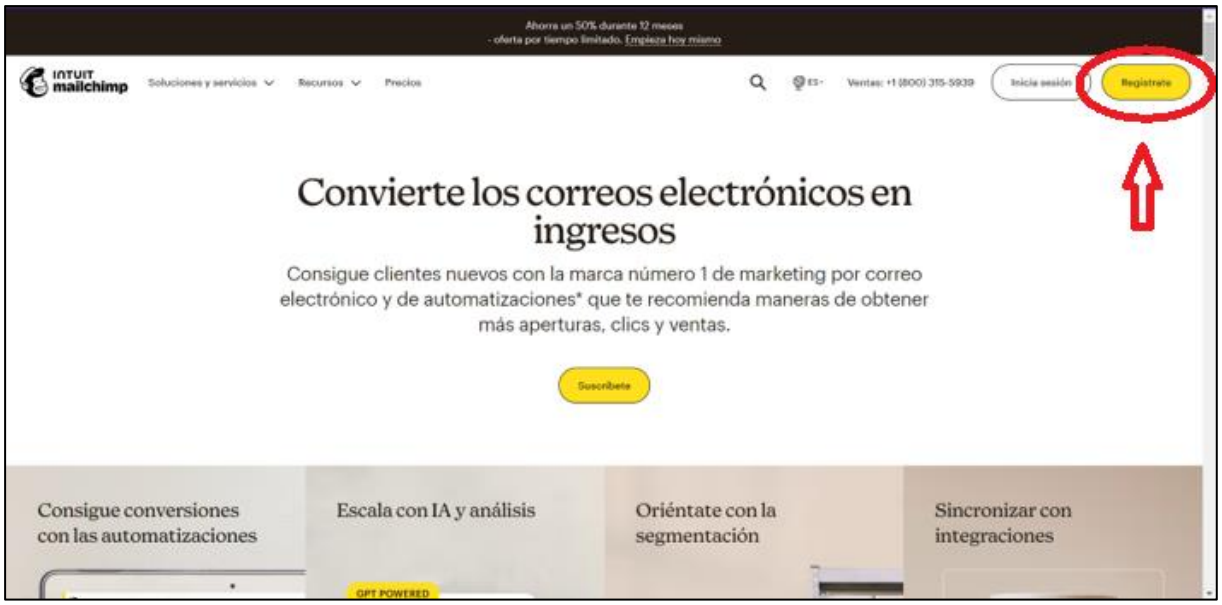


Figura 80. Página web principal de MailChimp.
Fuente: Las autoras.

Paso 4: Aparecerá una nueva ventana en la que se mostrarán los planes disponibles de MailChimp. La elección del plan dependerá de las necesidades del usuario, en este caso se usará el plan gratuito, como se muestra en la figura 81.

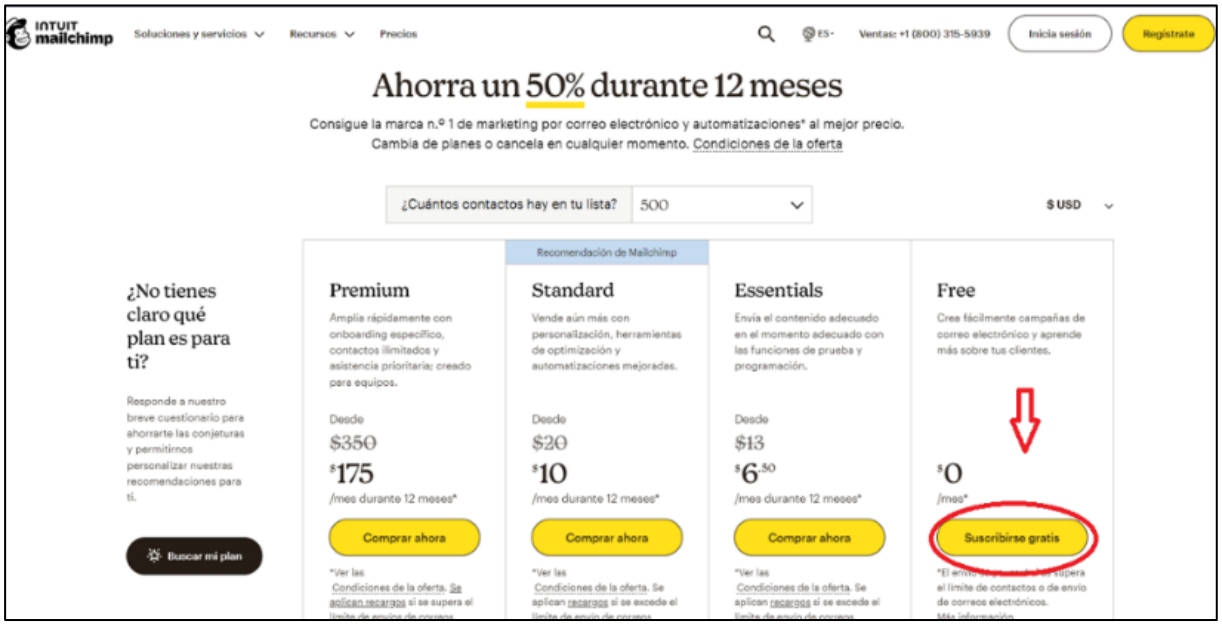


Figura 81. Planes de servicio de correos masivos de MailChimp.
Fuente: Las autoras.

Paso 5: El usuario debe proporcionar su correo electrónico, nombre de usuario, contraseña y confirmar los términos y condiciones", tal como se muestra en la figura 82.

Figura 82. Ventana emergente para el registro de usuario nuevo en MailChimp.
Fuente: Las autoras.

Paso 6: Después de completar el registro, es importante verificar el correo electrónico asociado. El mensaje indicará la necesidad de confirmar la identidad, por lo que se procederá a dar clic en “Activar cuenta”, tal como se muestra en la figura 83.

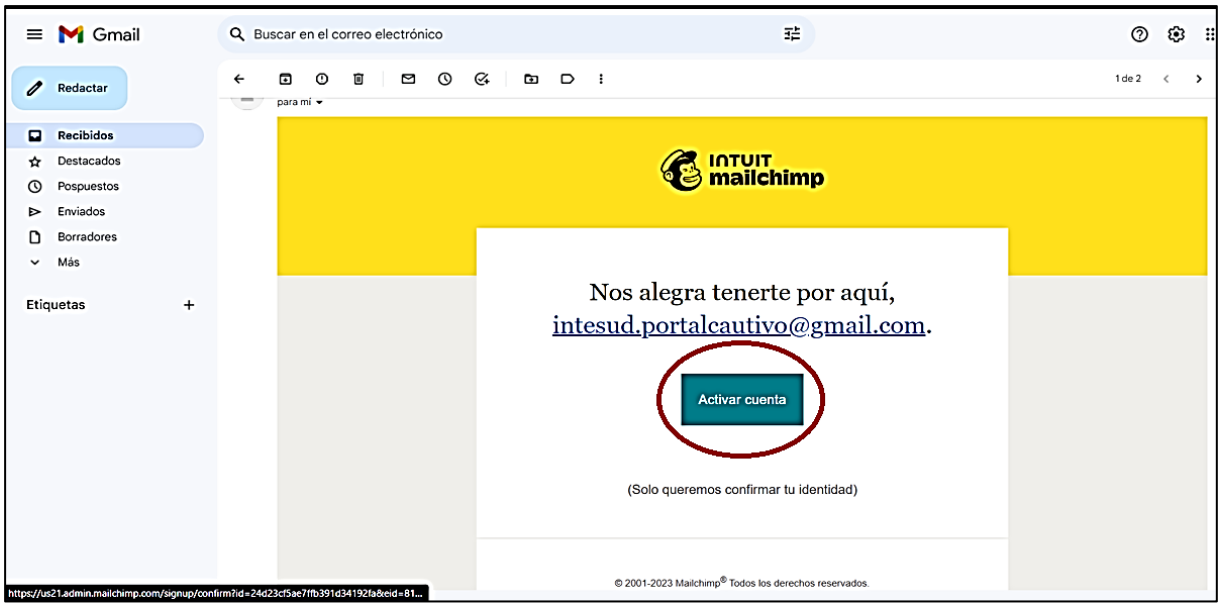
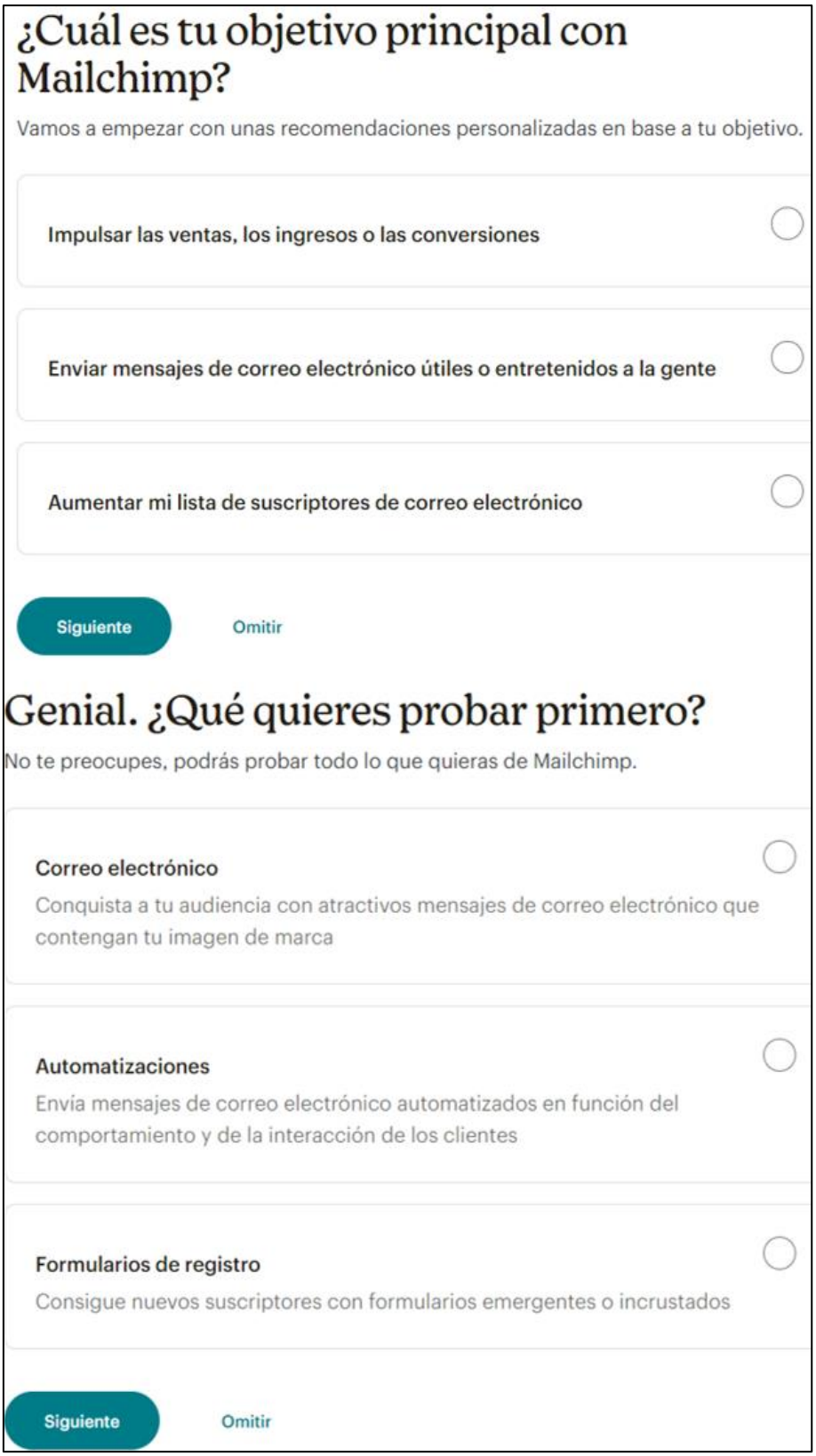


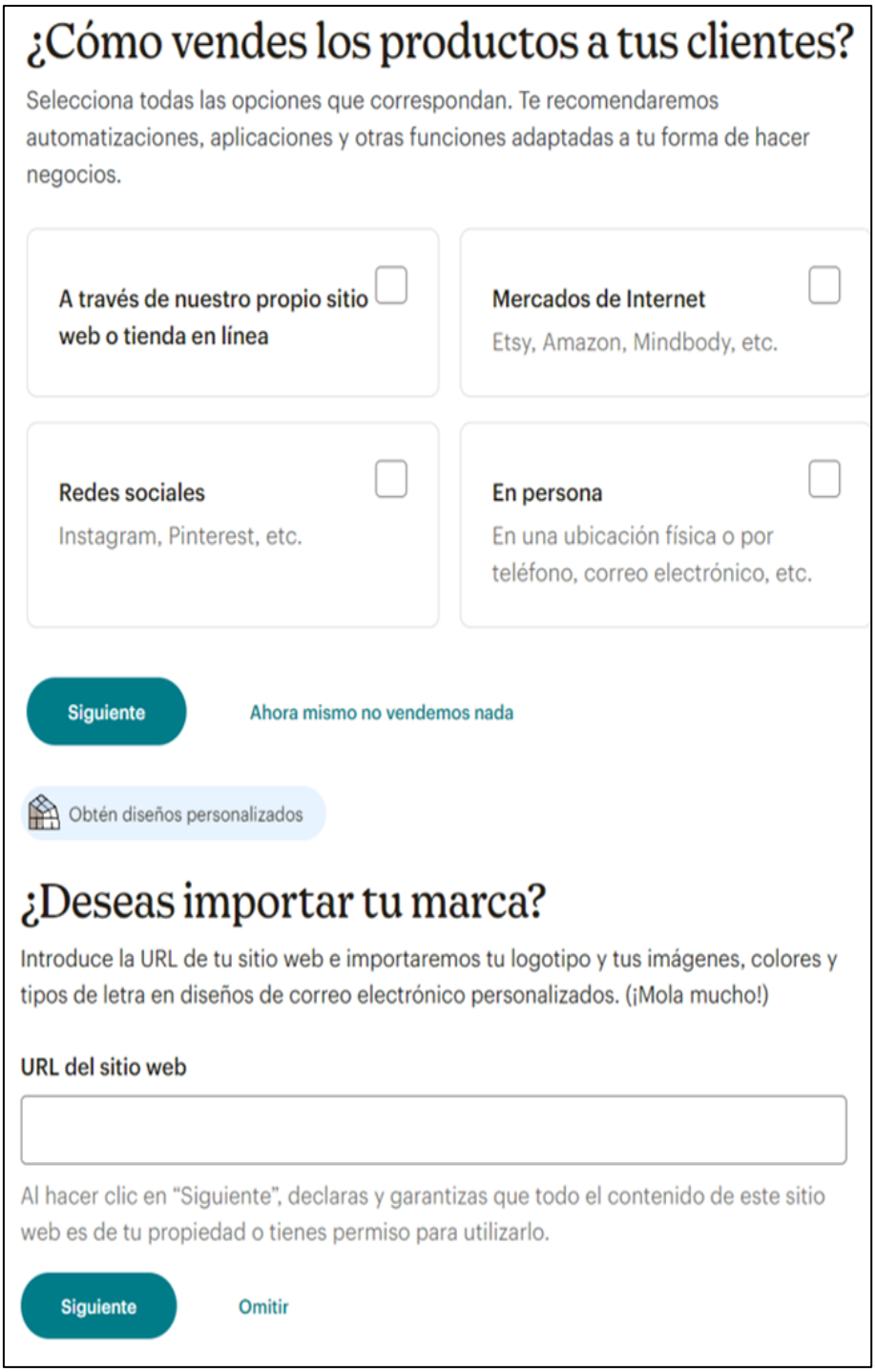
Figura 83. Correo de aprobación de MailChimp.
Fuente: Las Autoras

Paso 7: Una vez confirmada la identidad, se accederá a MailChimp. Aquí se introducirán los datos personales, junto con los objetivos a alcanzar, tal como se muestra en las siguientes figuras:

a) Configuración de los datos del usuario.



b) Configuración del objetivo principal para la que se utilizará MailChimp.



c) Configuración de análisis de las recomendaciones de correos MailChimp.

Figura 84. Configuración de una nueva cuenta de MailChimp.
Fuente: Las autoras.

Paso 8: En el siguiente paso, se elige el plan que mejor se adapte a las necesidades. En este caso, se selecciona la opción 'Plan Gratuito', como se muestra en la figura 85.

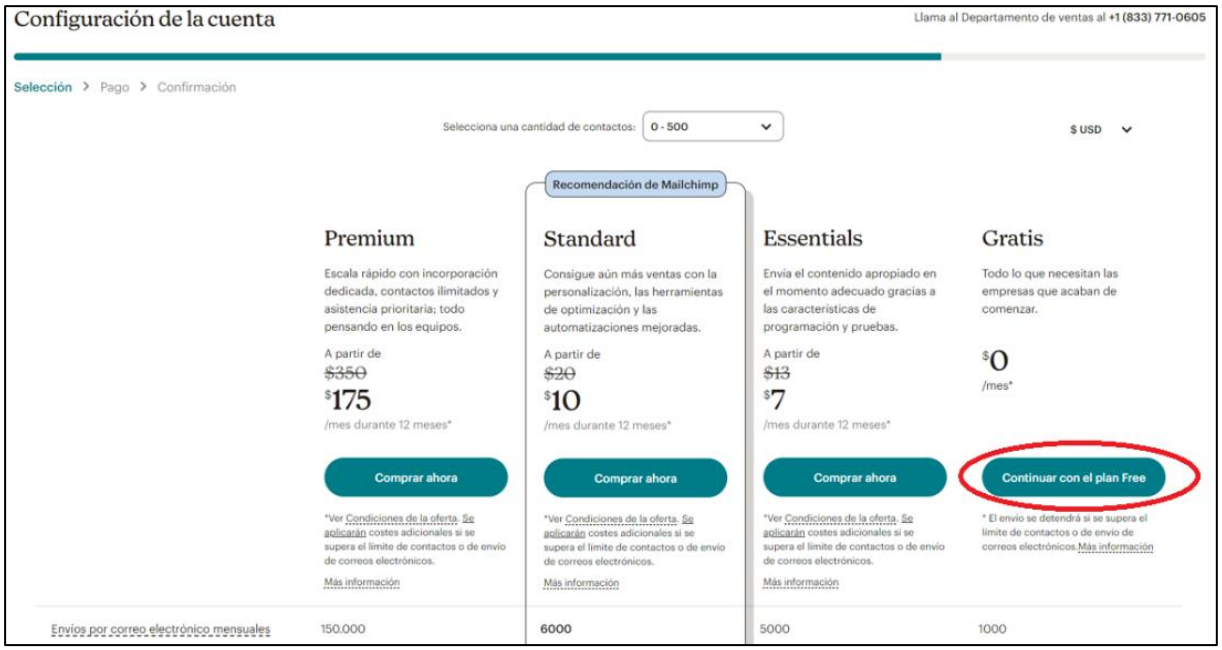


Figura 85. Selección del plan asociada a la nueva cuenta de MailChimp.
Fuente: Las autoras.

Paso 9: Se espera a que termine la configuración de la cuenta, como se muestra en la figura 85.

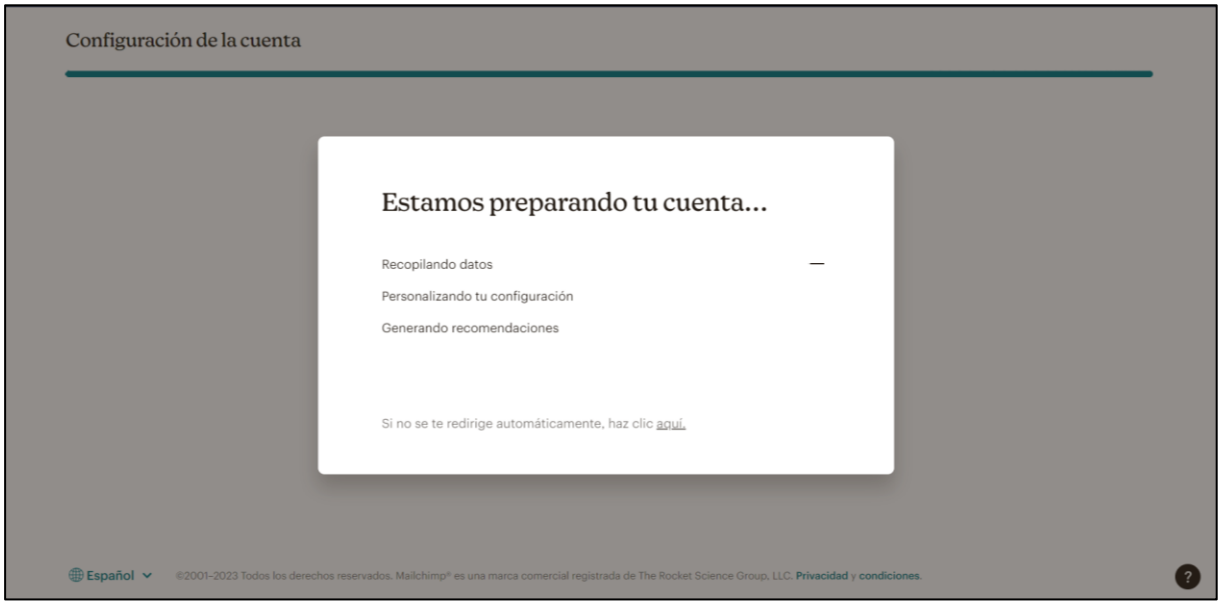


Figura 86. Proceso de creación de la nueva cuenta de MailChimp.
Fuente: Las autoras.

Paso 10: Al completar la configuración de la cuenta, se visualiza el menú de herramientas disponibles en la plataforma para crear correos personalizados, así como para enviarlos de manera masiva, como se muestra en la figura 87.

Figura 87. Página principal de la cuenta MailChimp.
Fuente: Las autoras.

Paso 11: En el siguiente paso, se dirige a la sección de “Campañas”, luego se seleccionan todas las campañas disponibles y después se hace clic en “Crear Campaña”, como se muestra en la figura 88.

Figura 88. Creación y configuración de "Campañas" en MailChimp.
Fuente: Las autoras.

Paso 12: A continuación, se ofrece la posibilidad de elegir varias opciones, y se opta por la de diseñar un correo electrónico, como se muestra en la figura 89.

Figura 89. Opciones de diseño de un correo electrónico en MailChimp.
Fuente: Las autoras.

Paso 13: Se completarán los siguientes datos para diseñar el correo electrónico, como se muestra en la figura 90.

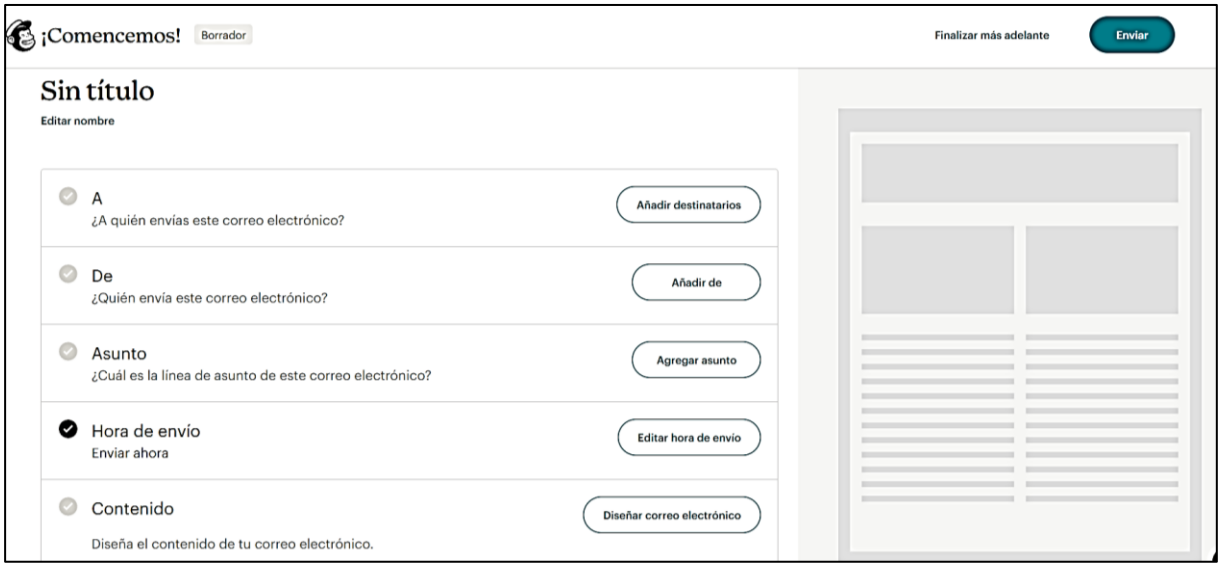


Figura 90. Partes del diseño de un correo electrónico.
Fuente: Las autoras.

Paso 14: Se ingresa el nombre, el cual para el proyecto será “Portal Cautivo”, como se muestra en la figura 91.

