



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
ESCUELA PROFESIONAL DE INGENIERIA EN
COMPUTACION E INFORMATICA



TESIS

“DISEÑO DE UN SISTEMA DE SEGURIDAD DE RED BASADO
EN LA INTEGRACIÓN DE LOS SERVIDORES RADIUS - LDAP
EN LINUX PARA FORTALECER EL ACCESO DE LA RED DE
LA CLÍNICA MILLENIUM CHICLAYO 2016”

PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN E INFORMÁTICA

AUTOR

BACH. ALBUJAR MORENO OSMAR RICARDO

ASESOR

ING. ALARCÓN GARCÍA ROGER ERNESTO

LAMBAYEQUE – PERÚ

2017

UNIVERSIDAD NACIONAL PEDRO RUIZ GLLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE COMPUTACIÓN E INFORMÁTICA

TESIS

“DISEÑO DE UN SISTEMA DE SEGURIDAD DE RED BASADO EN LA INTEGRACIÓN DE LOS SERVIDORES RADIUS – LDAP EN LINUX PARA FORTALECER EL ACCESO DE LA RED DE LA CLÍNICA MILLENIUM CHICLAYO 2016”

PRESENTADO POR:

BACH. ALBUJAR MORENO OSMAR RICARDO

ASESOR:

ING. ALARCÓN GARCÍA ROGER ERNESTO

UNIVERSIDAD NACIONAL PEDRO RUIZ GLLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE COMPUTACIÓN E INFORMÁTICA

Los Señores Miembros del Jurado de la tesis titulada **“Diseño de un sistema de seguridad de red basado en la integración de los servidores RADIUS – LDAP en linux para fortalecer el acceso de la red de la Clínica Milenium Chiclayo 2016”**, designados por el Decano de la Facultad de Ciencias Físicas y Matemáticas de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque, certifican y aprueban la defensa de la tesis presentado por el bachiller en Computación e Informática, Albuja Moreno Osmar Ricardo. En el cumplimiento parcial de los requisitos necesarios para la obtención del título profesional de Ingeniero en Computación e Informática.

M. Sc. Armando José Moreno Heredia
Presidente del jurado

M. Sc. Jessie Leila Bravo Jaico
Secretario del Jurado

Ing. Nilton César Germán Reyes
Vocal del Jurado

Fecha de Defensa: Setiembre – 2017

DEDICATORIA

Este trabajo se lo dedico a Dios, a mis padres, quienes son los modelos a seguir más grandes que tengo, me apoyaron en lo emocional y de la misma manera en todo el transcurso de mi formación profesional, teniendo confianza de mi capacidad para lograr esta meta.

A las personas cercanas que me incentivaron y fueron la fuerza para perseverar y cumplir mis objetivos.

Osmar Ricardo Albujar Moreno

AGRADECIMIENTO

El más profundo y sincero agradecimiento a:

La Clínica “Millenium” en la persona del MBA. Victor Loayza Carbajal, Gerente por ofrecerme la oportunidad y apoyo en las coordinaciones con las diversas áreas de la institución y así desarrollar el presente trabajo.

Al Ing. Roger Alarcón García por su guía y ayuda predispuesta a lo largo de la investigación realizada.

Al Ing. Miguel López Campoverde por proveerme desinteresadamente de información fundamental al inicio de este trabajo.

Al Ing. Iván Fernández Paz, Ing. Martin Leiva y a nuestros docentes porque cada uno de ellos aportó de manera importante en mi formación profesional.

A mis colegas, amigos y aquellas personas que me incitaron a la investigación a lo largo de estos años.

Osmar Ricardo Albujar Moreno

INTRODUCCIÓN

Las redes de telecomunicaciones en el sector salud han contribuido en ofrecer una mejor calidad de servicio a los pacientes, disminuyendo considerablemente el tiempo de espera, dando paso a la telemedicina la cual generó la disponibilidad de atención en localizaciones que antes era casi imposible lograr. Las redes cableadas proporcionan a los usuarios una buena seguridad y la capacidad de mover muchos datos de manera rápida y efectiva, este tipo de conexión trabaja a altas tasas de velocidad y en el proceso de transferencia de datos la velocidad se mantiene, no depende de agentes externos.

Adicionalmente, las redes inalámbricas Wi-Fi se están convirtiendo en el soporte de la movilidad en los entornos hospitalarios, y su despliegue está creciendo a una tasa exponencial. Estas redes no sólo están dando soporte al despliegue en movilidad de sistemas de voz o de la Historia Clínica Electrónica, sino que también están dando soporte a los cientos de dispositivos y aplicaciones médicas móviles, como los sistemas de monitorización de pacientes o de administración de medicamentos. Además, y como ocurre en cualquier otro entorno, las redes WLAN de los hospitales se están viendo saturadas por el uso de portátiles y Tablets para registrar y consultar datos de pacientes, además de los dispositivos personales que empleados y visitas utilizan de forma asidua.

El uso no controlado de estos dispositivos, no sólo por parte de personal facultativo, sino por el público en general, puede poner en peligro tanto la privacidad de la información de los pacientes como la disponibilidad de la propia red para dar servicio en condiciones adecuadas, al sobrepasar la capacidad de dicha red y de los recursos de TI. Los usuarios exigen cada vez más conectividad para sus Smartphone y Tablets cuando visitan el hospital. En principio, todos estos dispositivos van a utilizar el mismo entorno de red que los equipos médicos críticos (telemetría, biomedicina, sistemas RTLS, etc.), conectados tanto por cable como por Wi-Fi y cada uno de ellos con necesidades específicas en cuanto a seguridad, calidad de servicio, prioridad de acceso a datos y ancho de banda.