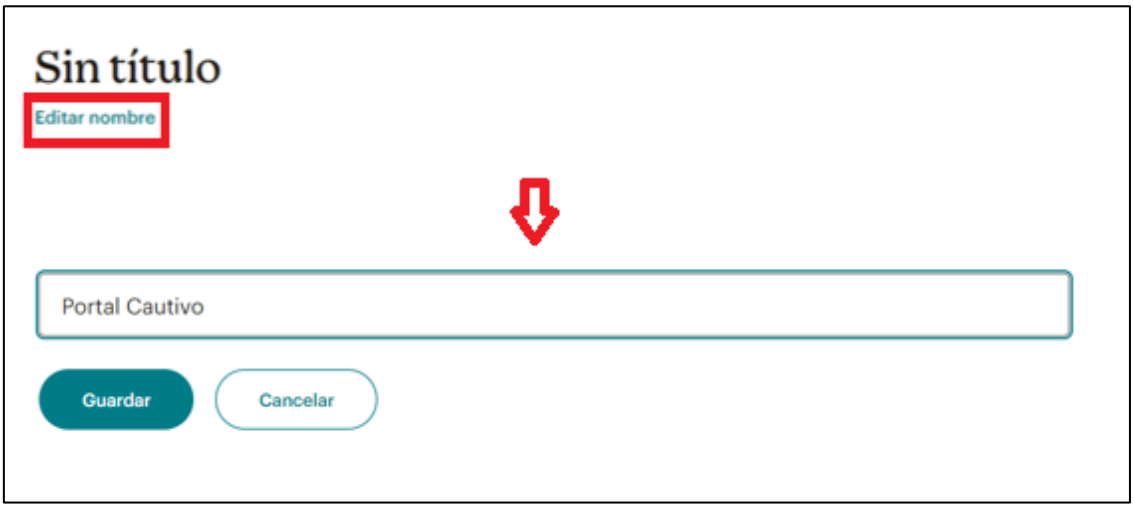


Figura 91. Título de la campaña.
Fuente: Las autoras.

Paso 15: En esta opción, “Enviar a”, se escoge a la persona que se enviará el mensaje, también permite enviar en grupo, como se muestra en la figura 92.

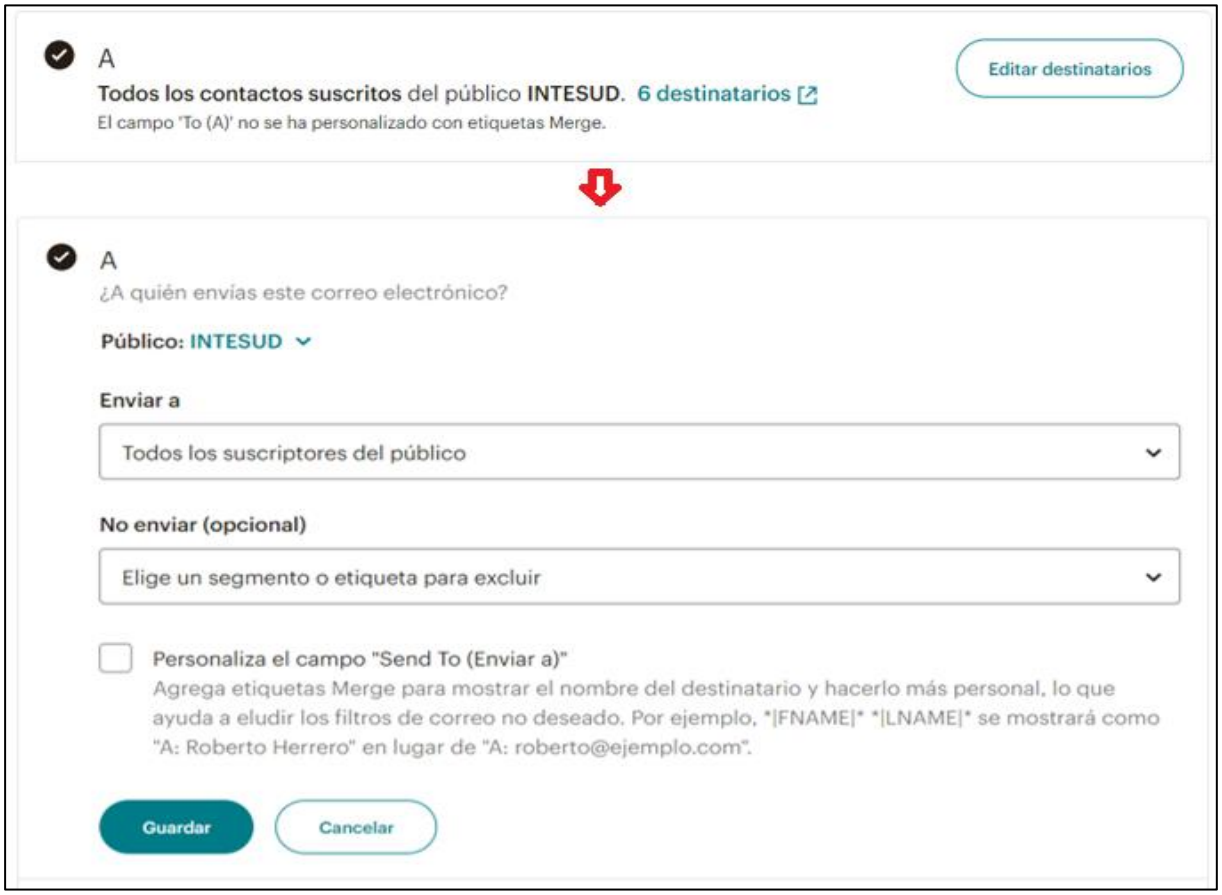


Figura 92. Selección de destinatarios para envió del correo electrónico.
Fuente: Las autoras.

Paso 16: En este paso, se selecciona la opción de importar contactos y luego se optará por cargar el archivo CSV, como se muestra en la figura 93.

Figura 93. Importación de usuarios mediante la carga de archivo CSV.
Fuente: Las autoras.

Paso 17: La persona puede elegir entre examinar el archivo o simplemente arrastrarlo, luego debe hacer clic en “Continuar”, como se muestra en la figura 94.

Figura 94. Carga y envió de archivos.
Fuente: Las autoras.

Paso 18: Se selecciona un estado, en este caso, “Suscrito”, se marca la opción “Actualizar los contactos existentes” y finalmente, se hace clic en “Continuar con el etiquetado”, como se muestra en la figura 95.

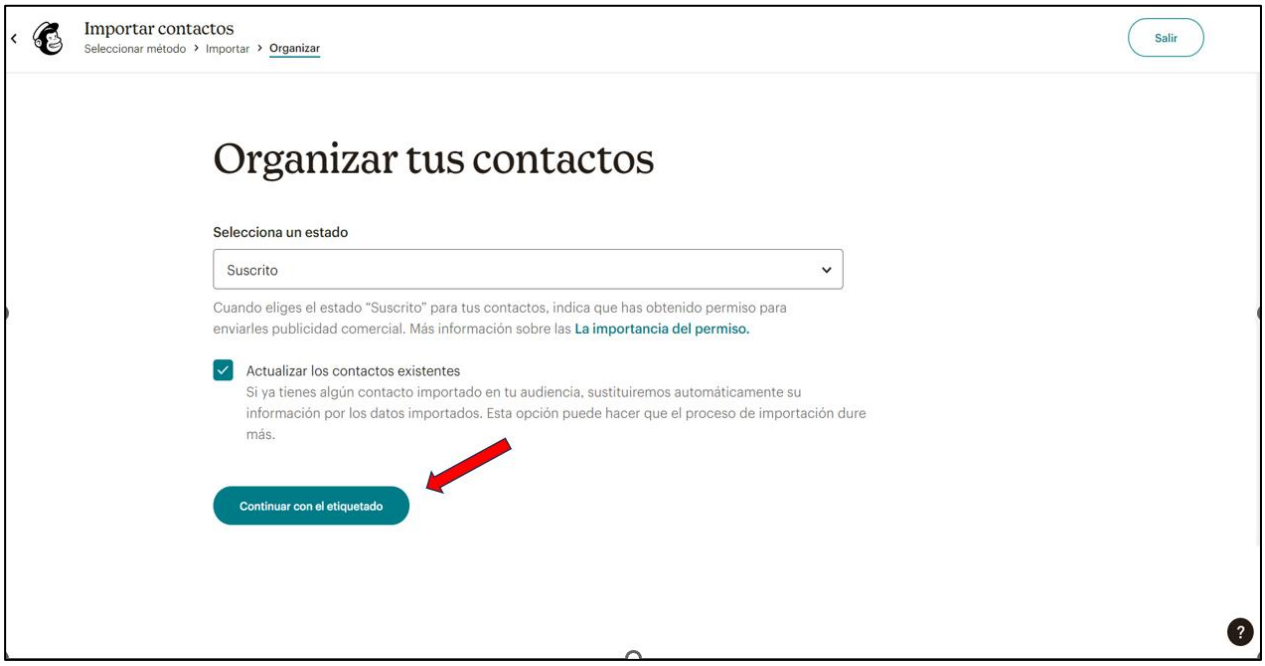


Figura 95. Organización de contactos.
Fuente: Las autoras.

Paso 19: En el etiquetado, se le da un nombre, en este caso, se llamará “Portal Cautivo”. Luego, se hace clic en “Continuar con la asociación”, como se muestra en la figura 96.

Figura 96. Etiquetado de contactos.
Fuente: Las autoras.

Paso 20: En la siguiente sección, se especifica quién será el remitente del correo, que en este caso es INTESUD, y también se indica su dirección de correo electrónico, luego hacer clic en 'Guardar', como se muestra en la figura 97.

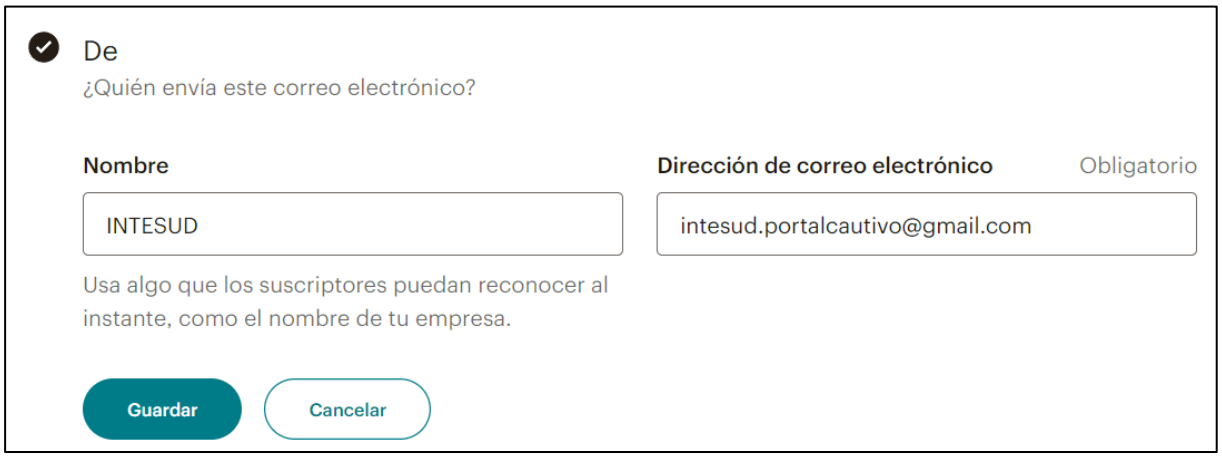


Figura 97. Detalles de ¿Quién envía este correo electrónico?
Fuente: Las autoras.

Paso 21: Aquí se designa el tema y se configura una vista previa de la comunicación que se enviará, como se muestra en la figura 98.

Figura 98. Tema designado para envío de información a usuarios.
Fuente: Las autoras.

Paso 22: La hora de envío se mantiene por defecto, como se muestra en la figura 99.

Figura 99. Hora de envió por defecto del correo electrónico.
Fuente: Las autoras.

Paso 23: En la sección de contenido, se debe hacer clic en “Diseñar correo electrónico”, como se muestra en la figura 100.

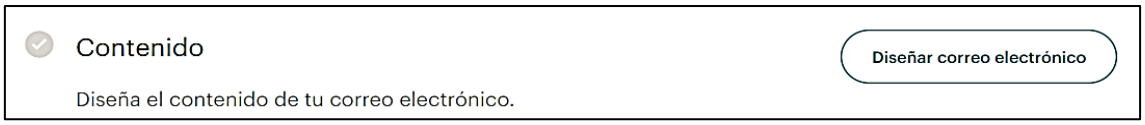


Figura 100. Diseño del contenido del correo electrónico.
Fuente: Las autoras.

Paso 24: Se presenta las opciones de seleccionar las plantillas disponibles. Sin embargo, en esta ocasión, se debe diseñar una plantilla personalizada, como se muestra en la figura 101.

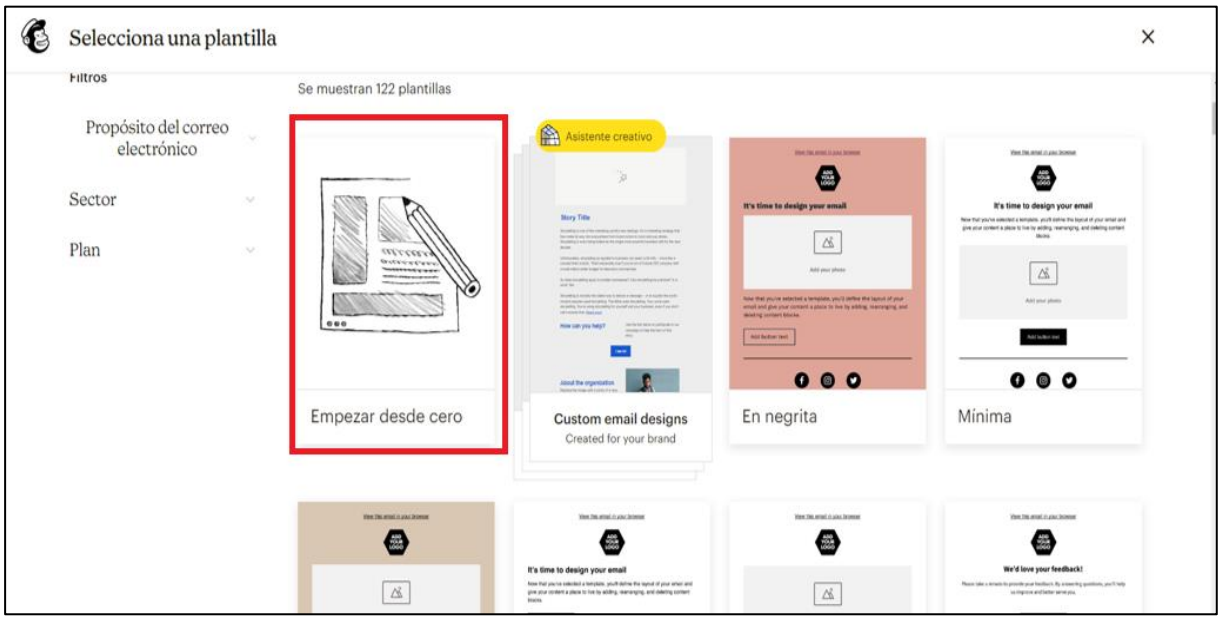


Figura 101. Plantillas de correo electrónico de MailChimp.
Fuente: Las autoras.

Paso 25: Se visualiza una plantilla base, como se muestra en la figura 102.

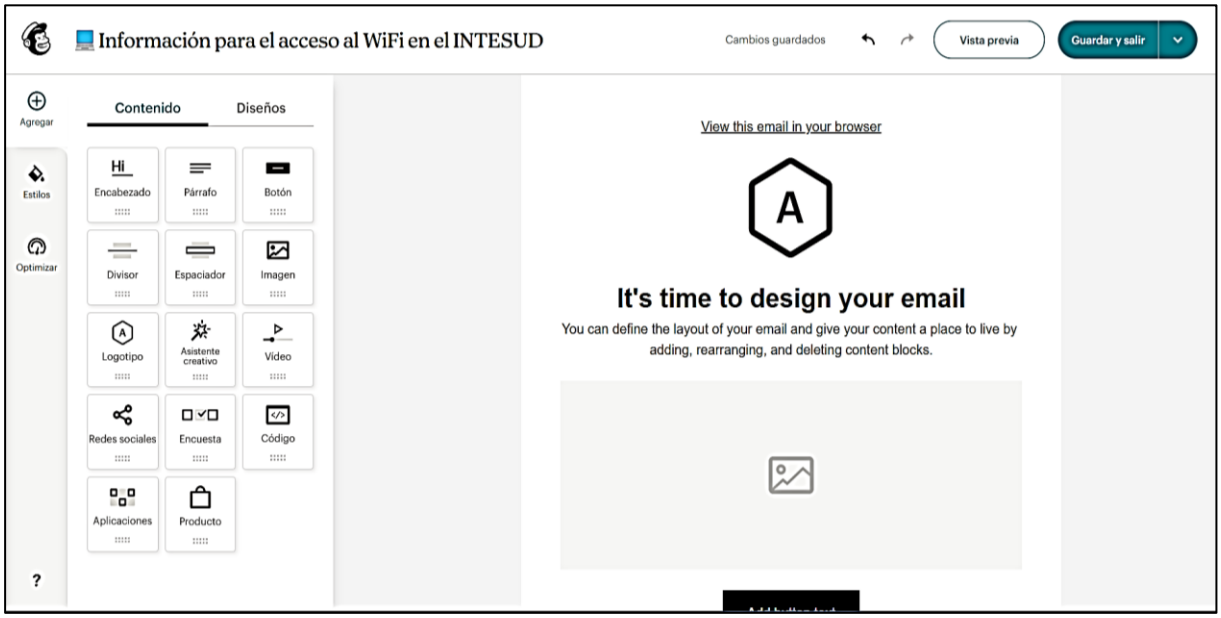


Figura 102. Plantilla base para la personalización.
Fuente: Las autoras.

Paso 26: Se deberá ingresar el logo de la institución que será utilizado para la creación de la plantilla, como se muestra en la figura 103.

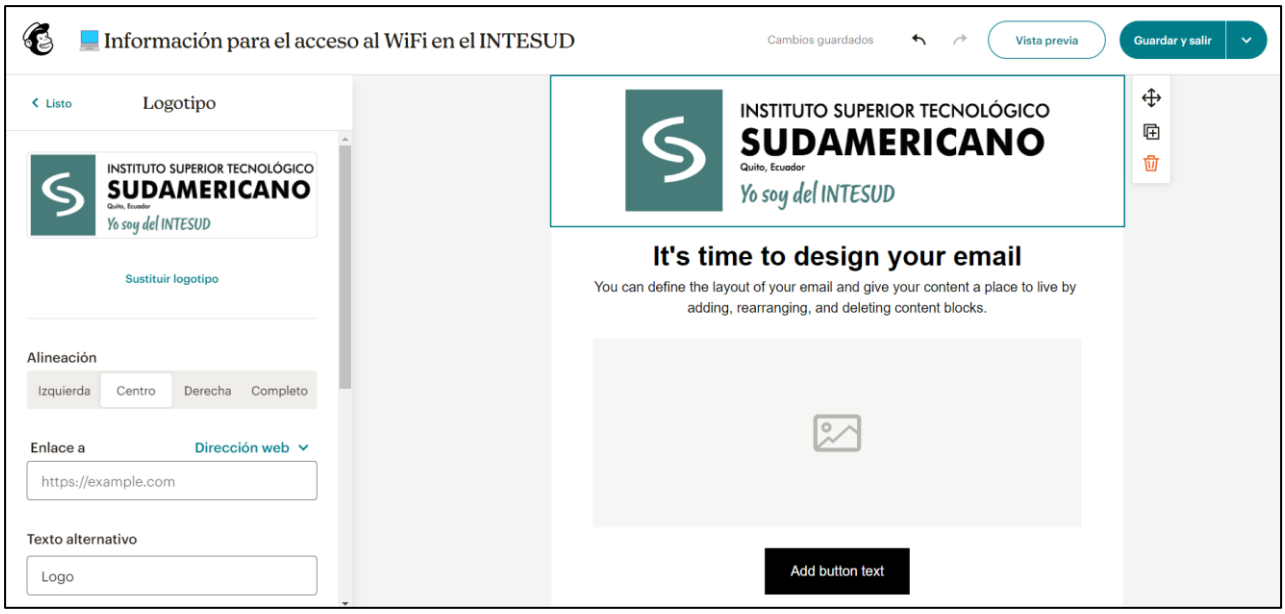


Figura 103. Personalización del correo masivo con el logo institucional.
Fuente: Las autoras.

Paso 27: Los archivos deben ser cargados en la plataforma para que luego aparezcan en el correo, como se muestra en la figura 104.

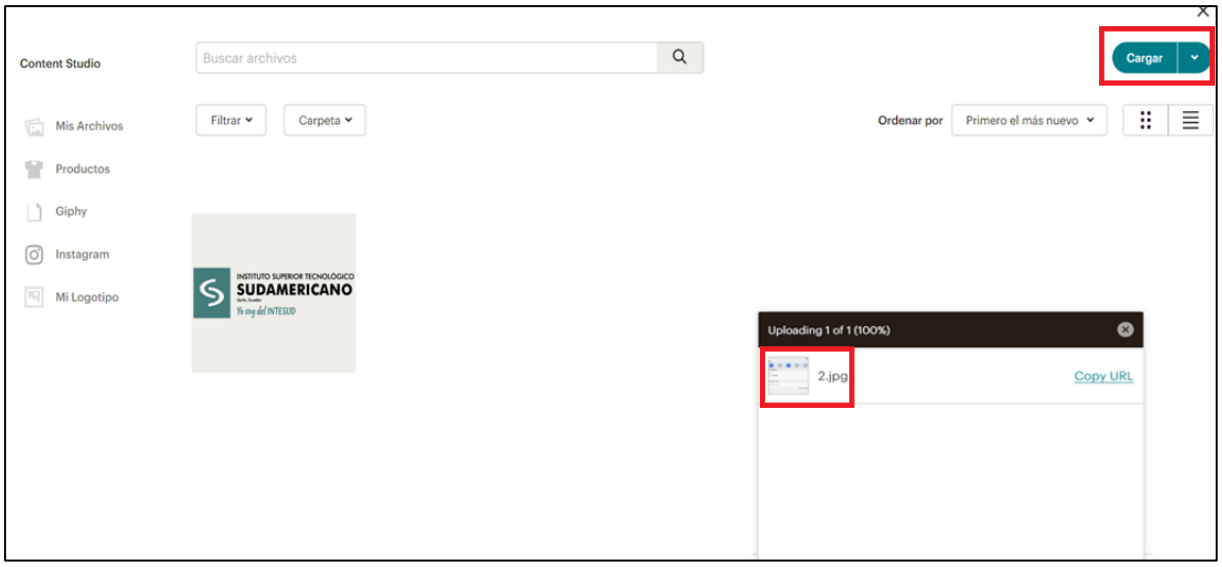
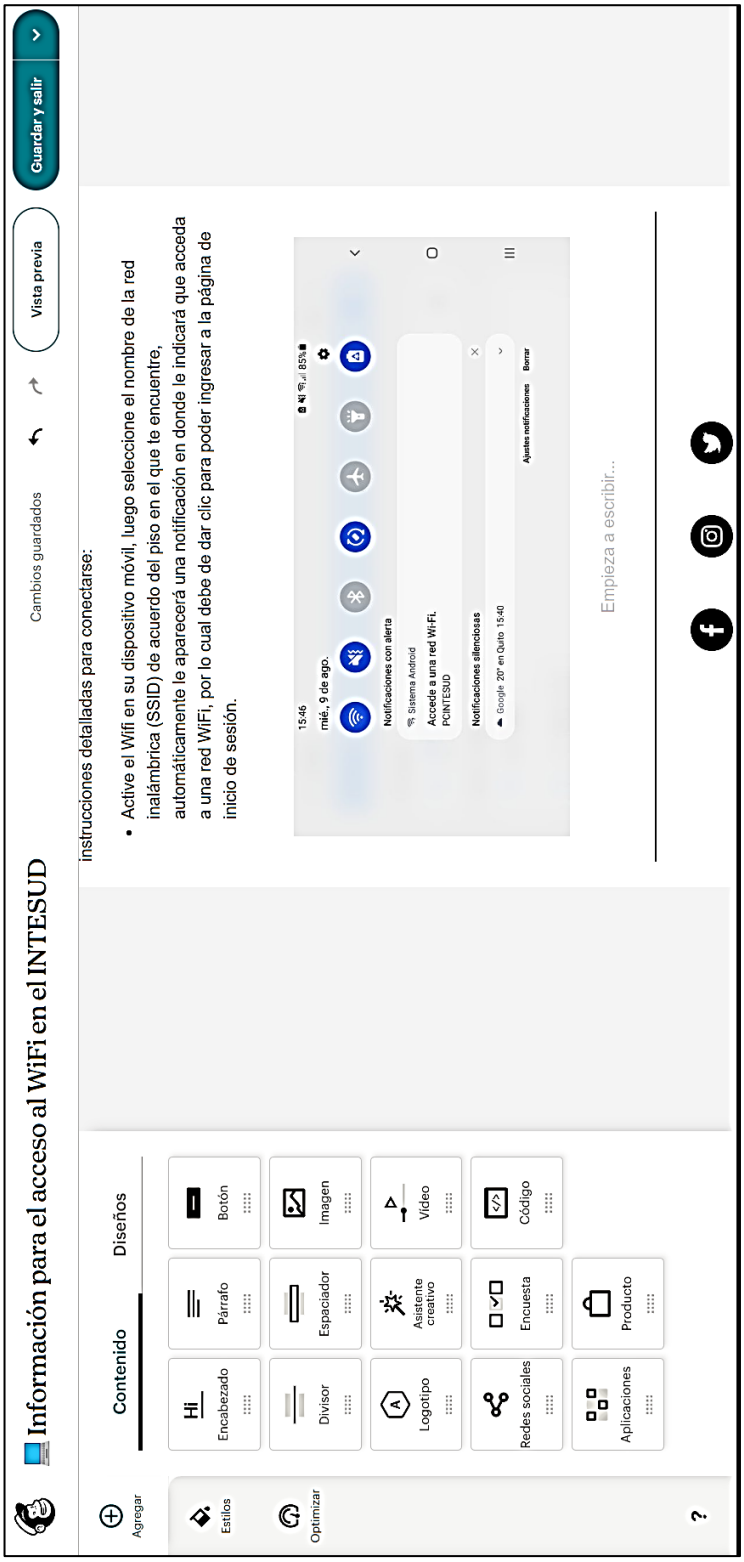


Figura 104. Carga de archivos a la plataforma MailChimp.
Fuente: Las autoras.

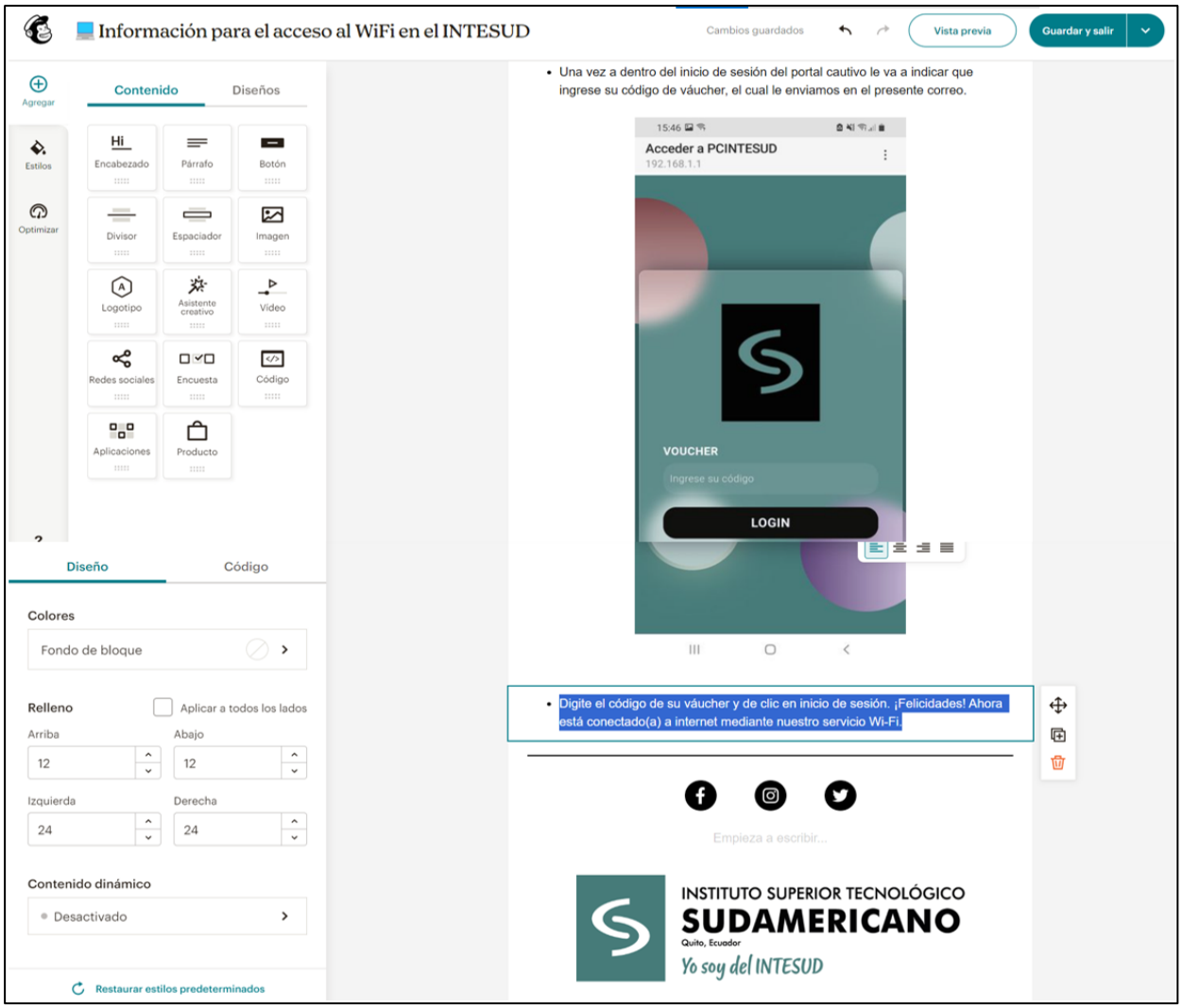
Paso 28: En el siguiente paso, se ingresa la información, donde se encuentra un punto clave, que son los "MERGE", los cuales insertan contenidos personalizados, como en este caso los nombres y el váucher para cada persona, como se muestra en la figura 105.

Figura 105. Introducción de información personalizado, envió correos masivos.
Fuente: Las autoras.

Paso 29: En el diseño de la plantilla, se detalla los pasos para que la persona que reciba el correo sepa cómo debe ingresar al portal cautivo desde su dispositivo móvil, como se muestra en las figuras 106.



a)



b)

Figura 106. Diseño de plantilla institucional para el envío de correos masivos por MailChimp.
Fuente: Las autoras.

En la siguiente figura se muestra un ejemplo del formato del correo que se envía a los estudiantes con sus credenciales e indicaciones de cómo deben conectarse a la red Wifi del edificio matriz de la Institución:

INSTITUTO SUPERIOR TECNOLÓGICO
SUDAMERICANO
Quito, Ecuador
Yo soy del INTESUD

¡Bienvenido querido estudiante!

Estimado(a) Ramos Adrian,

Recibe un cordial saludo por parte del Departamento de las Tecnologías de la Información del Instituto Superior Tecnológico Sudamericano Quito, nos emociona mucho tenerte como parte de nuestra comunidad académica y estamos aquí para asegurarnos de que tu experiencia sea excepcional desde el primer momento. Para ayudarte a conectarte con el mundo digital en nuestro edificio matriz, te proporcionamos las credenciales de acceso al WiFi y los detalles para ingresar a nuestro portal cautivo:

- Nombre de la red WiFi (SSID): INTESUD-P00X
  Donde X es el número de piso del 1 al 4.
- Contraseña de la red WiFi: yosoydelintesud
- Váucher portal cautivo: AhdPyZQx

Para acceder al internet, simplemente sigue estos pasos:

- Activa el Wifi en tu dispositivo móvil, luego selecciona el nombre de la red inalámbrica (SSID) de acuerdo al piso en el que te encuentres, automáticamente te aparecerá una notificación muy similar a la siguiente imagen para que puedas dar clic en ella y así ingresar a la página de inicio de sesión:

a)

- Luego visualizarás la página de ingreso como lo observas en la siguiente imagen.

- Como observas en la imagen anterior, hay un apartado en donde te indica que ingreses el código del váucher. Una vez ingresado el código, haz clic en el botón "LOGIN".

b)

¡Felicidades! Ahora estás conectado(a) a internet mediante nuestro servicio WiFi.

En este nuevo periodo académico, te animamos a abrazar cada oportunidad de aprendizaje y crecimiento. Cada día en el Instituto Superior Tecnológico Sudamericano Quito es una nueva ocasión para descubrir, conectar y superarte. Estamos aquí para apoyarte en tu trayecto educativo y deseamos que este periodo sea lleno de logros y satisfacciones.

No dudes en contactarnos si necesitas cualquier tipo de ayuda, el Departamento IT está a tú disposición a través del correo electrónico departamento.it@sudamericanoquito.edu.ec.

¡Estamos emocionados de tenerte a bordo y te deseamos mucho éxito en este emocionante viaje académico!

¡Adelante, empieza tu camino con energía y entusiasmo!

INTESUD

Has recibido este correo electrónico porque lo has aceptado en nuestro sitio web.

c)

Figura 107. Ejemplo de correo electrónico masivo para la socialización del ingreso al Wifi por váucher. Fuente: Las autoras.

6.4. Servidor NAS Synology

Para cumplir con el objetivo de implementar un Sistema de Almacenamiento en Red (NAS) que soporte la centralización y el acceso seguro a los archivos y recursos compartidos de la institución exclusivamente por la red LAN, se instaló el servidor Synology Disk Station Manager 7.2, conocido como DSM7.2, bajo las razones presentadas en la página 81 de este documento.

Por lo tanto, para el presente proyecto, se implementó este útil servidor para proporcionar un servicio adicional a la comunidad institucional que trabaja en el edificio matriz. En sentido de las VLAN, este servidor solo estará disponible para la VLAN 1, es decir, estará disponible solo para el área administrativa. Se le designó la dirección IPv4: 192.168.1.253 con el puerto 5000, manteniendo el orden de distribución de direciones de red estáticas manejada por el Departamento de Tecnologías de la Información del Instituto.

Se aclara que, la VLAN 8 ha sido configurada para el área académica o de laboratorios, ofreciendo un espacio independiente, lo que permite realizar actividades de investigación o aprendizaje en una subred dedicada a ello. Cabe mencionar que el área académica o laboratorios no tendrán acceso al servidor NAS, ya que este, está destinado únicamente al personal administrativo.

Se muestra a continuación una ilustración de la topología de red administrativa, dando énfasis a los servidores disponibles en el edificio matriz:

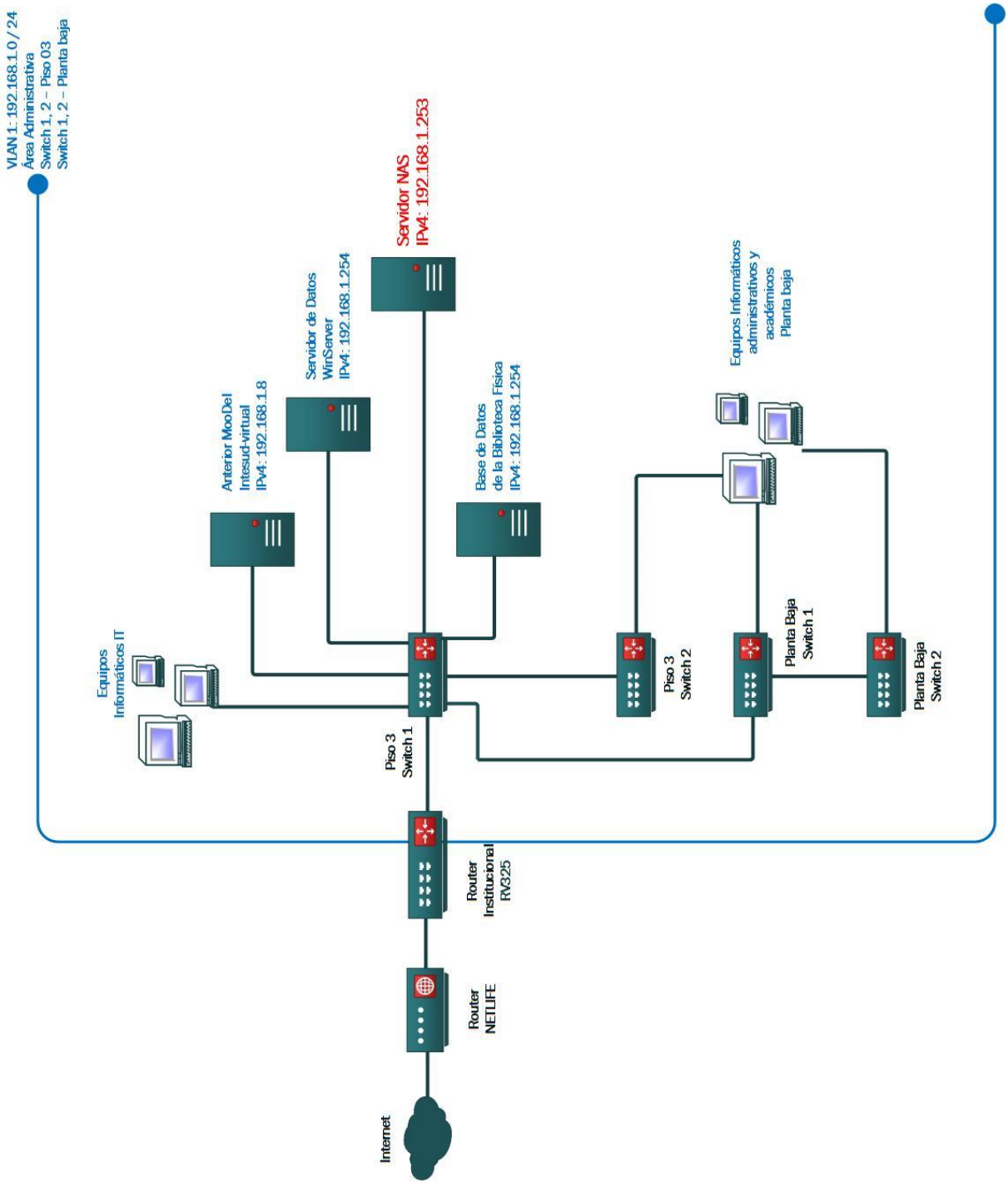


Figura 108. Topología de red administrativa y sus servidores.
Fuente: Las autoras.

6.4.1. Instalación y configuración del servidor NAS Synology DSM 7.2

La instalación y configuración del servidor NAS Synology con DSM 7.2 en el Instituto Superior Tecnológico Sudamericano Quito (INTESUD) se completó siguiendo una serie de pasos meticulosamente ejecutados:

1. *Preparación de hardware*. Se confirmó que el hardware del servidor NAS Synology estaba configurado adecuadamente, nuevamente el Departamento IT de la Institución facilitó un servidor HP que cumple con las siguientes características:
    - Arquitectura Electrónica Servidor Tower
    - Modelo HP Proliant ML310E Gen8 V2
    - Fuente de poder (capacidad) 750 W
    - Procesador Intel Pentium Intel® Xeon® E3-1200 v3
    - Sistema Operativo Linux ClearOS 6
    - Disco Duro 2 TB. No RAID, 7.2K RPM SATA 3.5 in Cabled Hard Drive
    - Memoria RAM 8GB DDR3
    - NIC (RJ45) 10/100/1000 Mbps
    - Respaldo energético UPS INS 725DA
2. *Preparación de la Llave DiskStation Manager (DSM) 7.2*. Como se tratase de una USB arrancable por computadora, con cualquier ISO de un sistema operativo.
3. *Conexión de red*. Se conectó el servidor NAS a la red local del instituto (LAN) utilizando un cable Ethernet para garantizar una conexión estable.
4. *Acceso al DSM*. A través de un navegador web en una computadora también conectada a la red del instituto en la VLAN 1, se ingresó a la interfaz del servidor NAS Synology usando la dirección IP asignada.

5. *Configuración inicial*. La primera vez que se accedió al servidor NAS mediante su dirección IP, se inició el proceso de configuración donde se estableció una cuenta de administrador y una contraseña robusta.
6. *Licencia y acuerdos*. Se aceptaron los términos de licencia y acuerdos de servicio presentados durante la configuración.
7. *Selección de volumen*. Se creó un volumen de almacenamiento en un único disco duro disponible.
8. *Instalación de DSM*. Se utilizó la versión de DSM 7.2.
9. *Personalización de ajustes*. Se personalizaron varios ajustes durante la configuración, incluyendo el nombre del servidor, la configuración de la zona horaria y las preferencias de actualización automática.
10. *Finalización*. Finalizada la configuración inicial, se accedió al escritorio de DSM, la interfaz de administración del servidor NAS Synology, donde se configuraron las carpetas compartidas, los usuarios y los permisos.
11. *Aplicaciones y servicios adicionales*. Además, se instalaron aplicaciones y servicios adicionales desde el Package Center de DSM para expandir las capacidades del servidor NAS y satisfacer los requerimientos adicionales del instituto.

Con estos pasos, el INTESUD aseguró una implementación exitosa del servidor NAS Synology, lo que le permitirá mejorar significativamente la gestión de sus recursos digitales y la centralización de sus datos solo dentro de la red interna del edificio matriz. Para el exterior ya se cuenta con tecnologías como Microsoft 365.

Pasos para la personalización y configuración del servidor NAS Synology

Paso 1: Tras conectar el cable de red, se enciende el servidor NAS, lo que hace que su propio Shell esté disponible. Se puede acceder a él desde otro ordenador utilizando la dirección IP que aparece en el Shell, como se muestra en la siguiente figura:

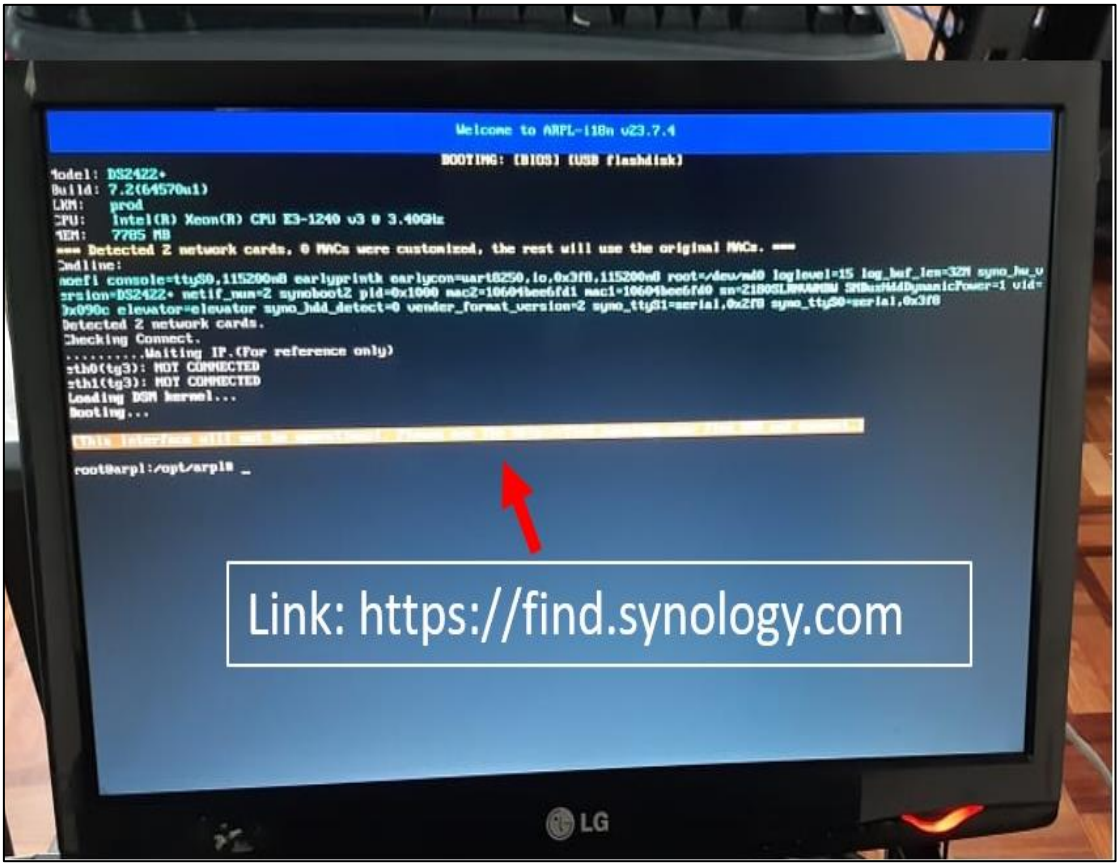


Figura 109. Terminal del servidor NAS.
Fuente: Las autoras.

Paso 2: Desde otro ordenador, se establece una conexión con el servidor NAS al ingresar la dirección IP fija **http://192.168.1.253:5000** en la barra del navegador web, lo que permite la carga de la interfaz de usuario del NAS. Al no contar con un servidor con DNS, no se le asignó un nombre de dominio al servidor NAS y se utilizará su IP y puerto para acceder a él. Esto se muestra en la siguiente figura:

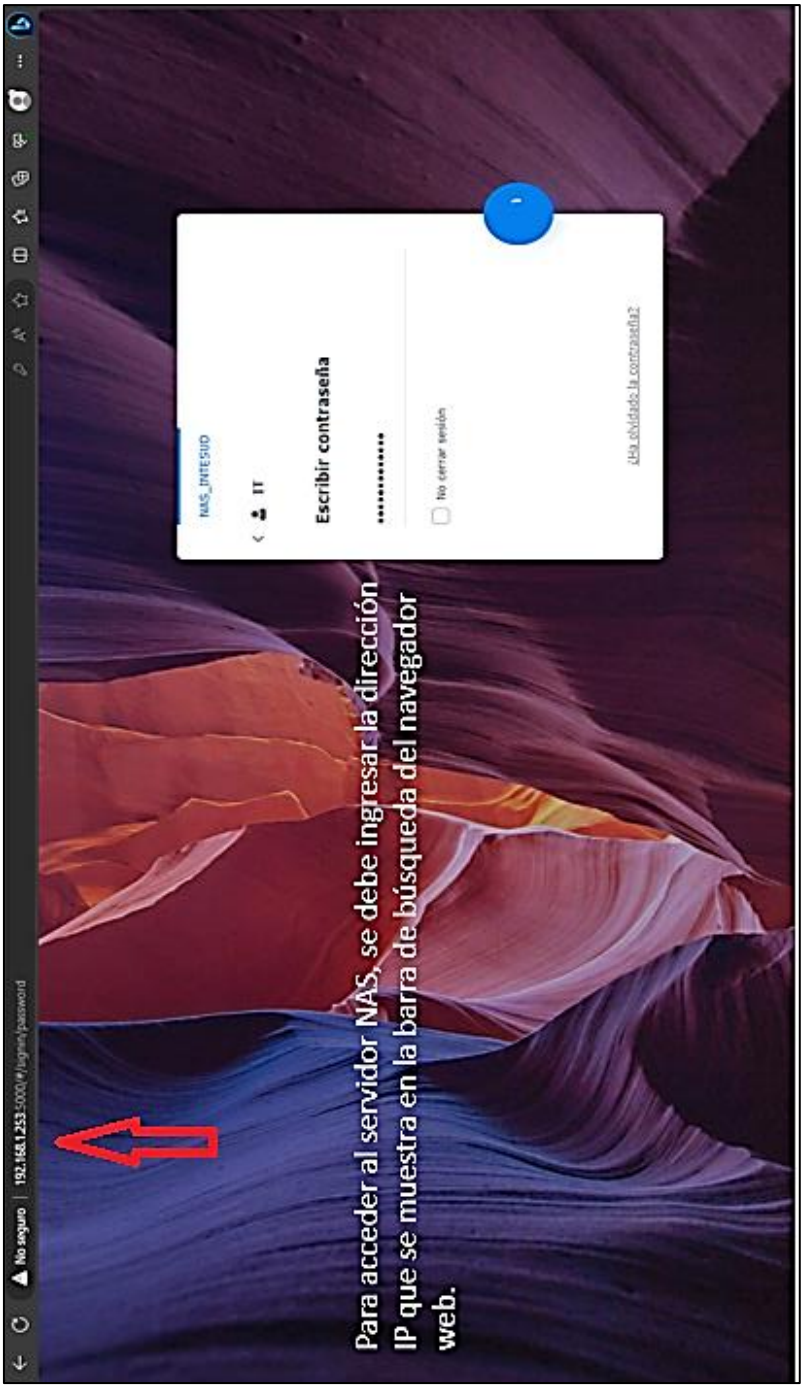


Figura 110. Acceso al servidor NAS Synology por navegador web.
Fuente: Las autoras.

Paso 3: Una vez ingresada la dirección IP, se despliega la pantalla de inicio de sesión del servidor NAS. En este punto, se introduce el nombre de usuario y la contraseña correspondiente. A partir de ese momento, se puede comenzar con la personalización y la carga de los archivos deseados, como se muestra en la siguiente figura:

Figura 111. Pantalla de inicio del Login del servidor NAS.
Fuente: Las autoras.

Paso 4: Una vez dentro del servidor NAS, se procede con la personalización, lo que implica la descarga de las aplicaciones que se usará. Para ello, se dirige al "Centro de Paquetes," donde

se encuentra las aplicaciones y que mejoran la funcionalidad del servidor NAS, como se muestra en la figura 111.

Figura 112. Descarga de aplicaciones en el servidor NAS.
Fuente: Las autoras.

Paso 5: A la izquierda, se encuentra la opción "Todos los paquetes". Desde ese punto, se procede a buscar e instalar las aplicaciones para el servidor NAS, como se muestra en la siguiente figura 112:

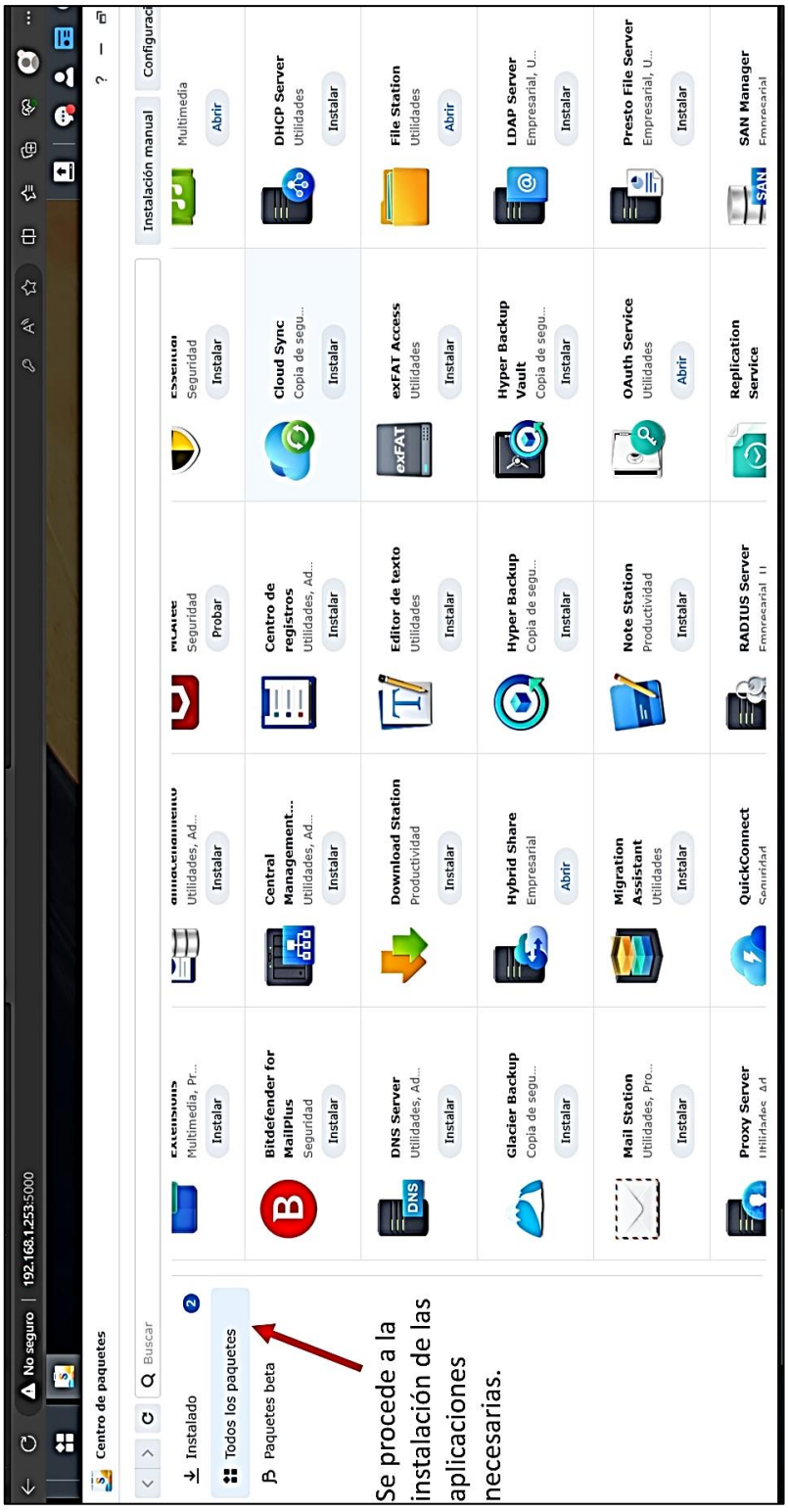


Figura 113. Centro de paquetes de instalación de aplicaciones del servidor NAS.
Fuente: Las autoras.

Paso 6: Se deberá verificar que las aplicaciones “File Station”, “Audio Station”, “Photos”, y “Video Station” estén descargadas, como se muestra en las siguientes figuras.

La siguiente figura es una captura de pantalla que muestra la Estación de archivos ubicación de archivos multimedia:

Figura 114. Estación de archivos, ubicación de archivos multimedia.
Fuente: Las autoras.

La siguiente figura es una captura de pantalla que muestra el gestor de música Audio Station:

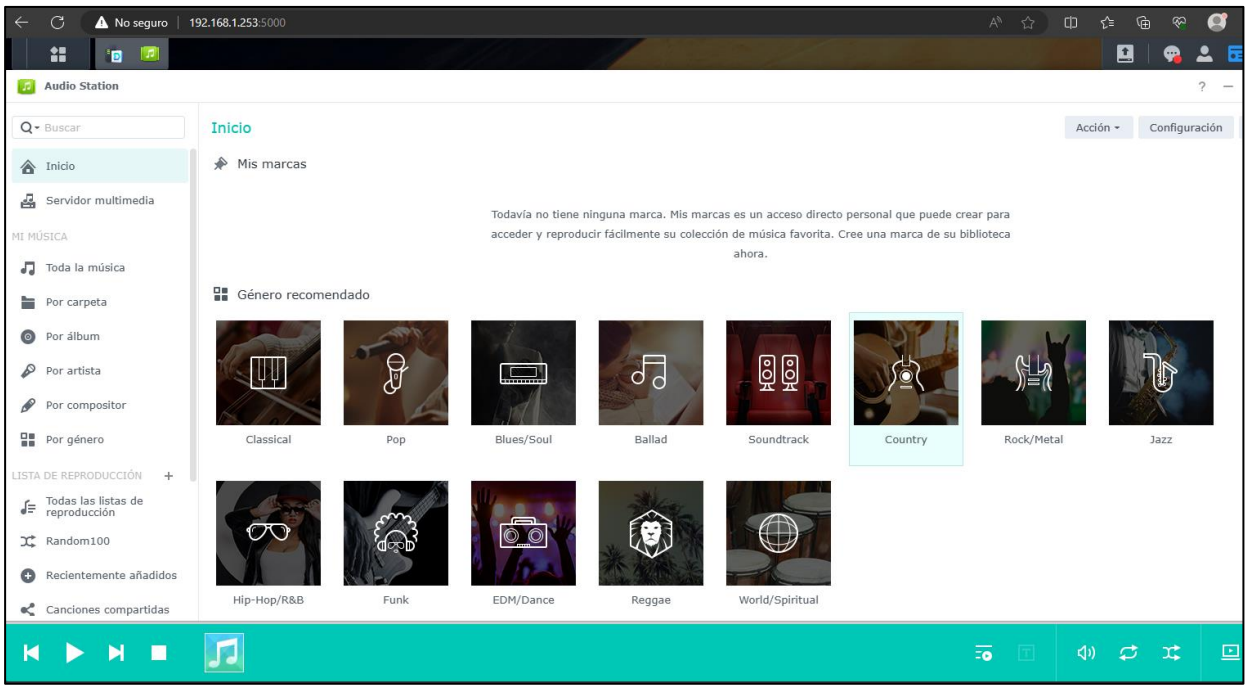


Figura 115. Audio Station, reproductor de música o gestor de música.
Fuente: Las autoras.

La siguiente figura es una captura de pantalla que muestra la Aplicación “fotos” donde se ubican los archivos de imágenes de usuario:

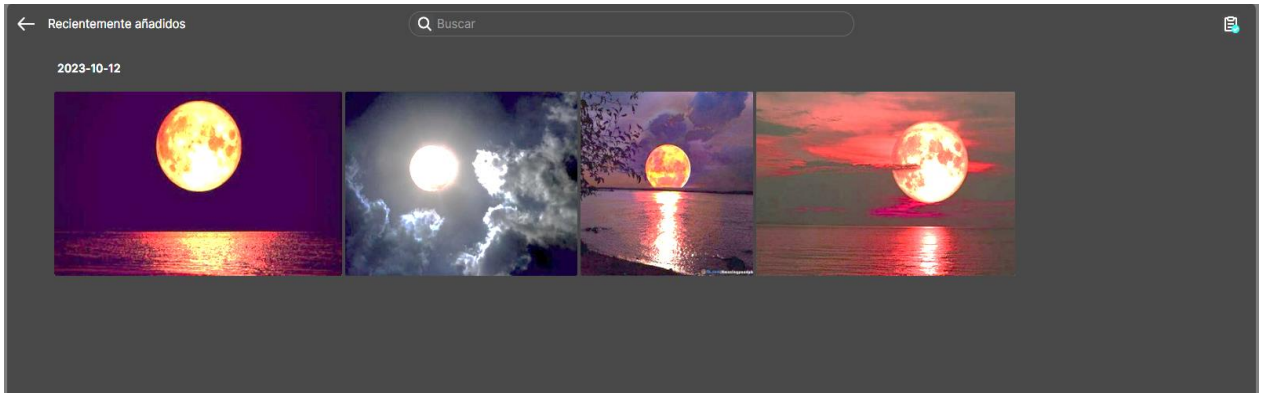


Figura 116. Aplicación “fotos” donde se ubican los archivos de imágenes del usuario.
Fuente: Las autoras.

La siguiente figura es una captura de pantalla que muestra el reproductor de vídeos Video Station:

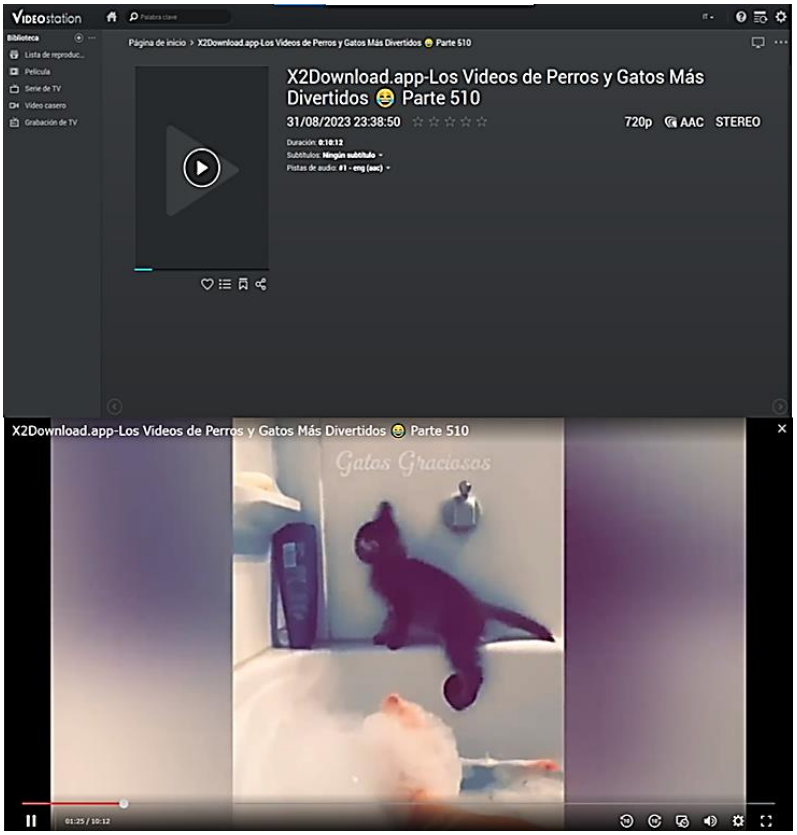


Figura 117. Video Station, reproductor de videos y de películas.
Fuente: Las autoras.

Paso 7: Para la gestión de archivos se procede con la descarga del Synology Drive para crear una carpeta compartida, configurar al usuario y, a partir de ese punto, descargar las aplicaciones tanto en el escritorio como en el celular, ya que al servidor solo se puede acceder por navegador, como se muestra en la figura siguiente.

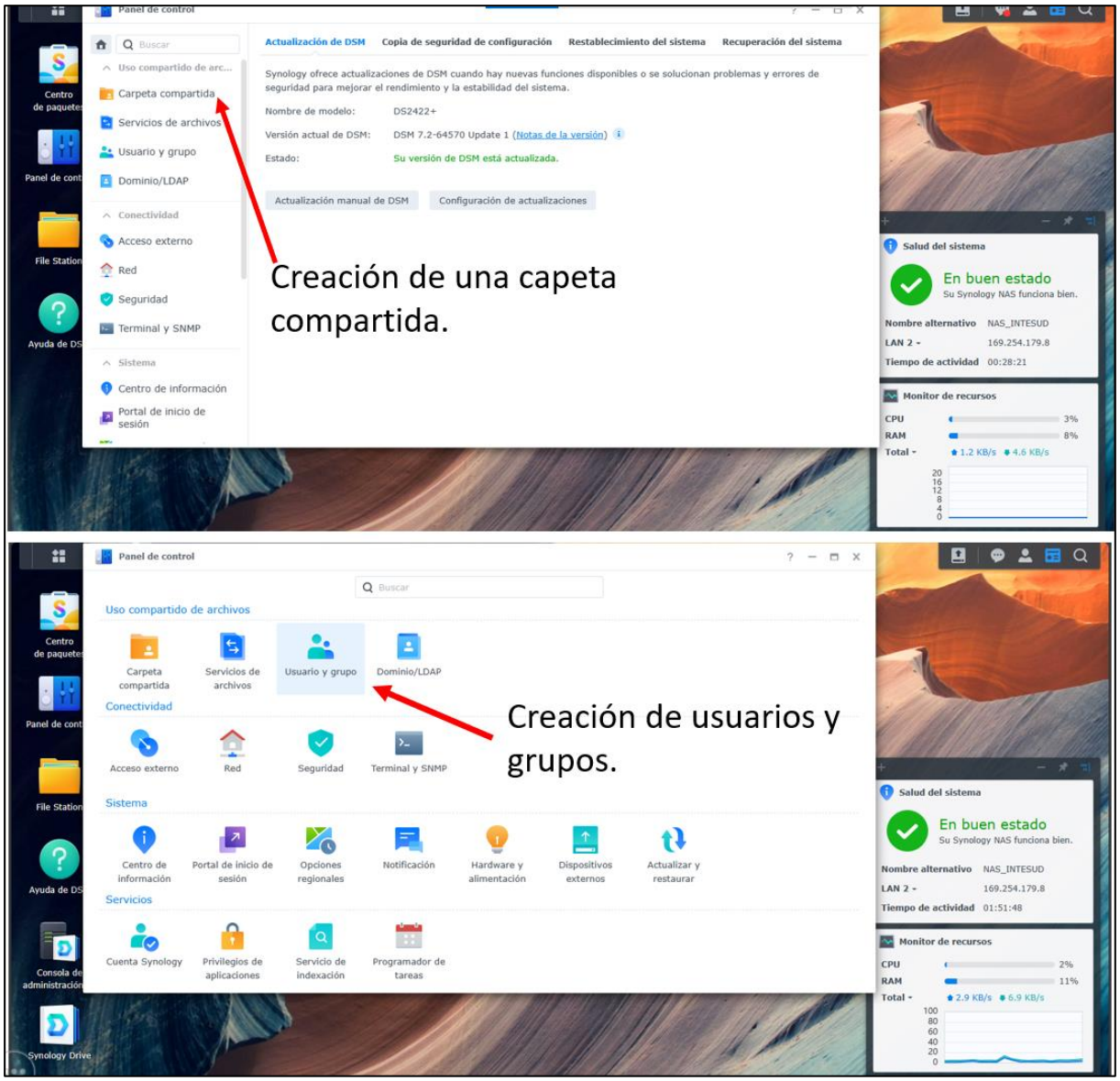


Figura 118. Configuración de usuario y de carpeta compartida.
Fuente: Las autoras.

Paso 8: Una vez creada la carpeta en el Drive, los archivos podrán sincronizarse, ya sea accediendo desde otro ordenador o un celular donde se tenga instalada la aplicación de Synology Drive, como se muestra en la siguiente figura:

Figura 119. Drive (carpeta compartida), sincronización de los archivos.
Fuente: Las autoras.

Paso 9: Se procede a dirigirse al Drive nuevamente; luego, se ubica en la opción "compartido conmigo". En esta sección, se desplegará un enlace que dice "acceda a Synology Drive desde cualquier lugar". Esta opción cumple con la función de proporcionar las aplicaciones necesarias, tanto para el escritorio como para dispositivos móviles, como se muestra en la siguiente figura:

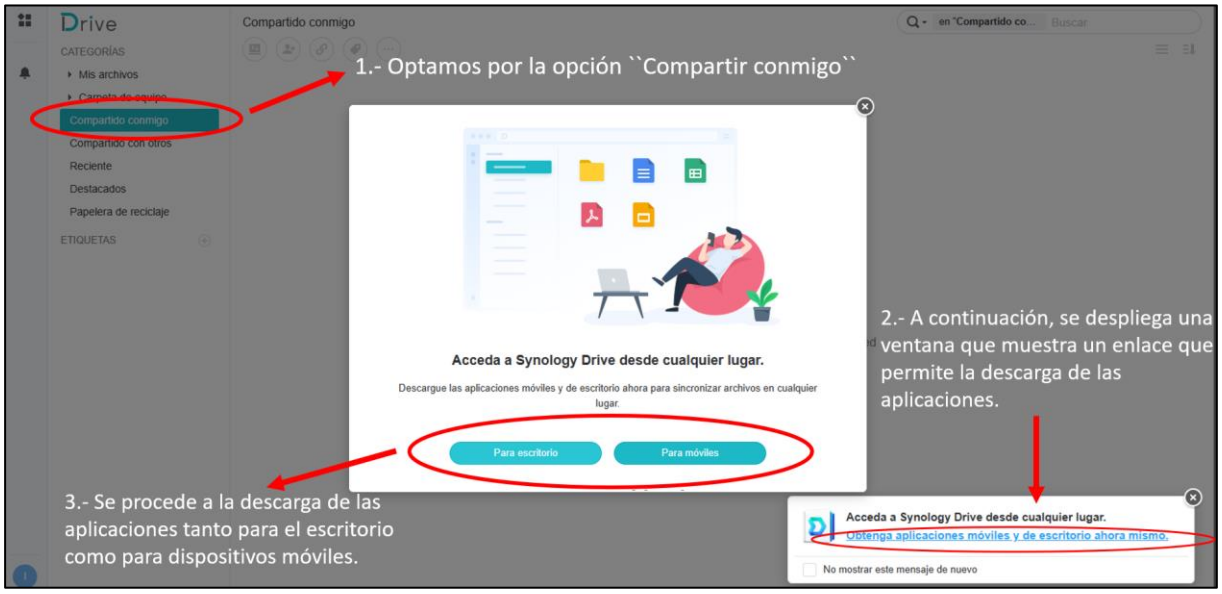


Figura 120. Drive, descarga de aplicación para escritorio y celular.
Fuente: Las autoras.

Paso 10: Al dar clic en el enlace, se descargará el programa de Synology Drive Client, que son las aplicaciones para el escritorio. Se ejecutará el programa y se deberá dar clic en aceptar, lo que desplegará otra ventana que dará la bienvenida, la cual mostrará las carpetas y aplicaciones. Luego, se da clic en "comenzar ahora", como se muestra en la siguiente figura:

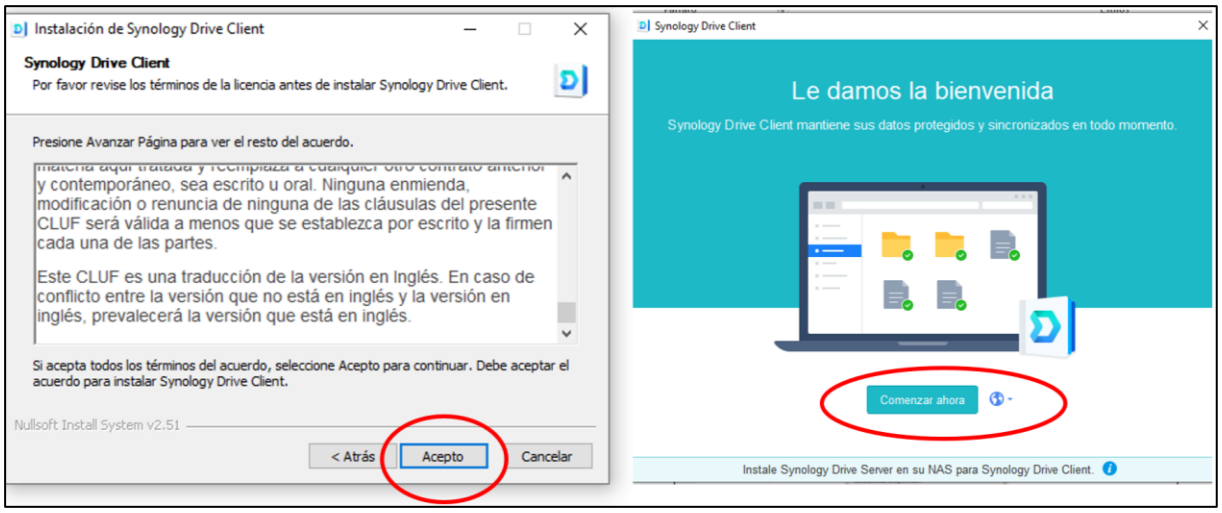


Figura 121. Ejecución de programa Synology Drive Client.
Fuente: Las autoras.

Paso 11: En la siguiente ventana, se pedirá la creación de los usuarios, la configuración para las carpetas de sincronización y dónde se ubicará la carpeta, permitiendo así su uso en beneficio de los usuarios, como se muestra en la siguiente figura:

Figura 122. Configuración de las carpetas de sincronización.
Fuente: Las Autoras.

Paso 12: El enlace para descargar las aplicaciones ofrece la opción para iOS y Android. Se escanea el código QR y esto dirigirá a un enlace de Synology Drive, desde donde se descargará una aplicación que permitirá conectarse al servidor NAS, como se muestra en la siguiente figura:

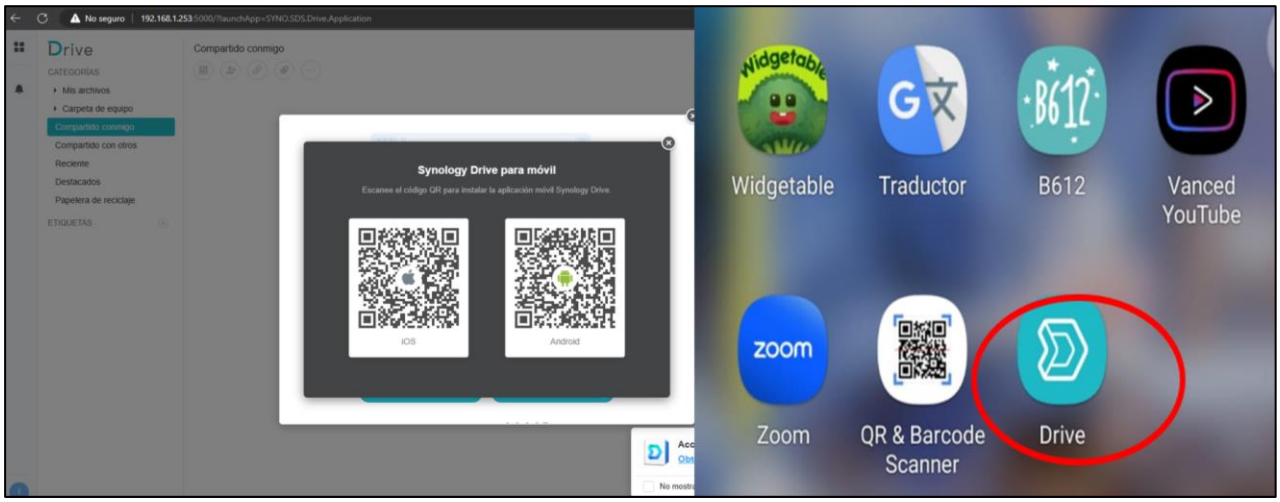


Figura 123. Descargar aplicaciones en el celular desde Synology Drive para móvil.
Fuente: Las autoras.

Paso 13: El enlace para descargar las aplicaciones ofrece la opción para iOS y Android. Al escanear el código QR, se es dirigido a un enlace de Synology Drive, desde donde se descargará una aplicación que permitirá la conexión al servidor NAS, como se muestra en la siguiente figura:

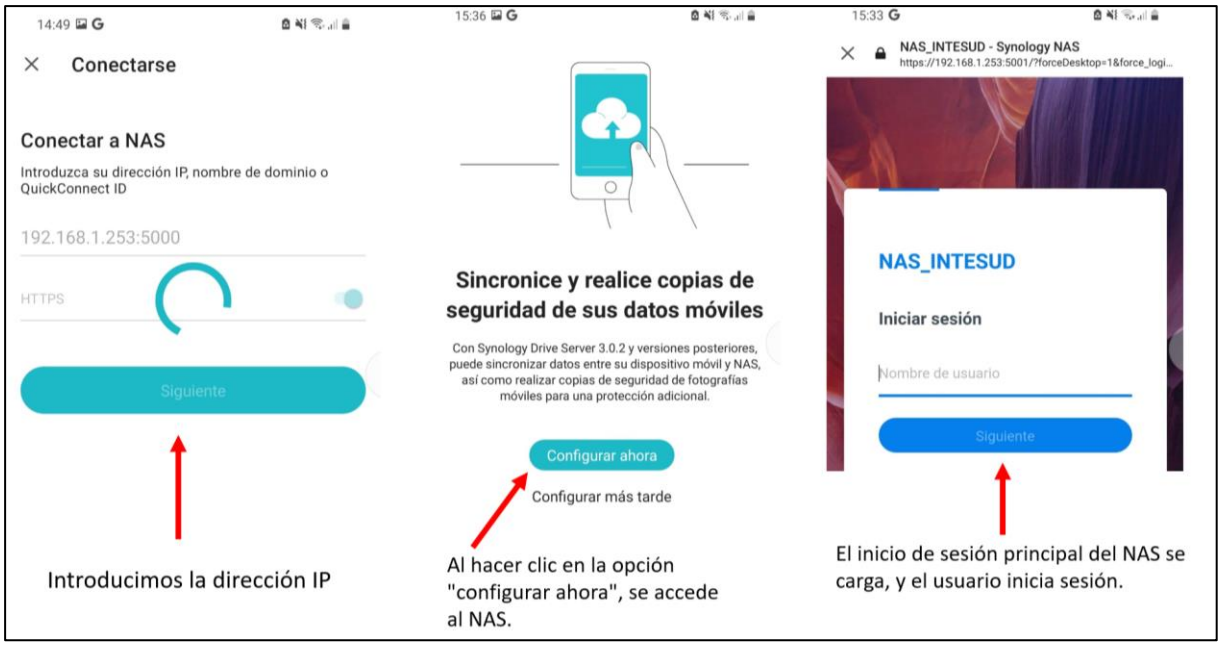


Figura 124. Acceso al servidor NAS desde un celular.
Fuente: Las autoras.

6.4.2. Creación de Usuarios y Grupos

Una vez configurado el servidor NAS, se procedió con la creación de grupos para clasificar cada departamento dentro del Instituto Superior Tecnológico Sudamericano Quito. Antes de crear estos grupos, se ingresaron a los usuarios asignándoles una contraseña para cada uno de ellos que les permitirá acceder al NAS y utilizando el correo institucional como identificador de usuario. Posteriormente, se realizó la asignación de cada usuario al grupo correspondiente a su departamento. El administrador siempre será quien asigne privilegios de acceso a las carpetas compartidas, archivos o aplicaciones, por lo cual en el perfil de cada usuario le aparece únicamente lo que el administrador asignó, como se muestra en las siguientes figuras.

Los grupos que se crearon son: Rectorado, departamento de Recursos Humanos, Departamento Financiero, Secretaría, Departamento IT, Departamento de Marketing y Comunidad.

A continuación, se tiene la tabla de los miembros administrativos, sus correos electrónicos y sus contraseñas:

Nombre	Correo	Descripción	Contraseña
Alisson Tapia	talento.humano@sudamericanoquito.edu.ec	Talento humano	Atapia1
Andrés Herrera	administración.empresas@sudamericanoquito.edu.ec	Administración empresas	Aherrera
Belén Hernández	vinculacion.ppp@sudamericanoquito.edu.ec	Vinculación	Bhernandez1
Cristian Martínez	gastronomia@sudamericanoquito.edu.ec	Gastronomía	Cmatrinez1
Daniel Sandoval	escuela.marketing@sudamericanoquito.edu.ec	Escuela Marketing	Dsandoval1
Diego Gálvez	diego.galvez@sudamericanoquito.edu.ec	TICs	Dgalvez1
Evelin Zumba	secretaria.general@sudamericanoquito.edu.ec	Secretaria General	Evelinzumba1
Francisco Jiménez	administracion.turística@sudamericanoquito.edu.ec	Administración Turística	Fjimenez
Gabriela Jácome	financiero@sudamericanoquito.edu.ec	Financiero	Gjacome
IT	intesud.portalcautivo@gmail.com	Administrador	Iadministrador1
Miriam Huaraca	proteccion.medioambiente@sudamericanoquito.edu.ec	Protección Medioambiente	Mhuaraca1
Oscar Toscano	rector@sudamericanoquito.edu.ec	Rector	Otoscano1
Stefanny Muñoz	marketing@sudamericanoquito.edu.ec	Marketing	Smuñoz1
Yadira Ramírez	gerencia@sudamericanoquito.edu.ec	Gerencia	Yramirez1

Tabla 7. Tabla de usuarios en el servidor NAS Synology institucional.
Fuente: Las autoras.

La siguiente imagen es una captura de pantalla que evidencia la creación de los usuarios en el NAS:

Figura 125. Evidencia de la creación de usuarios en el servidor NAS.
Fuente: Las autoras.

La creación de grupos en un servidor NAS Synology es esencial para simplificar la administración de permisos y recursos compartidos en una red. Permite agrupar usuarios con necesidades de acceso similares, facilitando la asignación y modificación de permisos de manera eficiente. Esto mejora la seguridad al aplicar políticas de acceso coherentes y simplifica la auditoría. Además, la gestión de usuarios en grupos es escalable y centralizada, lo que es especialmente útil en entornos empresariales y de red en crecimiento. A continuación, se tiene la tabla de los grupos en el NAS Synology:

Nombre	Descripción
Administración_Empresas	Grupo Administración de Empresas INTESUD
Administración_Turística	Grupo Administración Turística INTESUD
Comunidad	Grupo Comunidad Institucional INTESUD
Financiero	Grupo Financiero INTESUD
Gastronomía	Grupo Gastronomía INTESUD
Gerencia	Grupo de Gerencia INTESUD
Marketing	Grupo Marketing INTESUD
Protección del Medio Ambiente	Grupo de Protección del Medio Ambiente INTESUD
Rectorado	Grupo Rectorado INTESUD
Recursos Humanos	Grupo de Recursos Humanos INTESUD
Secretaria General	Grupo secretaria general INTESUD
TICS	Grupo INTESUD
Vinculación	Grupo de Vinculación INTESUD

Tabla 8. Tabla de grupos del servidor NAS Synology institucional.
Fuente: Las autoras

La siguiente imagen es una captura de pantalla que evidencia la creación de los grupos en el NAS:

Figura 126. Creación de grupos en el servidor NAS.
Fuente: Las autoras.

6.4.3. Ubicación del servidor NAS y acceso a los servicios

Una vez instalado el servidor, este se lo ubicó en la parte inferior del rack de piso situado en el departamento de Tecnologías de la Información (TI), tercer piso, dentro del edificio principal de la institución. Desde esa posición, se establece el puente de conexión hacia el conmutador, el cual distribuye su conexión al área administrativa del edificio. La siguiente figura evidencia al servidor NAS en su lugar dentro del rack:

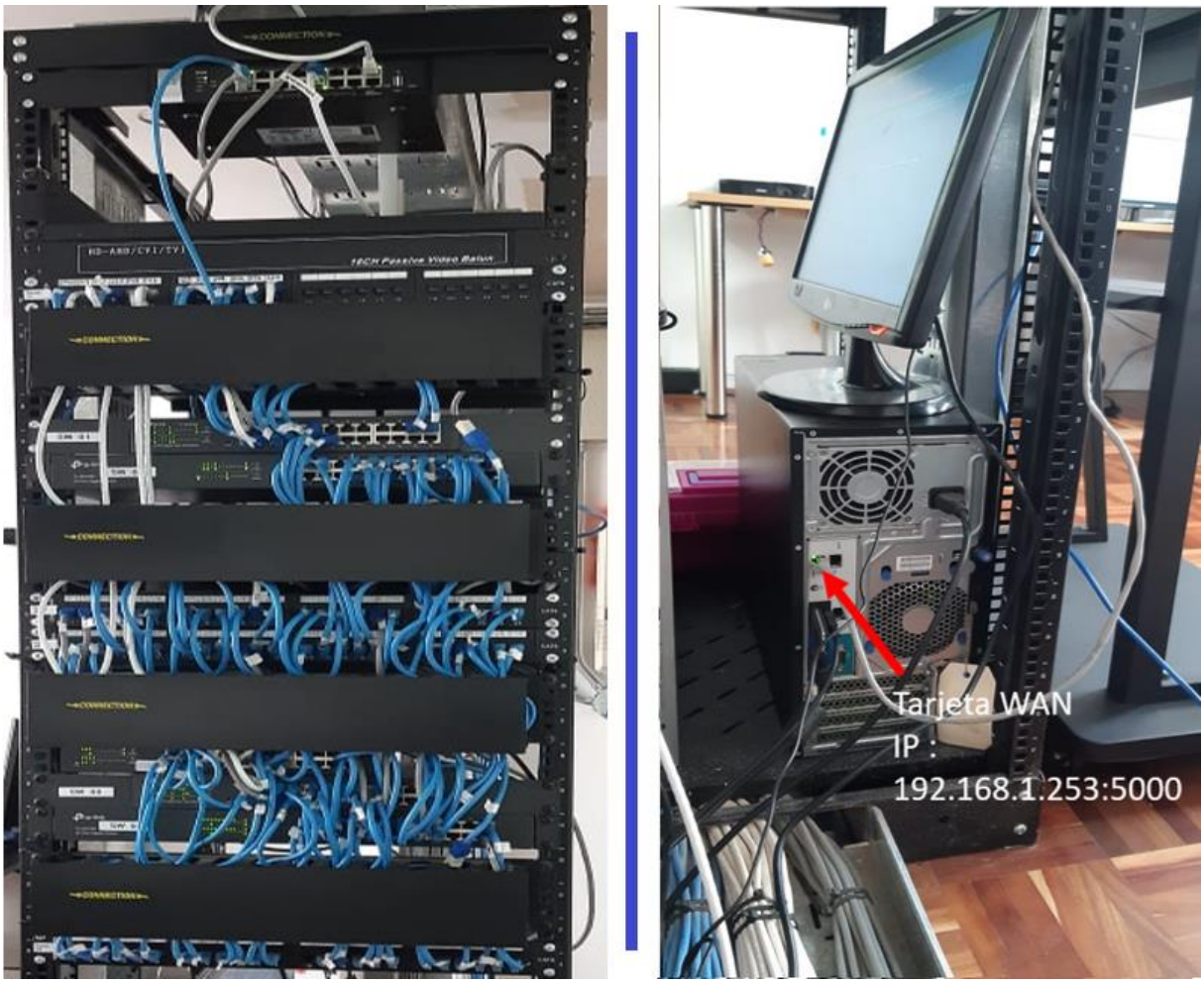


Figura 127. Ubicación del servidor NAS Synology DSM7.2 en el Rack de piso.
Fuente: Las autoras.

Como se explicó, para acceder al servidor NAS y a sus servicios, se ingresa en el navegador web en la computadora del usuario la dirección IPv4 192.168.1.253 y el puerto 5000, es decir

de digita **http://192.168.1.253:5000** en la barra de direcciones del navegador web del cliente, lo que permite cargar la interfaz de usuario del NAS.

Al no contar el edificio matriz con un servidor DNS interno al momento de desarrollar este proyecto, no se le asignó un nombre de dominio al servidor NAS, por lo tanto, para que los usuarios puedan ingresar de forma cómoda a sus cuentas en el servidor NAS, se proceda a ingresar la URL descrita y a grabar en Favoritos del navegador web de cada cliente la página de interfaz de usuario del NAS institucional, permitiendo de esta forma una fácil y rápida forma de ingresar al servicio sin necesidad de que el usuario final recuerde la IP y el puerto.

6.5 Funcionamiento y pruebas

Para cumplir con el objetivo de realizar pruebas de funcionamiento para verificar la efectividad del portal cautivo, durante una semana de pruebas, se evaluó el funcionamiento del proyecto, empezando por una constante vigilancia de la operabilidad de las VLAN por la reestructuración de la red informática del edificio matriz realizada.

A la vez, se realizaron las pruebas de funcionamiento del Portal Cautivo, en los cuatro puntos de acceso inalámbrico para estudiantes ubicados en cada piso destinados a aulas del edificio matriz y también considerando diversos escenarios, incluyendo pruebas con y sin váuchers.

De la misma forma, se llevaron a cabo pruebas del correcto envío de los correos masivos con MailChimp, centrándose en la campaña de socialización de los váuchers con las instrucciones de uso y conexión al Wifi del edificio matriz. Para estas pruebas se utilizaron diferentes correos electrónicos para validar su correcto funcionamiento.

Luego, se verificó el servidor NAS, asegurando su accesibilidad y correcta entrega de servicios dentro del entorno establecido que es la VLAN 1 o VLAN Administrativa.

Por último, se entregaron todas las credenciales administrativas al Departamento IT de la Institución. Todas las evaluaciones realizadas permitieron corroborar la operatividad del proyecto.

Se monitoreó constantemente el servicio de Internet en los equipos informáticos de ambas VLAN y no se reportó ningún problema de conectividad, ni en área Administrativa, ni en el área de Laboratorios de informática. Esto demuestra la correcta restructuración de la red informática en el edificio matriz. La siguiente imagen evidencia la reorganización y repeinado de los patch cords del rack principal del edificio matriz:

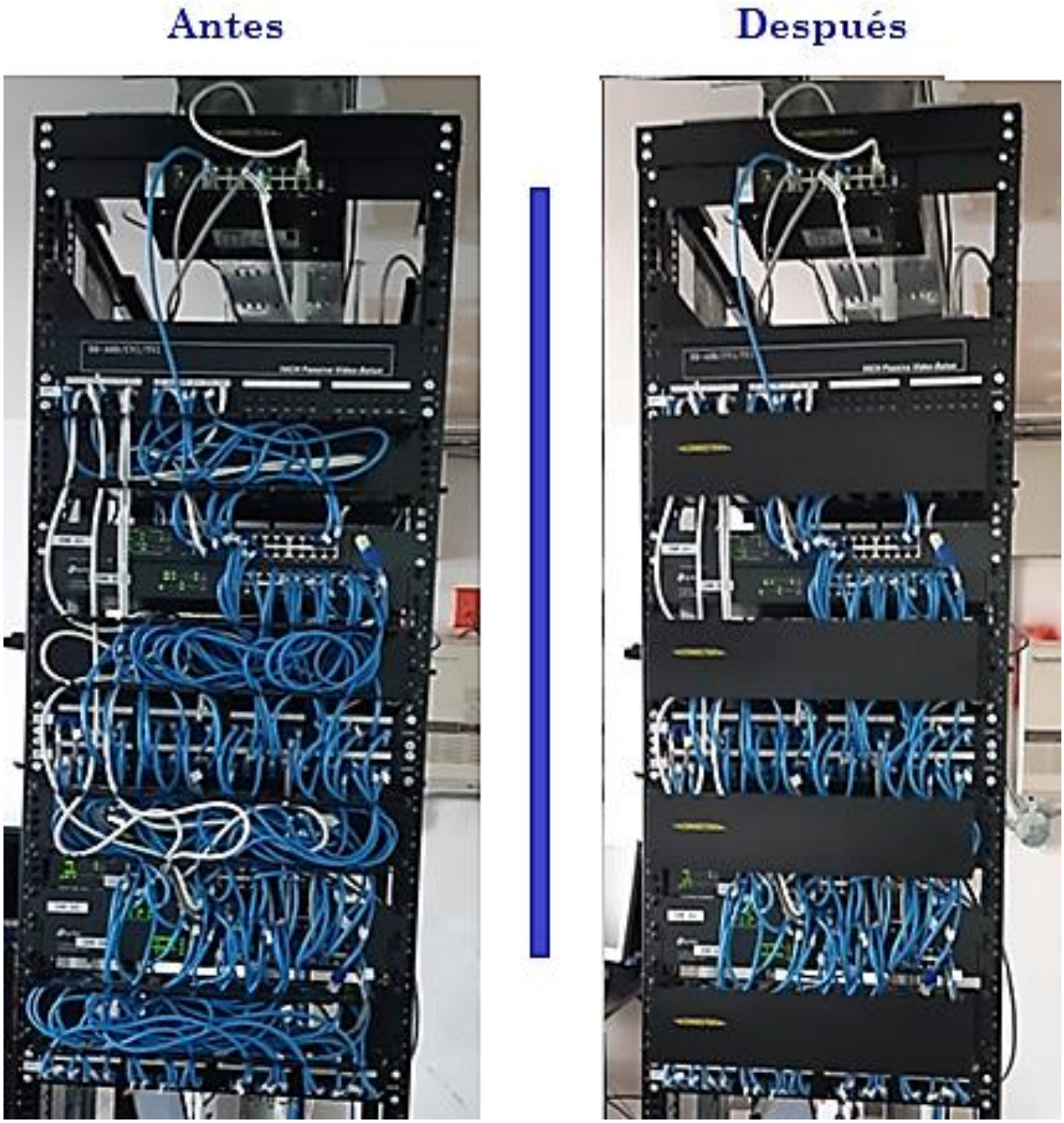


Figura 128. Reorganización del rack.
Fuente: Las autoras.

La creación de dos VLAN en el edificio matriz del INTESUD ha sido una estrategia clave para mejorar el servicio de Internet y optimizar el ancho de banda disponible para los usuarios. Originalmente, la existencia de una única VLAN para todas las áreas y la asignación de una LAN clase C con DHCP para aproximadamente 200 usuarios simultáneos en las áreas Administrativa y de Laboratorios, incluyendo los dispositivos móviles de los estudiantes,

conducía a una serie de problemas graves de conectividad, congestión de tráfico de la red y la disminución considerables en la calidad del servicio.

Las pruebas demuestran que la implementación de dos VLAN separadas trajo consigo mejoras significativas como:

Segmentación del Tráfico: Al dividir la red en dos VLAN distintas, una para la Administración (VLAN 1) y otra para los Laboratorios (VLAN 8), se logró una segregación efectiva del tráfico. Esto significa que las actividades administrativas críticas, que pueden incluir transacciones financieras, comunicaciones internas y gestión de recursos humanos, no compiten con el tráfico de datos generado por los laboratorios y los dispositivos de los estudiantes. Cada VLAN tiene su propio dominio de broadcast, reduciendo así la cantidad de tráfico innecesario que atraviesa la red y mejorando el rendimiento general.

Optimización del Ancho de Banda: Con dos VLAN, se facilita la asignación de ancho de banda y se puede aplicar Calidad de Servicio (QoS). Esto quiere decir que se puede dar prioridad al ancho de banda para el área Administrativa, asegurando que las operaciones esenciales no se vean afectadas por el consumo de ancho de banda en los laboratorios o por el uso intensivo de la red por parte de los estudiantes. En la VLAN de los laboratorios, se puede configurar el ancho de banda de acuerdo con las necesidades y cumplir con al ancho de banda mínimo que los usuarios deben tener establecido por instituciones de control como el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES). Así, al momento de realizar las pruebas de este trabajo, se tiene en el edificio matriz un ancho de banda total de 300 Mbps y este se distribuye de manera simétrica entre las dos VLAN, es decir, cada VLAN recibe 150 Mbps.

Según los listados de alumnos matriculados para el periodo académico 2023-2024 facilitados por Secretaría General a la Coordinación de la Escuela de Desarrollo de Software se tiene aproximadamente 160 alumnos matriculados en la sección diurna y que reciben clases de manera presencial al edificio matriz. A esto sumado los 10 PC del Laboratorio 3-A, 9 PC del 3-B, 7 del 3-C, 16 del laboratorio 3-D son 42 equipos que requieren direcciones IP.

Por lo tanto, en el peor de los casos, si se tienen 200 usuarios conectados simultáneamente en cada VLAN, el ancho de banda disponible para cada usuario se calcularía dividiendo el ancho de banda total asignado a esa VLAN entre el número de usuarios conectados. Por lo tanto, para cada VLAN, el cálculo sería:

$$\frac{150Mbps}{200} = 0{,}75Mbps = 750kbps$$

Esto significa que, en el peor escenario, con una distribución equitativa de la QoS, cada usuario podría disponer de un promedio de 0,75 Mbps. Esto cumple con el indicador cuantitativo del CACES, que según el documento “Modelo de evaluación externa 2024 con fines de acreditación para los institutos superiores técnicos y tecnológicos. Mayo, 2021”, establece que el ancho de banda promedio por usuario potencial es de, al menos, 500 kilobits por segundo.

Es importante mencionar que esta es una estimación teórica y que el ancho de banda real experimentado por cada usuario puede variar debido a múltiples factores, como el tipo de tráfico de red, las políticas de QoS establecidas y la capacidad de los dispositivos Access Point como de los propios usuarios.

Seguridad Mejorada: La separación lógica entre las redes administrativas y académicas también refuerza la seguridad ya que los datos generados en cada VLAN no se pueden ver ni compartir en la otra.

Gestión y Resolución de Problemas: Con dos VLAN, la identificación y resolución de problemas de red se simplifica. Los problemas pueden ser aislados y diagnosticados dentro de una VLAN específica sin afectar a la otra, facilitando así una gestión más efectiva y una menor interrupción del servicio.

En resumen, la introducción de dos VLAN en el INTESUD ha sido una mejora significativa en la gestión de la infraestructura de red, proporcionando una distribución más eficiente del ancho de banda, una mejora en la calidad del servicio de Internet, una mayor seguridad y una gestión de la red más simplificada.

Las pruebas de funcionamiento del portal cautivo con pfSense en la VLAN 8 del Instituto se llevaron a cabo con éxito. Los usuarios de prueba pudieron autenticarse sin problemas, evidenciando un control de acceso efectivo y una gestión de ancho de banda eficiente. El sistema demostró estabilidad y mantuvo un rendimiento óptimo a lo largo de las sesiones de usuario. Además, se logró un cumplimiento adecuado de las políticas de seguridad, con una interfaz de usuario clara e intuitiva que facilitó la experiencia de conexión. Los informes generados por pfSense proporcionaron análisis detallados del tráfico, confirmando la escalabilidad del sistema y su capacidad para soportar la demanda actual y futura.

La siguiente imagen evidencia la instalación y correcto funcionamiento del servidor pfSense al mostrar la terminal o shell administrativa:

Figura 129. Shell o terminal del servidor pfSense.
Fuente: Las autoras.

La siguiente figura evidencia al servidor pfSense ubicado en el rack, que ofrece el servicio de Portal Cautivo a los estudiantes mediante los puntos de acceso inalámbricos ubicados en los pisos del 1 al 4:

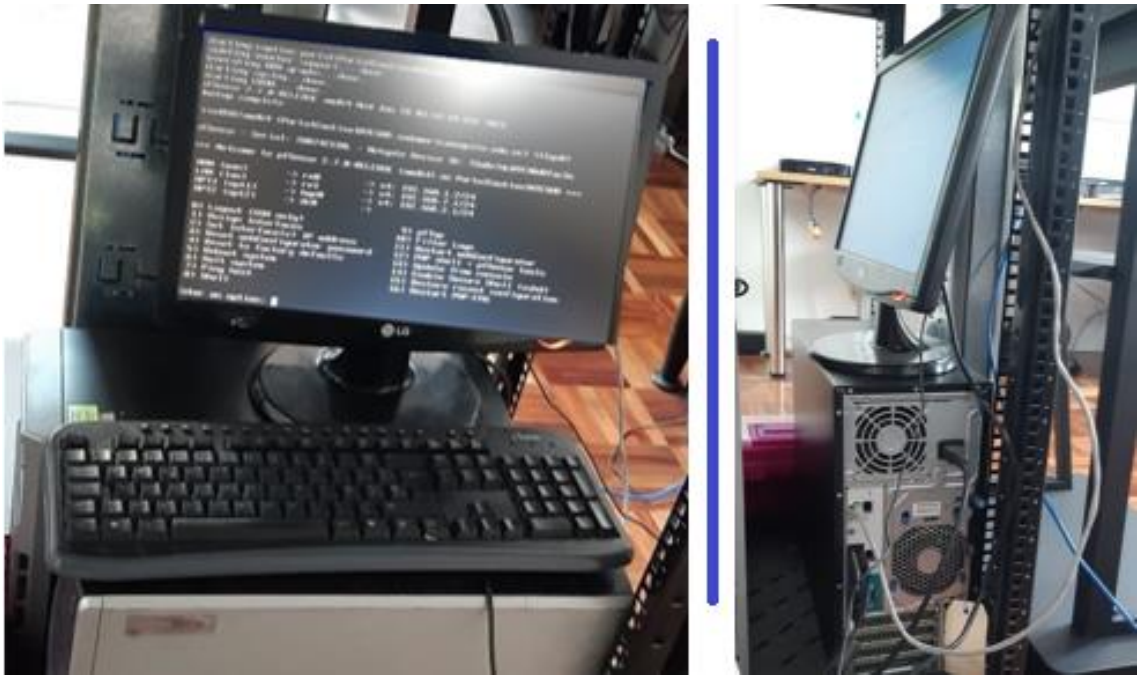


Figura 130. Ubicación del servidor pfSense Portal Cautivo en el Rack de piso.
Fuente: Las autoras.

La siguiente imagen muestra al “Gráfico Interactivo” en donde se puede observar la información relacionada con el tráfico de red, la utilización de recursos, el estado del sistema y otros aspectos del funcionamiento del firewall y el enrutador pfSense. Como se muestra la curva de funcionamiento es mínima indicando que no hay sobrecarga en la configuración establecida:

Figura 131. Estadísticas del Gráfico Interactivo de pfSense.
Fuente: Las autoras.

La siguiente figura muestra el análisis del tráfico de datos en la tarjeta WAN del servidor pfSense, en donde se aprecia que no se presenta saturación de tráfico de paquetes:

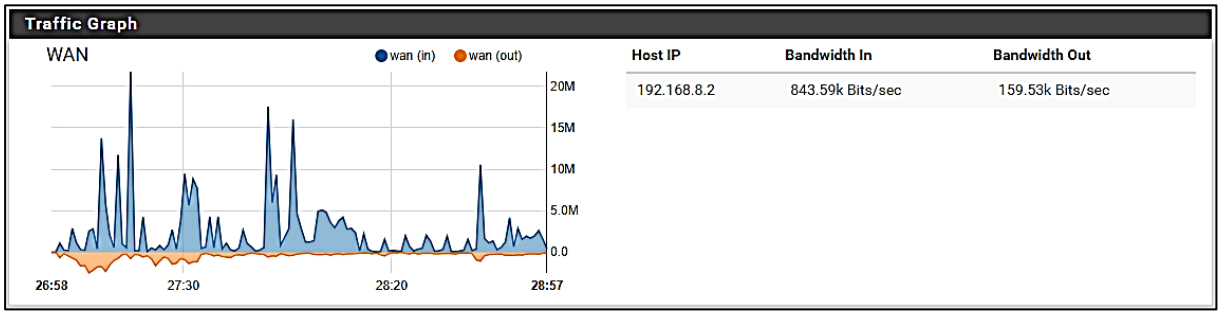


Figura 132. Estadísticas del tráfico de datos WAN en el servidor pfSense.
Fuente: Las autoras.

La siguiente figura muestra el análisis del tráfico de datos en la tarjeta LAN del servidor pfSense, en donde se aprecia que no se presenta saturación de tráfico de paquetes:

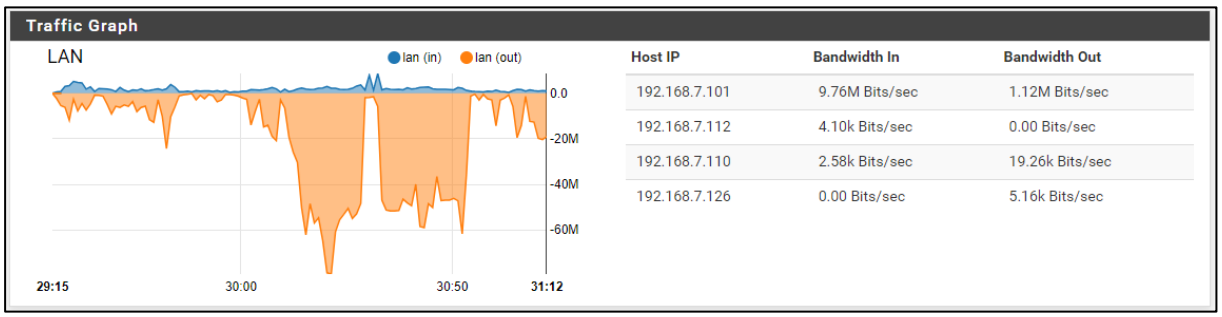


Figura 133. Estadísticas del tráfico de datos de LAN.
Fuente: Las autoras.

La siguiente imagen indica las pruebas de arrendamiento de las direcciones IPv4 de manera dinámica otorgadas por el servicio DHCP en base a las conexiones de los estudiantes. Se determinó que un alquiler de IP por parte del DHCP de 7200 segundos (120 minutos – 2 horas) es suficiente para mantener fluido el servicio, es decir el usuario será desconectado de manera automática a los 120 minutos si no se detecta actividad en los últimos minutos del arrendamiento, para retornar y tener el servicio de Internet nuevamente, el usuario deberá reconectarse y se le renovará la conexión con el arrendamiento de una nueva IP, así mismo por 120 minutos.

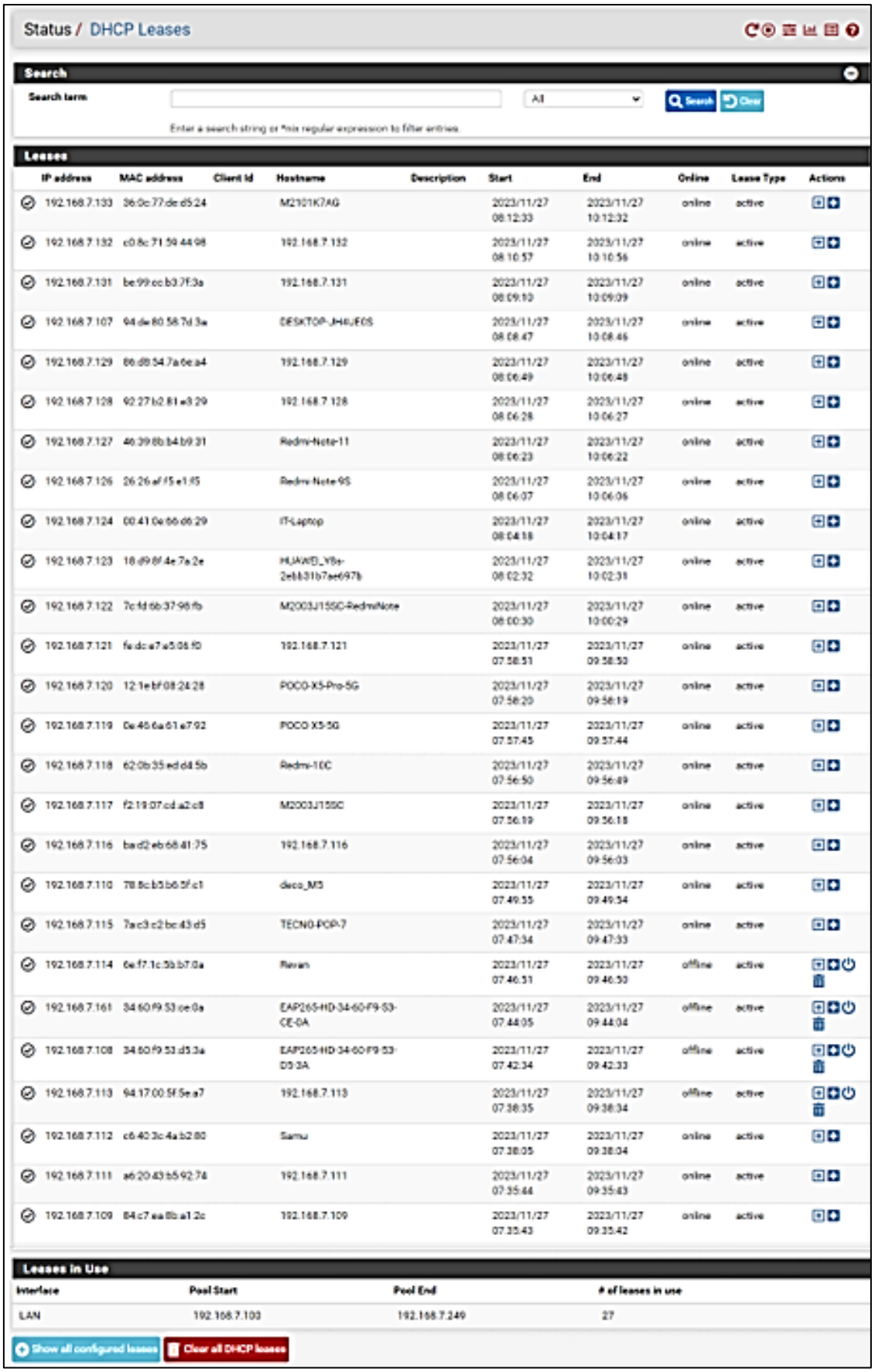


Figura 134. Pruebas de arrendamiento de direcciones IPv4 por el DHCP del Portal Cautivo. Fuente: Las autoras.

La siguiente imagen evidencia la generación y configuración de los váuchers:

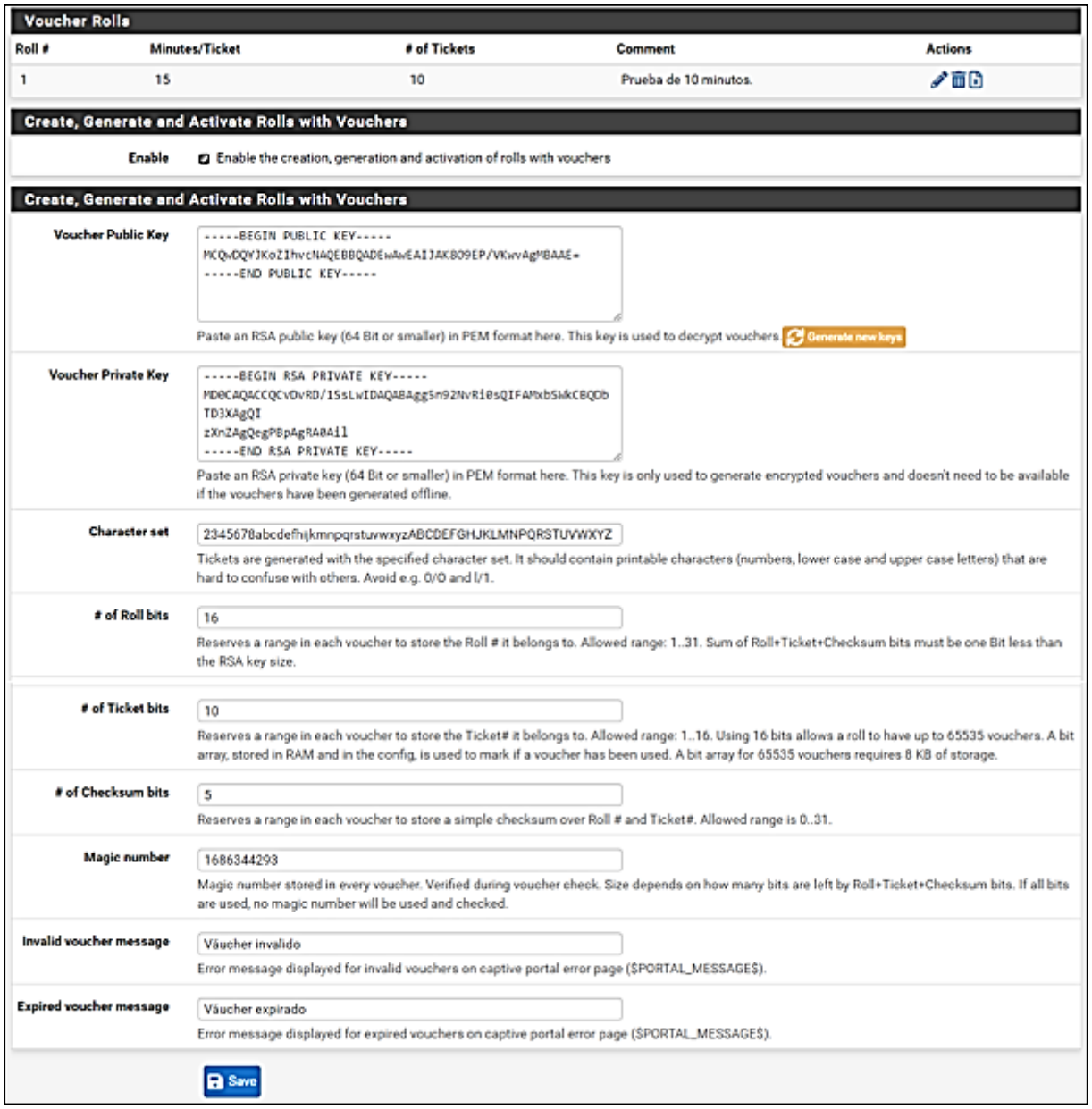


Figura 135. Pruebas de configuración y generación de váuchers Portal Cautivo.
Fuente: Las autoras.

Luego de generar el rol (grupo de vaúchers) para los estudiantes, se procede a descargar el archivo CSV que contiene el listado de los códigos que se generaron en función del número de estudiantes y del total de minutos que se usarán en el semestre. Las autoras consideran que 64.800 minutos por vaúcher para cada estudiante es suficinte para cubrir el periodo académico y no se hace indefinido para tener un control de los estudiantes que continuan sus estudios y

están al día con sus obligaciones económicas. Este análisis se fundamentó bajo el siguiente análisis:

Primero, se determinó los días laborables y días de descanso:

Un semestre o periodo académico = 6 meses

Días laborables en un mes = 30 días (aproximadamente considerando un mes promedio)

Días de descanso (sábados y domingos) en un mes = 2 * 4 = 8 días (suponiendo que hay 4 semanas en un mes)

Cálculo del total de días laborables en 6 meses:

Días laborables en 6 meses = Días laborables en un mes * Meses en 6 meses

Días laborables en 6 meses = 30 días/mes * 6 meses = 180 días laborables en 6 meses

Segundo, se calculó el total de minutos que un estudiante usaría internet en días laborables:

Horas de uso diario = 6 horas (considerando horario de la Escuela de Gastronomía y que los estudiantes pudieran quedarse a tutorías académicas).

Minutos en 6 horas = 6 horas * 60 minutos/hora = 360 minutos al día

Cálculo de los minutos diarios por el total de días laborables en 6 meses:

Total, de minutos en 6 meses = Minutos diarios * Días laborables en 6 meses

Total, de minutos en 6 meses = 360 minutos/día * 180 días = 64.800 minutos en 6 meses

Por lo tanto, en 6 meses, un estudiante que usa internet durante 6 horas al día únicamente en días laborables (de lunes a viernes) acumularía un total de 64.800 minutos de uso de internet.

Un cálculo parecido se realizó para el rol destinado para los Docentes que imparten clases de manera presencial en el edificio matriz de la Institución. Para ellos se realizó en siguiente análisis:

Horas de uso diario del profesor = 8 horas

Minutos en 8 horas = 8 horas * 60 minutos/hora = 480 minutos al día

Ahora, se calculó el total de minutos que un profesor usaría internet en un año (365 días):

Total, de minutos en un año = Minutos diarios * Días en un año

Total, de minutos en un año = 480 minutos/día * 365 días = 175,200 minutos en un año

Por lo tanto, un profesor que use internet durante 8 horas al día, sin contar sábados y domingos, acumularía un total de 175.200 minutos de uso de internet en un año.

La siguiente imagen muestra parte de un archivo CSV descargado del rol para estudiantes:

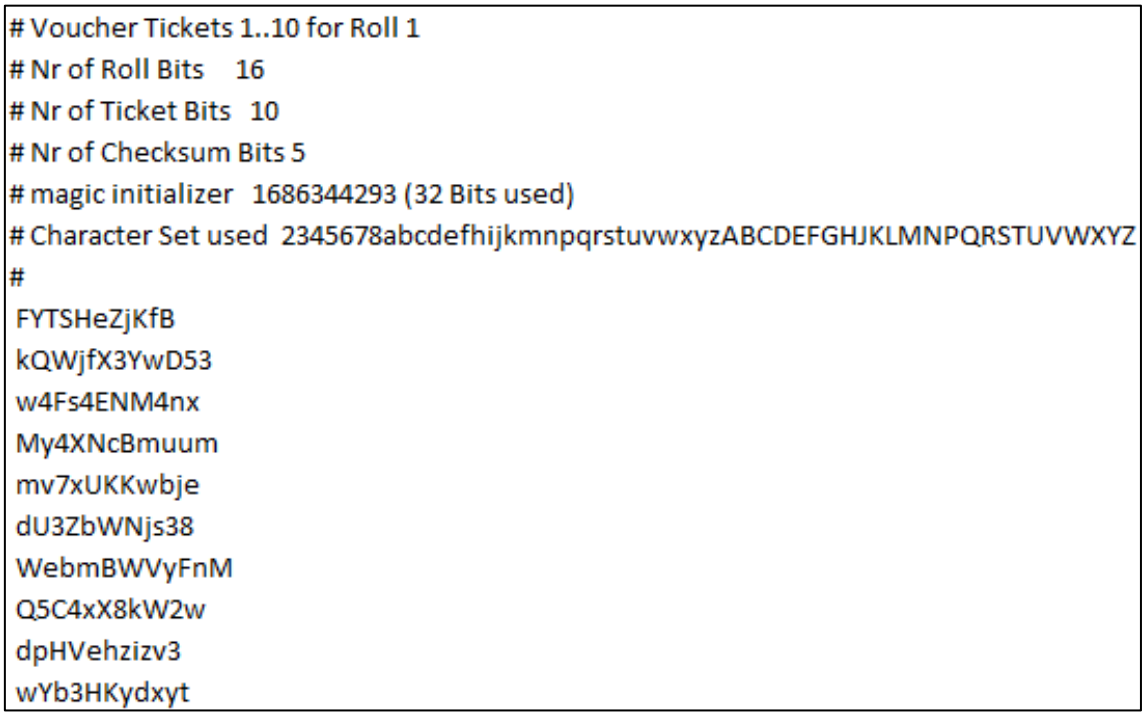
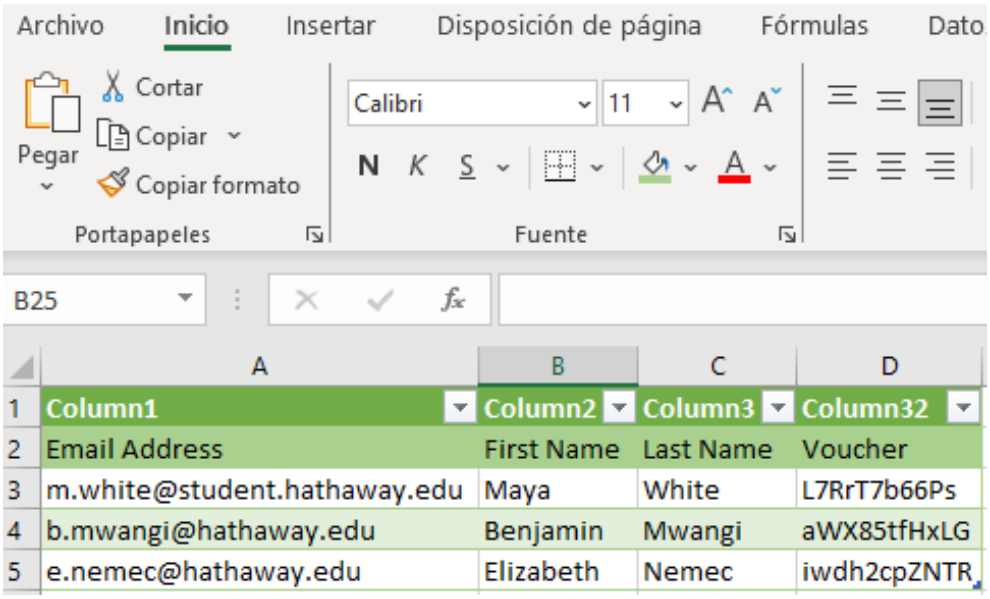


Figura 136. Prueba del rol de estudiantes (váuchers) para el ingreso por el Portal Cautivo. Fuente: Las autoras.

Para el envío de los váucher a cada estudiante mediante MailChimp se utiliza el archivo CSV generado en el pfSense, para luego asignar cada código a un estudiante usando para ello

el listado de estudiantes, que están debidamente matriculados, y que es facilitado por Secretaría. Es decir, se debe realizar un archivo en Excel con los nombres y apellidos de los estudiantes, con sus respectivos correos electrónicos y el vaúcher que se le asigne. La siguiente imagen muestra parte de una archivo Excel que se sube a MailChimp para el uso de la campaña de socialización de vaúchers:



	A	B	C	D
1	Column1	Column2	Column3	Column32
2	Email Address	First Name	Last Name	Voucher
3	m.white@student.hathaway.edu	Maya	White	L7RrT7b66Ps
4	b.mwangi@hathaway.edu	Benjamin	Mwangi	aWX85tfHxLG
5	e.nemec@hathaway.edu	Elizabeth	Nemec	iwdh2cpZNTR

Figura 137. Archivo Excel formateado para MailChimp para la campaña de socialización de váuchers. Fuente: Las autoras.

De necesitarse impedir el ingreso a un usario, este mismo archivo permitirá ubicar el número de vaúcher y borrarle el permiso de ingreso, la siguiente imagen indica la pantalla para realizarlo. De ser necesario regresarle el permiso, se genera o se le otorga un nuevo número de vaúcher.

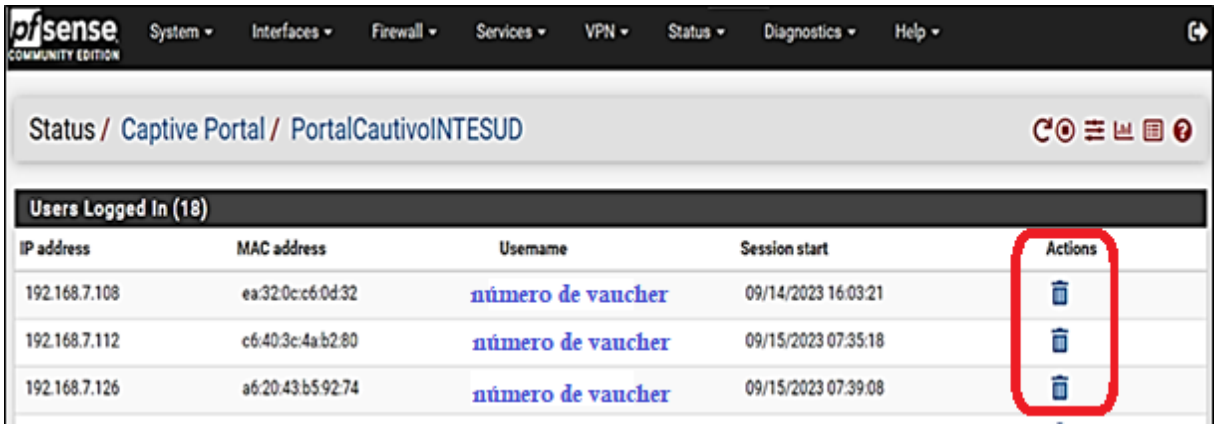
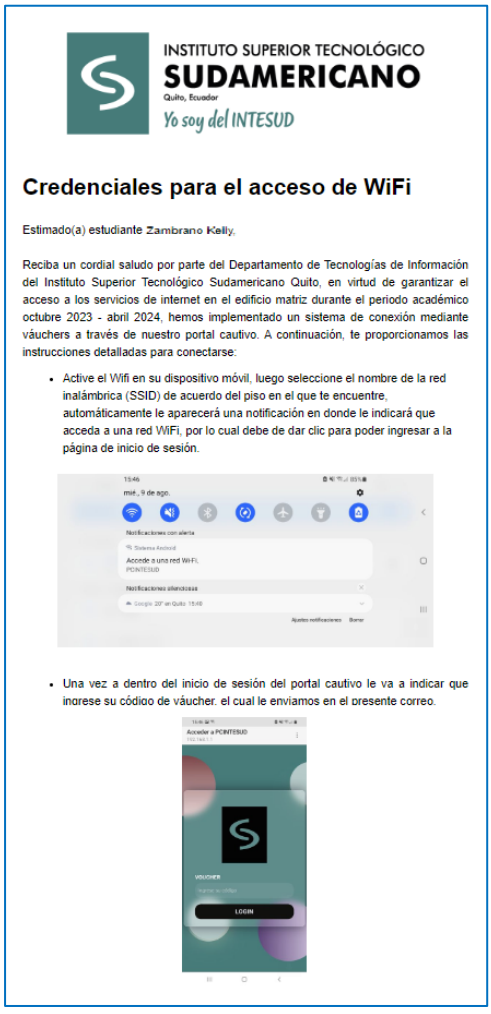


Figura 138. Pantalla de pfSense para dar de baja a usuarios del Portal Cautivo.
Fuente: Las autoras.

La siguiente imagen es un correo electrónico que recibe un estudiante y es evidencia del envío de la campaña de socialización de los váuchers funciona:



a) Parte 1 del e-mail.

b) Parte 2 del e-mail.

Figura 139. Pruebas del envío de correo masivo con MailChimp.
Fuente: Las autoras.

La siguiente imagen indica la prueba de funcionamiento del ingreso a la red Wifi del Instituto, pasando por la página web del Portal Cautivo en un dispositivo móvil sin la utilización de vaúchers. El usuario solo debe presionar el botón de “Login”.

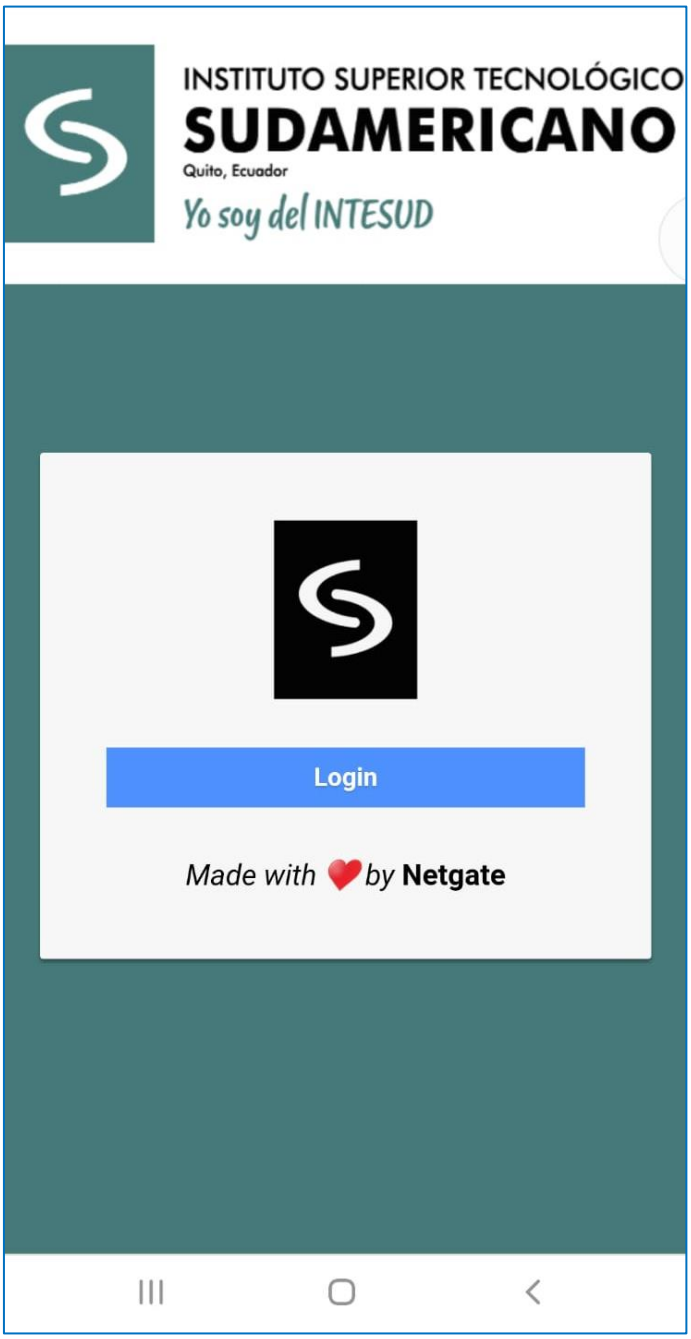


Figura 140. Ingreso por el Portal Cautivo a la red Wifi sin utilización de váuchers.
Fuente: Las autoras.

La siguiente imagen muestra la prueba de funcionamiento del ingreso a la red Wifi del Instituto, pasando por la página web del Portal Cautivo en un dispositivo móvil pero esta vez con la utilización de vaúchers. El usuario debe ingresar su código y luego presionar el botón de “Login”.

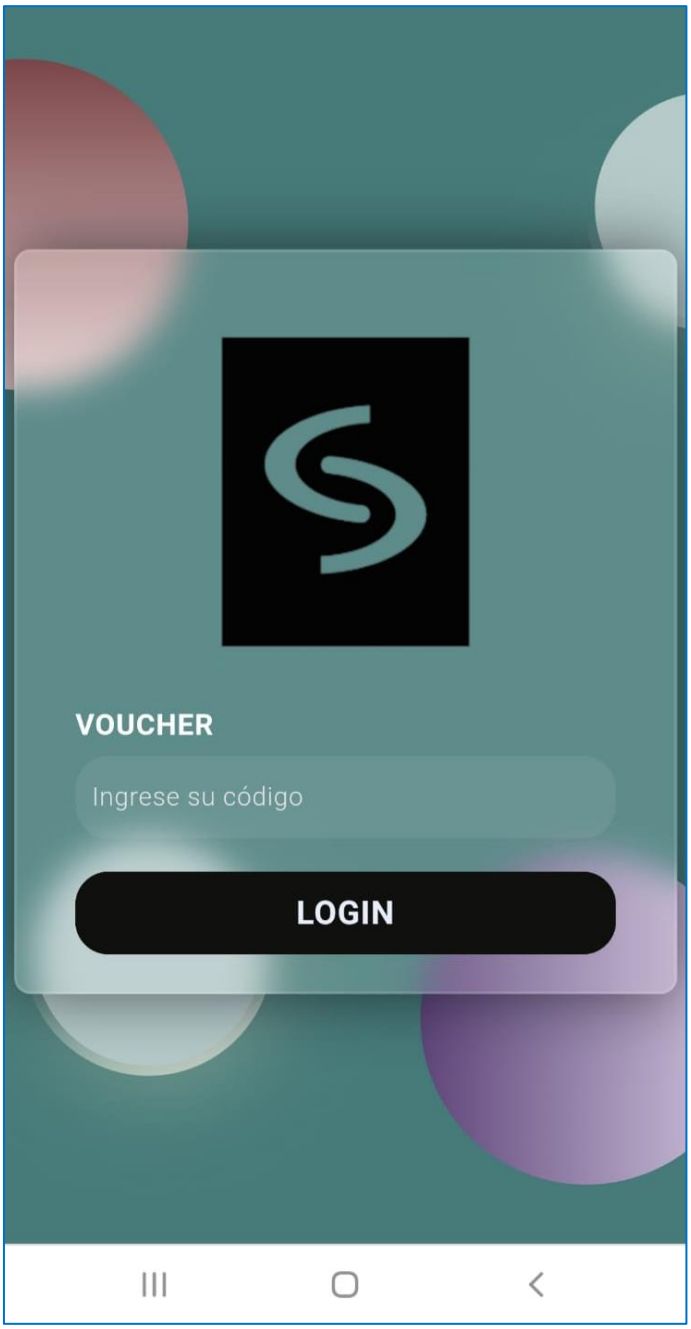


Figura 141. Ingreso por el Portal Cautivo a la red Wifi con utilización de váuchers.
Fuente: Las autoras.

Las dos imágenes anteriores demuestran el funcionamiento del Portal Cautivo en dos escenarios, sin la utilización de váuchers y con el uso de ellos. El proyecto se entrega con el Portal Cautivo sin la utilización de los váuchers ya que se necesita la autorización por parte de las autoridades para su implementación con váuchers.

También, las imágenes muestran la capacidad de personalización de la página web del Portal Cautivo, cuestión que se puede aprovechar para personalizarla con algún mensaje que se requiera hacer llegar a los estudiantes.

Para poder habilitar o no, el uso de los váuchers, como la sección para personalizar la página web del Portal Cautivo se detallan en la figura 72 de este documento.

Las pruebas realizadas en el servidor NAS Synology dentro de la VLAN 1 del Instituto Superior Tecnológico Sudamericano Quito resultaron exitosas. El personal administrativo que se ofreció para hacer las pruebas, accedió al sistema sin dificultades, y la seguridad de los datos quedó demostrada como robusta y confiable. Se observó un rendimiento excelente en el almacenamiento y recuperación de datos, con el NAS mostrando una respuesta rápida y sin retrasos. La estabilidad fue constante, y la integración en la VLAN 1 no presentó conflictos. La configuración de usuarios y permisos se alineó con las políticas institucionales. Finalmente, las actualizaciones y el mantenimiento preventivo del NAS se manejaron con fluidez, asegurando así una gestión eficaz del almacenamiento de datos para la administración del Instituto. La siguiente imagen indica la ubicación del servidor NAS en el rack de piso de la oficina de Coordinación de la Escuela de Desarrollo de Software y Departamento de las tecnologías de la Información:

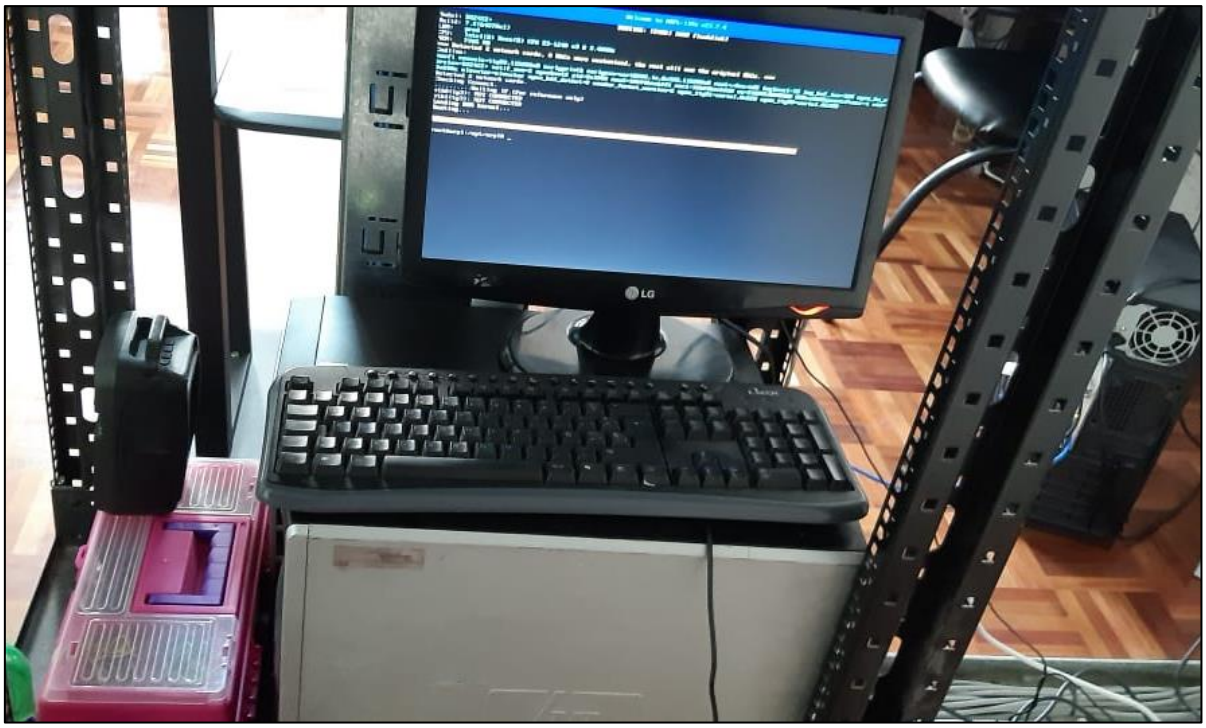


Figura 142. Ubicación del servidor NAS en el Rack de piso.
Fuente: Las autoras.

En la siguiente imagen se evidencia el ingreso al servidor NAS por la aplicación que se instala en el dispositvo móvil que se llama Drive, lo que permite cargar la interfaz administrativa de usuario del servidor NAS. En las figuras 110 a la 122 de este trabajo se indicó el ambiente de trabajo con el servidor NAS bajo el navegador web de un computador de escritorio.

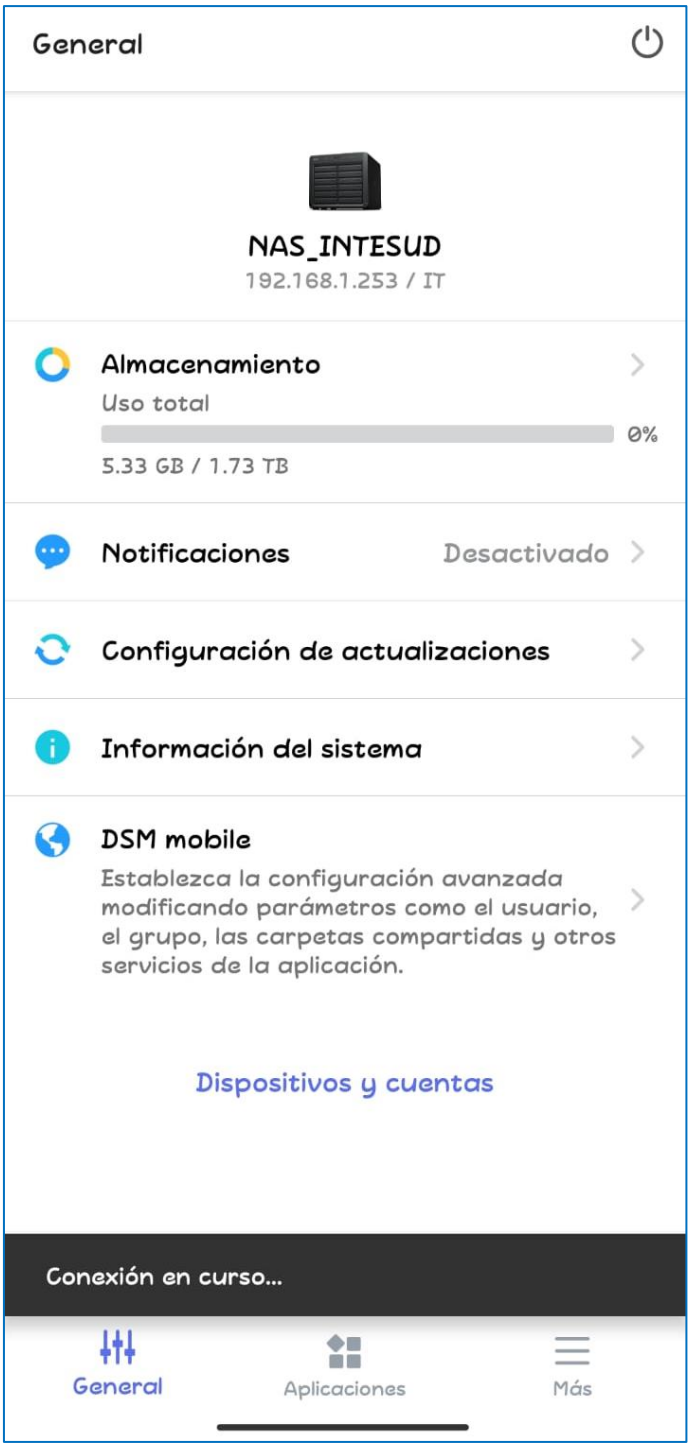


Figura 143. Pruebas de funcionamiento del servidor NAS Synology, pantalla principal administrativa por la app DS Find desde un dispositivo móvil.
Fuente: Las autoras.

La siguiente imagen muestra las aplicaciones necesarias para poder gestionar los archivos y servicios del servidor NAS Synology desde el móvil del usuario. "DS finder" es una aplicación móvil desarrollada por Synology que permite a los usuarios localizar y acceder a su

NAS Synology desde los dispositivos móviles, este ofrece funcionalidades como la supervisión del estado del sistema, gestión de servicios y alertas de eventos del NAS.

Además de "DS finder", Synology ofrece varias otras aplicaciones para maximizar el uso del NAS:

- DS audio: Para organizar y transmitir música.
- DS photo: Para acceder y compartir fotos.
- DS video: Para gestionar y reproducir videos.
- DS file: Un administrador de archivos para el NAS.
- DS get: Para controlar descargas de BitTorrent.
- DS note: Para sincronizar y acceder a notas.
- DS cam: Para supervisar cámaras de vigilancia.
- DS cloud: Para sincronizar archivos entre el NAS y dispositivos móviles.

Estas aplicaciones permiten aprovechar diversas funcionalidades del NAS Synology, desde gestión de medios hasta sincronización de archivos y seguridad, mejorando la experiencia de usuario y expandiendo las capacidades del dispositivo NAS. La siguiente imagen evidencia la instalación de estas apps:

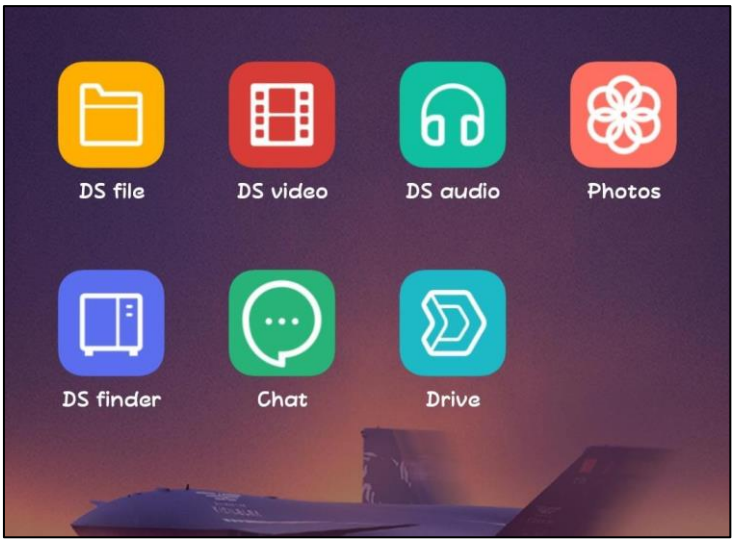


Figura 144. Aplicaciones para dispositivos móviles para la gestión de servicios del servidor NAS.
Fuente: Las autoras.

Las pruebas realizadas en las aplicaciones móviles de Synology para el servidor NAS en el Instituto Superior Tecnológico Sudamericano Quito culminaron con éxito. "DS finder" facilitó eficazmente la localización y gestión del NAS, mientras que aplicaciones como "DS audio", "DS photo", y "DS video" demostraron ser herramientas excepcionales para organizar y acceder a contenidos multimedia. "DS file" se destacó en la gestión de archivos, "DS get" en el control de descargas y "DS note" en la sincronización de notas. La aplicación "DS cam" funcionó a la perfección para la supervisión de cámaras de vigilancia, y "DS cloud" se mostró eficiente en la sincronización de archivos. Todas las aplicaciones probaron ser valiosas para mejorar la accesibilidad y la funcionalidad del servidor NAS, contribuyendo significativamente a la eficiencia y productividad de la administración y actividades académicas del instituto.

Por último, se entregó formalmente, por parte de las autoras, todas las credenciales relacionadas con la implementación del proyecto al Departamento de Tecnologías de la Información (IT), mediante oficio, para que tomen posesión el proyecto.

7. Conclusiones y Recomendaciones

7.1. Conclusiones

- Se realizó la revisión bibliográfica de las tecnologías y marcos teóricos relacionados con portales cautivos para fundamentar el diseño e implementación del sistema.
- Se evaluó y optimizó la infraestructura inicial de la red de computadoras del edificio matriz, lo que permitió asegurar su compatibilidad con la implementación del portal cautivo y la configuración existente de los puntos de acceso Wifi (hotspots).
- Se diseñó y se configuró una red de área local virtual (VLAN 8), específicamente en el router institucional existente Cisco RV325, lo que permitió segmentar el tráfico de la red y mejorar la seguridad y eficiencia de la red interna. No se lo pudo realizar en los equipos switch, ya que estos no son configurables, y por lo tanto, no tienen capacidad de crear VLAN.
- Se seleccionó, instaló y configuró pfSense como el software más apropiado para gestionar el portal cautivo del edificio matriz de la institución, el cual cumple con los criterios de seguridad, estabilidad y compatibilidad.
- Se desarrolló un sistema de distribución de váuchers que asegura un acceso restringido y monitoreado a la red Wifi, y que está reservado para los miembros autorizados, sobre todo los estudiantes habilitados, de la comunidad institucional.
- Se implementó un Sistema de Almacenamiento en Red (NAS) que soporta la centralización y el acceso seguro a los archivos y recursos compartidos de la institución exclusivamente por la red LAN (VLAN 1 Administrativa).
- Se realizó las pruebas de funcionamiento para verificar la efectividad del portal cautivo y del sistema NAS en escenario de uso real, y se puede reajustar la configuración según sea necesario para cumplir con los funcionamientos esperados.

- Se diseñó e implementó un portal cautivo en el edificio matriz del Instituto Superior Tecnológico Sudamericano Quito para mejorar la gestión y seguridad del acceso a la red Wifi.

7.2. Recomendaciones

- El desarrollar el proyecto permitió a las autoras conocer la realidad de un Departamento IT y todas sus obligaciones. Consideramos que dos personas encargadas de la administración y gestión de este departamento es insuficiente, por lo tanto, recomendamos contratar y designar a una nueva persona que se encargue y se responsabilice de utilizar y supervisar el correcto funcionamiento del portal cautivo, los correos masivos, y la salud del NAS. Esto permitirá que el departamento continúe ofreciendo sus servicios con responsabilidad y no exista sobrecarga en sus funciones, que de ocurrir, puede conllevar a un declive en los servicios que ofrece a la comunidad institucional.
- Se recomienda recordar tanto a los docentes como a los estudiantes que disponen de un tiempo límite (172.200 minutos y 64.800 minutos respectivamente), el cual estará vigente durante todo el semestre y será renovado al inicio de cada nuevo periodo académico.
- Se recomienda recordar tanto a los profesores y estudiantes que el váucher solo será válido para un solo dispositivo, ya sea laptop o celular. En caso de desear conectar otro dispositivo, será necesario apagar el wifi del dispositivo en uso y conectarse con el váucher en el otro dispositivo.
- En el caso de realizar modificaciones en la configuración del Portal Cautivo, se recomienda primero guardar un respaldo de la configuración actual, para posterior, proceder con la modificación, de esta manera se resuelve cualquier situación inesperada.

- Se recomienda capacitar al personal administrativo sobre el sistema de almacenamiento NAS, con temas como su acceso, sus funcionalidades y sus ventajas.
- Se recomienda que el Departamento de las Tecnologías de la Información instale un servicio interno de DNS para que el acceso al servidor NAS no sea por IPv4 y su puerto, sino se le asigne un nombre de dominio para facilitar de acceso por parte de los usuarios.
- Para garantizar el éxito continuado del proyecto de portal cautivo en el Instituto Superior Tecnológico Sudamericano Quito, se recomienda mantener el software constantemente actualizado y realizar un monitoreo continuo para garantizar seguridad y rendimiento óptimos. Es esencial tener una persona con conocimiento para el uso adecuado del sistema y mantener un plan de respuesta ante incidentes. Regularmente, se deben realizar copias de seguridad y auditorías de seguridad, así como evaluar el rendimiento y la escalabilidad del sistema para adaptarse a las necesidades en evolución del instituto. Además, es importante recoger retroalimentación de los usuarios y asegurarse de cumplir con las normativas vigentes en materia de uso de Internet y protección de datos, buscando siempre la mejora continua del portal cautivo.

8. Referencias

KeepCoding. (17 de octubre de 2022). *Diferencia entre Google Sheets y Excel*. Obtenido de KeepCoding Tech School: https://keepcoding.io/blog/diferencia-entre-google-sheets-y-excel/

Adrián, D. R. (2013). *Estructura básica de una página Web - html, head y body*. Recuperado el 23 de semptiembre de 2023, de Akus.net Diseño Web: https://disenowebakus.net/domine-html-y-dhtml-primeros-pasos.php

amazon.com. (11 de julio de 2023). *Que es una red de computadoras*. Obtenido de aws: https://aws.amazon.com/es/what-is/computer-networking/

Antonio, J. (s.f.). *Qué es un Switch o conmutador LAN y para qué sirve*. Recuperado el 04 de octubre de 2023, de Profesional Review: https://www.profesionalreview.com/2020/02/21/switch-conmutador/

asirclaret-com.webnode.es. (12 de julio de 2023). *Tipos de vlan*. Obtenido de asirclaret-com.webnode.es: https://asirclaret-com.webnode.es/planificacion-y-administracion-de-redes/tema-7-configuracion-y-administracion-de-conmutadores/tipos-de-vlan/

asus. (s.f.). *asus*. Recuperado el 29 de octubre de 2023, de asus: https://techinstyle.asus.com/wp-content/uploads/2017/03/bios-6c.jpg

Atecnis. (s.f.). *¿Qué es Sendinblue?* Recuperado el 10 de noviembre de 2023, de Atecnis: https://www.atecnis.com/que-es-sendinblue/

Atecnis. (10 de noviembre de 2021). *¿Qué es AWeber?* Obtenido de Atecnis.

aurum-informatica. (13 de abril de 2021). *¿Qué es el cableado de red y qué tipos existen?* Obtenido de AURUM INFORMÁTICA: https://www.aurum-informatica.es/blog/cableado-de-red-tipos

Bembibre., V. (febrero de 2009). *Definición de Tarjeta de red*. Recuperado el 20 de semptiembre de 2023, de DefiniciónABC: https://www.definicionabc.com/tecnologia/tarjeta-de-red.php#apa-abc

Bhatti, S. (21 de marzo de 2022). *¿Qué es la topología de red de malla?* Obtenido de HashDork: https://hashdork.com/es/what-is-mesh-network-topology/

biblus. (s.f.). *Redes de Área Local Inalámbricas*. Recuperado el 04 de octubre de 2023, de pdf: https://biblus.us.es/bibing/proyectos/abreproy/11579/fichero/f.+Cap%C3%ADtulo+2+-+Familia+IEEE+802.11.pdf+

blackbox. (s.f.). *Ventajas de la topología de anillo en Networking*. Recuperado el 12 de julio de 2023, de BlackBox: https://www.blackbox.com.mx/mx-mx/page/41987/Recursos/Technical/black-box-explica/LAN/Ring-Topologies-in-Networking

blog.incom. (s.f.). *QUE ES UNA RED ÓPTICA PASIVA (PON)*. Recuperado el 04 de octubre de 2023, de IMCOMBLOG.

Cabrera, A. (13 de diciembre de 2021). *¿Qué es MailChimp y para qué sirve?* Obtenido de atecnis: https://www.atecnis.com/que-es-mailchimp-y-para-que-sirve/

Caracao, M. A. (03 de mayo de 2023). *Qué es Odoo*. Obtenido de OpenWebinars: https://openwebinars.net/blog/que-es-odoo/

Carmen, J. (. (24 de julio de 2023). *¿Qué Es y Para Qué Sirve una Pagina Web?* Obtenido de cualhost: https://www.cualhost.com/sitios-web/para-que-sirve-una-pagina-web/

Carracao, M. Á. (03 de mayo de 2023). *Odoo*. Obtenido de OpenWebinars.net: https://openwebinars.net/blog/que-es-odoo/

Chillispot. (s.f.). *Chillispot*. Recuperado el 09 de noviembre de 2023, de Chillispot: https://www.chillispot.org/

CISCO. (18 de octubre de 2021). *¿Qué es un router?* Obtenido de CISCO: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html

CISCO. (18 de octubre de 2021). *¿Qué es un router?* Obtenido de CISCO: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html#~how-does-a-router-work

clearOS. (s.f.). Recuperado el 09 de noviembre de 2023, de clearOS: https://www.clearos.com/

Cloudfare. (9 de 07 de 2023). Obtenido de Red empresarial: https://www.cloudflare.com/es-es/learning/network-layer/enterprise-networking/

cloudflare. (s.f.). *¿Qué son las redes empresariales?* Recuperado el 21 de septiembre de 2023, de CLOUDFLARE: https://www.cloudflare.com/es-es/learning/network-layer/enterprise-networking/

cloudflare.com. (05 de julio de 2023). *Cloudflare*. Obtenido de que es una LAN: https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-lan/

cloudflare.com. (09 de julio de 2023). *Red empresarial*. Obtenido de Cloudflare: https://www.cloudflare.com/es-es/learning/network-layer/enterprise-networking/

Concepto. (10 de 07 de 2023). Obtenido de Html: https://concepto.de/html/

Concepto. (10 de 07 de 2023). Obtenido de Windows: https://app.bibguru.com/p/9aa9a6d1-eb21-422d-a5a5-b3262de29312

concepto.de. (05 de julio de 2023). *Concepto*. Obtenido de red LAN: https://concepto.de/red-lan/

concepto.de. (09 de julio de 2023). *Internet*. Obtenido de Concepto.de: https://concepto.de/internet/#ixzz86RT7DR6c

ConceptoABC. (11 de junio de 2020). *Redes inalámbricas*. Obtenido de ConceptoABC: https://conceptoabc.com/redes-inalambricas/

conceptoabc. (18 de mayo de 2021). *Red PAN*. Obtenido de ConceptoABC: https://conceptoabc.com/red-pan/

consejoderedaccion. (07 de agosto de 2023). *Aprende a crear listas y enviar correos masivos con MailChimp*. Obtenido de Consejo de Redacción: https://consejoderedaccion.org/formacion/crea-listas-correo-enviar-masivo-mailchimp

Coppola, M. E. (s.f.). *Cuál es la estructura HTML de una página web*. Recuperado el 23 de septiembre de 2023, de HupSpot: https://blog.hubspot.es/website/estructura-html#:~:text=La%20estructura%20HTML%20de%20una%20p%C3%A1gina%20web%20se%20compone%20de,elementos%20visibles%20de%20la%20p%C3%A1gina.

Datademia. (13 de enero de 2022). *¿Qué es Google Sheets?* Obtenido de Datademia: https://datademia.es/blog/que-es-google-sheets

DesarrolloWeb. (01 de enero de 2001). *Qué es HTML*. Obtenido de DesarrolloWeb.com: https://desarrolloweb.com/articulos/que-es-html.html

Ecured. (s.f.). *IPCop*. Recuperado el 09 de noviembre de 2023, de Ecured: https://www.ecured.cu/IPCop

Equipo editorial Etecé. (05 de agosto de 2021). *Internet*. Obtenido de Concepto.de: https://concepto.de/internet/

Equipo editorial, E. (s.f.). *Página web*. Recuperado el 23 de septiembre de 2023, de Concepto: https://concepto.de/pagina-web/

Equipo editorial, E. (s.f.). *Windows*. Recuperado el 23 de septiembre de 2023, de Concepto: https://concepto.de/windows-2/

Equipo editorial, Etecé. (05 de agosto de 2021). *Red de computadoras*. Obtenido de Concepto: https://concepto.de/red-de-computadoras/#ixzz83icbN8tA

Equipo editorial, Etecé. (05 de agosto de 2021). *Wifi*. Recuperado el 19 de septiembre de 2023, de concepto.de: https://concepto.de/wifi/

Fernández, Y. (. (9 de junio de 2023). *Xacata Basics*. Obtenido de Canva: https://www.xataka.com/basics/que-canva-como-funciona-como-usarlo-para-crear-diseno

Fernández, Y. (06 de marzo de 2020). *Encriptación*. Obtenido de Xataka Basics: https://www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos

Fernandez, Y. (23 de julio de 2021). *wps*. Obtenido de xataka.com: https://www.xataka.com/basics/boton-wps-router-que-se-usa

Fernández, Y. (3 de Octubre de 2023). *Servidores NAS: qué son, cómo funcionan y qué puedes hacer con uno*. Obtenido de Xataka: https://www.xataka.com/basics/servidores-nas-que-como-funcionan-que-puedes-hacer-uno

Flores, F. (22 de julio de 2022). *Qué es Visual Studio Code y qué ventajas ofrece*. Obtenido de OpenWebinars: https://openwebinars.net/blog/que-es-visual-studio-code-y-que-ventajas-ofrece/

fortinet. (s.f.). *¿Qué es una DMZ ?* Recuperado el 15 de agosto de 2023, de FORTINET: https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz

Fortiz. (06 de enero de 2013). *Qué es una PON, passive optical network?* Obtenido de CPVmicro: https://lafibraopticaperu.com/que-es-una-pon-passive-optical-network/

Galarza Vecilla, H. (Junio de 2023). *Proyecto de Titulación Héctor Galarza*. Obtenido de Repositorio del Instituto Superior Tecnológico Sudamericano de Quito: http://intesud-repositoriodigital.edu.ec:8080/jspui/bitstream/INTESUD/76/1/Proyecto%20de%20Titulaci%c3%b3n%20-%20Galarza%20Vecilla%20H%c3%a9ctor%20Andr%c3%a9s.pdf

García, F. (24 de julio de 2023). *que es google sheets*. Obtenido de Cliengo Blog: https://blog.cliengo.com/que-es-google-sheets/

García, Faviana. (14 de abril de 2023). *¿Qué es Google Sheets y cómo funciona? Lo que necesitas saber*. Obtenido de Cliengo Blog: https://blog.cliengo.com/que-es-google-sheets/

Ghimiray, D. (26 de agosto de 2022). *¿Qué es el WPA2 (Acceso protegido inalámbrico 2)?* Obtenido de AVG: https://www.avg.com/es/signal/what-is-wpa2

Gonzáles, M. S. (11 de agosto de 2013). *Redes telemáticas*. Obtenido de Switch: https://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

Gustavo, B. (11 de junio de 2023). *¿Qué es CSS?* Obtenido de HOSTINGER : https://www.hostinger.es/tutoriales/que-es-css

Gutiérrez, P. (s.f.). *¿Qué es MailChimp? Guía práctica en español para hacer email marketing*. Recuperado el 06 de agosto de 2023, de Comparapps: https://www.comparapps.com/que-es-mailchimp/

Hernández, S. (s.f.). *Servicio de red: ¿Qué son, para qué sirven y cuáles existen actualmente?* Recuperado el 22 de se`ptiembre de 2022, de INTERNETPASOAPASO: https://internetpasoapaso.com/servicio-de-red/

indaws. (s.f.). *Especialistas en Odoo*. Recuperado el 23 de septiembre de 2023, de inDAWS blog: https://www.indaws.es/en/blog/indaws-blog-1

Indaws. (s.f.). *Especialistas en Odoo*. Recuperado el 23 de septiembre de 2023, de inDAWS blog: https://www.indaws.es/en/blog/indaws-blog-1

informaticamoderna. (s.f.). *Tarjetas de red para fibra ópctica*. Recuperado el 20 de septiembre de 2023, de Informaticamoderna: https://www.informaticamoderna.com/Tarjetas_opticas.htm

internationalit. (28 de septiembre de 2021). *Topología de Red: conozca los principales tipos*. Recuperado el 21 de septiembre de 2023, de International IT:

https://www.internationalit.com/post/topologia-de-red-conozca-los-principales-tipos?lang=es

internationalit.com. (28 de septiembre de 2021). *International IT*. Obtenido de Topoloía de red: https://www.internationalit.com/post/topologia-de-red-conozca-los-principales-tipos?lang=es

InvestGlass. (18 de agosto de 2023). *Correo electrónico masivo: Definición, buenas prácticas y preguntas frecuentes.* Obtenido de InvestGlass: https://www.investglass.com/es/mass-email-definition-best-practices-and-faqs/

iTecan. (15 de Noviembre de 2021). *Guía rápida de Odoo: El mailing masivo*. Obtenido de iTecan: https://itecan.es/guia-rapida-mailing-odoo/

Jariam. (31 de mayo de 2020). *¿Qué es, para qué sirve y cómo funciona una red CAN?* Obtenido de Mira Cómo se hace: https://miracomosehace.com/sirve-como-funciona-red-can/

Javired, J. (2 de diciembre de 2020). *Que Es Una Red de Área Metropolitana Y Sus Características*. Obtenido de MundoApps: https://mundoapps.net/que-es-una-red-de-area-metropolitana/

jimdofree. (s.f.). *Topologías*. Recuperado el 21 de septiembre de 2023, de Mis clases de informárica: https://peopleuniversity.jimdofree.com/software/topologias/

John. (06 de julio de 2021). *¿Qué es un patch panel y por qué lo necesitamos?* Obtenido de FS community: https://community.fs.com/es/blog/what-is-a-patch-panel-and-why-use-it.html

keepcoding. (s.f.). *¿Qué es pfSense?* Recuperado el 28 de junio de 2023, de KeepCoding Tech Shool: https://keepcoding.io/blog/que-es-pfsense/

Keepcoding. (5 de 08 de 2022). *Keepcoding*. Obtenido de Etiquetas básicas en HTML: https://keepcoding.io/blog/7-etiquetas-basicas-en-html/

keepcoding. (23 de octubre de 2023). *¿Qué es pfSense?* . Obtenido de KEEPCODING: https://keepcoding.io/blog/que-es-pfsense/

Lorente, V. M. (14 de mayo de 2014). *Implementación de un portal cautivo con Wifidog*. Obtenido de AULA SOFT WARE LIBRE: https://www.uco.es/aulasoftwarelibre/375-implementacion-de-un-portal-cautivo-con-wifidog/

luz, S. (. (15 de junio de 2023). *Vlan*. Obtenido de RedesZone: https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Mailchimp. (10 de Noviembre de 2023). *Planes de precios de Mailchimp*. Obtenido de Mailchimp: https://mailchimp.com/es/pricing/marketing/

mailchimp. (s.f.). *Acerca de los niveles de precios de Mailchimp*. Recuperado el 23 de septiembre de 2023, de INTUIT mailchimp: https://mailchimp.com/es/help/mailchimp-pricing-tiers/

Medina, F. (21 de diciembre de 2021). *Google Sheets vs. Excel: ¿Qué herramienta te conviene utilizar?* Obtenido de crehana: https://www.crehana.com/blog/negocios/google-sheets-vs-excel/

microinformatica.jimdofree. (s.f.). *Conectores de red*. Recuperado el 20 de septiembre de 2023, de Técnico en sistemas Microinfórmaticos: https://microinformatica.jimdofree.com/inicio/conectores-de-red/

Mit Mut. (23 de Febrero de 2021). *La aplicación de Marketing por e-mail en Odoo*. Obtenido de Lajapyme S.A de C.V: https://www.mit-mut.com/blog/aplicaciones-de-odoo-6/e-marketing-12

Moes, T. (julio de 2023). *¿Qué es un firewall (cortafuegos)? Todo sobre ello (2023)*. Recuperado el 22 de septiembre de 2023, de Software: https://softwarelab.org/es/que-es-un-firewall/

Moraestudiocreativo. (s.f.). *Guía Mailchimp*. Recuperado el 10 de noviembre de 2023, de Mora Estudio Creativo: https://moraestudiocreativo.es/email-marketing-con-mailchimp/

Muñoz, I. (16 de marzo de 2023). *¿Qué hace el botón WPS de tu router?* . Obtenido de Computer hoy: https://computerhoy.com/tutoriales/hace-boton-wps-router-descubre-funcion-como-usarlo-1216262

Netgate. (s.f.). *Vales*. doi:https://docs.netgate.com/pfsense/en/latest/captiveportal/vouchers.html

Nettix. (s.f.). *¿Qué es pfsense? Y porque es un Firewall tan popular*. Recuperado el 09 de noviembre de 2023, de Nettix: https://www.nettix.com.pe/documentacion/administracion/vpn/que-es-pfsense-y-porque-es-un-firewall-tan-popular/

Nettix. (24 de febrero de 2021). *¿QUÉ ES PFSENSE? Y PORQUE ES UN FIREWALL TAN POPULAR*. Obtenido de Nettix: https://www.nettix.com.pe/documentacion/administracion/vpn/que-es-pfsense-y-porque-es-un-firewall-tan-popular/

nettix. (s.f.). *ANÁLISIS DE PFSENSE COMO UNA ALTERNATIVA A OTROS FIREWALLS COMERCIALES*. Recuperado el 07 de agosto de 2023, de nettix: https://www.nettix.com.pe/blog/firewall/analisis-de-pfsense-como-una-alternativa-a-otros-firewalls-comerciales/

Nettix. (s.f.). *Análisis de PfSense como una alternativa a otros firewalls comerciales*. Recuperado el 09 de noviembre de 2023, de Nettix: https://www.nettix.com.pe/blog/firewall/analisis-de-pfsense-como-una-alternativa-a-otros-firewalls-comerciales/

nettix. (s.f.). *CARACTERÍSTICAS TÉCNICAS Y FUNCIONALIDADES DE PFSENSE*. Recuperado el 09 de noviembre de 2023, de Nettix:

https://www.nettix.com.pe/blog/web-blog/caracteristicas-y-funcionalidades-de-pfsense/

Nettix. (s.f.). *CARACTERÍSTICAS TÉCNICAS Y FUNCIONALIDADES DE PFSENSE*. Recuperado el 07 de agosto de 2023, de nettix: https://www.nettix.com.pe/blog/web-blog/caracteristicas-y-funcionalidades-de-pfsense/

Newman, P. (. (30 de junio de 2023). *Reseña de Aweber 2023: funciones, precios y principales pros y contras*. Obtenido de EMAIL VENDOR SELECTION: https://www.emailvendorselection.com/es/resena-de-aweber/

Odoo. (07 de agosto de 2023). *Odoo*. Recuperado el 07 de agosto de 2023, de Odoo S.A.: https://www.odoo.com/es_ES/pricing-plan

ordenadores-y-portatiles. (1 de junio de 2020). *¿Qué es y Para que Sirve un Punto de Acceso?* Obtenido de Ordenadores y Portátiles: https://ordenadores-y-portatiles.com/punto-de-acceso/

Pablo. (05 de diciembre de 2022). *el cifrado AES*. Obtenido de By Orange: https://blog.orange.es/navegacion-segura/cifrado-aes/

Pablok. (30 de 09 de 2022). *¿Qué es el DMZ?* Obtenido de CTX Detectives: https://www.ctxdetectives.com/que-es-el-dmz/

Pardo, L. (26 de marzo de 2022). *IPCop: Linux hecho firewall*. Obtenido de NEOTEO: https://www.neoteo.com/ipcop-linux-hecho-firewall-15273/

Pérez Porto, J. y. (17 de agosto de 2011). *Red de computadoras*. Obtenido de Tecnoloía: https://definicion.de/red-de-computadoras/

Pfsense. (s.f.). *Pfsense*. Recuperado el 29 de octubre de 2023, de Pfsense: https://www.pfsense.org/download/

Plieshakov, A. (. (19 de septiembre de 2023). *¿Qué es una tarjeta de red y cuál es su función?* Recuperado el 20 de semptiembre de 2023, de INFOCOMPUTER: https://www.info-computer.com/blog/que-es-una-tarjeta-de-red-y-cual-es-su-funcion/

Porto, P. (16 de octubre de 2019). *Firewall*. Obtenido de Definición.de: https://definicion.de/firewall/

profesores. (s.f.). *concepto de una red*. Recuperado el 20 de septiembre de 2023, de INTRODUCCION A REDES: https://www.profesores.frc.utn.edu.ar/sistemas/ingcura/archivos_com/componentes.asp

Rada, A. (15 de Febrero de 2023). *Precios de Mailchimp 2023*. Obtenido de vibetrace: https://vibetrace.com/es/mailchimp-precio-cuanto-cuesta-en-2023/

Randrianarimanana, M. (s.f.). *Installation d'un Serveur d'authentification WifiDog.* Recuperado el 09 de noviembre de 2023, de mrandrianarimanana.wordpress.com: https://mrandrianarimanana.files.wordpress.com/2019/05/fiche_de_procc3a9dure_wifidoginstallation_mikajy_randrianarimanana-portail_captif_v-v2.pdf

redesinformaticas. (11 de marzo de 2023). *Redes SAN: ¿Qué son? Características, funciones y ventajas*. Obtenido de REDESINFORMATICAS: https://redesinformaticas.org/red-san/

redesinformaticas. (s.f.). *Redes SAN: ¿Qué son? Características, funciones y ventajas*. Recuperado el 04 de octubre de 2023, de Redes Informáticas: https://redesinformaticas.org/red-san/

redesinformaticas. (s.f.). *Redes WLAN: ¿Qué es? Características, funciones y ventajas*. Recuperado el 21 de septiembre de 2023, de REDESINFORMATICAS: https://redesinformaticas.org/red-wlan/

Roberto, C. (22 de junio de 2011). *ClearOS, solución de servidor de código libre para las pymes*. Obtenido de Pymes y Autonomos: https://www.pymesyautonomos.com/tecnologia/clearos-solucion-de-servidor-de-codigo-libre-para-las-pymes

Rojas, J. (7 de junio de 2023). *WLAN, ¿Qué es y como funciona?* Obtenido de clavedemodem: https://clavedemodem.com/wlan/

Roymo. (s.f.). *Mailchimp.* Recuperado el 10 de noviembre de 2023, de Rommel y Montgomery: https://roymo.es/glosario/mailchimp/

Rufus. (s.f.). *Rufus*. Recuperado el 29 de octubre de 2023, de Rufus: https://rufus.ie/es/

Ruiz, P. (9 de Enero de 2017). *ClearOS: Una distribución GNU/Linux que simplifica la administración de servidores*. Recuperado el 09 de noviembre de 2023, de Somebooks.es: http://somebooks.es/clearos-una-distribucion-gnulinux-simplifica-la-administracion-servidores/

Sanchez, A. L. (s.f.). *¿Qué es un switch?* Recuperado el 04 de octubre de 2023, de About Español: https://www.aboutespanol.com/que-es-un-switch-841388

SendPulse. (s.f.). *Correos masivos*. Recuperado el 23 de septiembe de 2023, de SendPulse: https://sendpulse.com/latam/support/glossary/bulk-email

Shaw, K. (03 de febrero de 2018). *IDG Communications S.A.U.* Obtenido de COMPUTERWORLD: https://www.computerworld.es/wifi/80211-estandares-de-wifi-y-velocidades

Sisternas, P. (22 de sepriembre de 2022). *Todas las diferencias entre Excel y Google Sheets*. Obtenido de Just EXW by Fleebe: https://es.justexw.com/todas-las-diferencias-entre-excel-y-google-sheets.html

slideshare. (06 de octubre de 2015). *pfsense*. Obtenido de slideshare: https://pt.slideshare.net/anthonypereapedraza/pfsense-53628113?next_slideshow=true

soporteti. (16 de diciembre de 2015). *IpCop Linux Firewall Parte II Características*. Obtenido de El Blog de soporteTI: https://blog.soporteti.net/ipcop-linux-firewall-parte-ii-caracteristicas/

Sossa, D. Z. (s.f.). *Evolución de los estándares IEEE 802.11*. Recuperado el 22 de septiembre de 2023, de Sutori: https://www.sutori.com/en/daniela-zurita-sossa?tab=profile

stackscale. (10 de febrero de 2023). *¿Qué es una VPN, cómo funciona y para qué se usa?* Obtenido de Stackscale: https://www.stackscale.com/es/blog/que-es-una-vpn/

Sutori. (9 de 07 de 2023). Obtenido de Evolución de los estándares: https://www.sutori.com/en/story/estandar-ieee-802-11--8CkpVc7WCJZMSUno2tJwuUaq

Synology. (s.f.). *¿Qué es NAS?* Recuperado el 12 de Noviembre de 2023, de Synology: https://www.synology.com/es-mx/dsm/solution/what-is-nas/for-home

techinstyle. (s.f.). *techinstyle*. Recuperado el 28 de octubre de 2023, de techinstyle: https://techinstyle.asus.com/wp-content/uploads/2017/03/bios-6c.jpg

TerraMaster. (s.f.). *¿QUÉ ES NAS?* Recuperado el 12 de Noviembre de 2023, de Terra-Master.com: https://www.terra-master.com/es/what_is_nas/#:~:text=TNAS%20(TerraMaster%20NAS)%20es%20un,las%20peque%C3%B1as%20y%20medianas%20empresas.

ticportal. (05 de diciembre de 2022). *Servidores*. Obtenido de tic.PORTAL: https://www.ticportal.es/glosario-tic/servidores

ticportal.es. (05 de diciembre de 2022). *Servidores*. Obtenido de tic.PORTAL: https://www.ticportal.es/glosario-tic/servidores

tokioschool. (18 de enero de 2023). *¿Qué tipos de redes informáticas existen?* Obtenido de Tokio: https://www.tokioschool.com/noticias/tipos-redes-informaticas/

Topología de red. (28 de 09 de 2021). Obtenido de Topolía de red: https://www.internationalit.com/post/topologia-de-red-conozca-los-principales-tipos?lang=es

trendmicro. (12 de julio de 2023). *¿Qué es seguridad de red?* Obtenido de TREND micro: https://www.trendmicro.com/es_es/what-is/network-security.html

trey.es. (19 de julio de 2023). *Odoo*. Obtenido de Trey, Kilobytes de Soluciones S.L.: https://trey.es/que-es-odoo-y-como-funciona

Urrutia, D. (19 de abril de 2023). *Qué es Encriptación*. Obtenido de ARIMETRICS: https://www.arimetrics.com/glosario-digital/encriptacion

wikipedia. (12 de julio de 2023). Obtenido de wikipedia: https://es.wikipedia.org/wiki/IEEE_802.11

wikipedia. (23 de agosto de 2023). *Red de área amplia*. Obtenido de wikipedia: https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_amplia

wikipedia. (27 de mayo de 2023). *Red de área metropolitana*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_metropolitana

Wikipedia contributors. (s.f.). *TrueNAS*. Recuperado el 12 de Noviembre de 2023, de Wikipedia, The Free Encyclopedia: https://es.wikipedia.org/w/index.php?title=TrueNAS&oldid=138028384

wikipedia. (s.f.). *Red privada*. Recuperado el 21 de septiembre de 2023, de Wikipedia: https://es.wikipedia.org/wiki/Red_privada

Wikipedia. IEEE, 802.11. (9 de 07 de 2023). Obtenido de Wikipedia : https://es.wikipedia.org/wiki/IEEE_802.11

wikiwand. (s.f.). *IEEE 802.1Q*. Recuperado el 22 de septiembre de 2023, de Wikiwand: https://www.wikiwand.com/es/IEEE_802.1Q#Referencias

wordpress. (09 de mayo de 2017). *Red en bus*. Obtenido de Clasificación de las redes: https://clasificaciondelasredesblog.wordpress.com/2017/05/09/topologia-estrella/

wordpress. (s.f.). *CREPS de Poitiers*. Obtenido de Stage BTS2SIO.

Zawi, A. (28 de noviembre de 2020). *Result*. Obtenido de pfSense: https://redmine.pfsense.org/attachments/3262

ANEXOS

Anexo 1: Documentación de pfSense

Anexo 2: Documentación de correo masivos MailChimp

Anexo 3: Documentación del servidor NAS