El sector de telecomunicaciones en el Perú se encuentra en un proceso de cambio. La rápida expansión de la telefonía móvil, la transición digital, el impulso del gobierno electrónico y la decisión política de universalizar el acceso a servicios de banda ancha, dando oportunidad de crecimiento para la ampliación del acceso a internet. Sin embargo, son pocas las empresas que, a pesar de tener implementado una red de telecomunicaciones moderna, pueda usarse a cabalidad debido a la falencia de seguridad en las redes, en especial en lo que se refiere a red inalámbrica.

II

RESUMEN

La presente tesis, se enfoca en casos relevantes a desarrollar en la Clínica Millenium de Chiclayo, por consiguiente se considera importante y necesario realizar el diseño de un sistema de seguridad basado en la integración de los servidores RADIUS – LDAP en linux.

El proceso empieza con una introducción sobre la problemática de la Clínica Millenium de Chiclayo, entre los principales inconvenientes está la estructura de red inconveniente (pocas áreas están conectas en la red y asignaciones de IP's sin registros ni administración), no hay control al acceso de red inalámbrica, no existe un área de TI en la que se administre la red (el router, switches, servidores se encuentra en distintas ubicaciones y los ambientes son inadecuados).

Esto ha ocasionado alta latencia de la red en horas pico, retrasando los procesos en la clínica y en algunos casos caída total de la red. El ingreso a la red por contraseña compartida facilita el robo de información, cualquier usuario sin necesidad de autenticarse puede ingresar a la red conociendo la contraseña compartida.

Por ello, la integración del servidor RADIUS-LDAP implementada mediante la metodología de Top-Down network design proveerá con servicios de autenticación especializada. Se propone rediseñar la red con cableado estructurado para restablecer la transferencia de información constante, brindar soporte de redes LAN virtuales, de esta manera segmentar las áreas en subredes y aumentar el nivel de protección (Asignaciones de IP's administrada y Listas de control de Acceso ACL's), diseño del área TI, la adquisición de equipos y dispositivos de red intermediarios de gama alta (Switches, Router, Firewall, etc).

Todo sumado con el propósito de elevar la seguridad, productividad de la clínica, haciéndola robusta y escalable ante un crecimiento tecnológico futuro.

III

ABSTRACT

The present Thesis focuses in relevant cases to develop in Millenium's Clinic from Chiclayo, for that reason it considers important and necessary to make a design of a security system based in RADIUS – LDAP server's integration on linux, documenting the design process.

Process starts with an introduction about Millenium's Clinic problematic, among the main disadvantages is the inconvenient network structure (just few areas are connected in network and IP assignments without registry or management), there is not wireless network access control, doesn't exist an IT area which gets management the network (router, switches, servers are located in different places and the environments are inappropriate).

It brings about high latency in network in several moments, slowing down process in the clinic and some cases total fall of network. The network entrance by shared password get easy the thief of information, any user can enter without authenticate, he just need to know the shared password.

Therefore, integration of servers RADIUS – LDAP, implemented though Top-Down network design methodology will provide with specialized authentication services. It proposes redesign the network with structured cabling to restart a constant information transfer, providing LAN virtual network support, in this way get segment areas in subnetworks and increase the protection level (management of IP assignments and Access control Lists ACL's), IT area design, the acquisition of equipment and intermediary network devices (Router, Switches, Firewall, etc.).

All added to propose to gets the security high, productivity of the clinic, make it robust and scalable against an increase technological future.

IV

ÍNDICE

INTRODUCCION.....	I
RESUMEN.....	II
ABSTRACT.....	III
INDICE.....	IV
INDICE DE ILUSTRACIONES.....	V
INDICE DE TABLAS.....	VI
CAPITULO I: Datos Generales de la Organización.....	17
1.1. Descripción de la Organización	17
1.2. Misión, Visión y Objetivos de la Organización.....	17
1.2.1. Misión.....	17
1.2.2. Visión	17
1.2.3. Objetivos.....	17
1.3. Estructura Orgánica	18
CAPITULO II: Problemática de la Investigación	20
2.1. Realidad Problemática	20
2.1.1. Planteamiento del Problema	20
2.2. Formulación del Problema.....	25
2.3. Justificación e Importancia de la Investigación.....	25
2.3.1. Justificación Social.....	27
2.3.2. Justificación Económica	27
2.3.3. Justificación Tecnológica	27
2.4. Objetivos de la Investigación	28
2.4.1. Objetivo General	28
2.4.2. Objetivos Específicos.....	28
2.5. Limitaciones de la Investigación.....	28
CAPITULO III: Marco Metodológico	30
3.1. Tipo de Investigación	30
3.2. Hipótesis.....	30
3.3. Variables.....	30
CAPITULO IV: Marco Teórico	32
4.1. Antecedentes	32
4.1.1. Antecedentes en el contexto internacional	32
4.2. Base Teórica	34
4.2.1. Autenticación	34
4.2.2. Autorización	43

4.2.3. Accounting	45
4.2.4. Modelo de referencia TCP/IP	46
4.2.5. Seguridad en redes Inalámbricas	50
4.2.6. Protocolos de confidencialidad e integridad de datos	58
4.2.7. Sistemas Operativos Linux	59
4.2.8. Protocolos RADIUS y LDAP	64
4.2.9. Servidor de Dominios	67
4.2.10. Servidor RADIUS y LDAP	73
4.2.11. Metodología de Redes	77
4.2.12. Redes Privadas Virtuales – VLAN	80
4.3. Concepto y definiciones	86
CAPÍTULO V: Desarrollo de la Propuesta	90
5.1. Recursos Humanos	90
5.2. Metodología CISCO Top-Down Network Design	90
5.2.1. Fase I: Análisis de Negocios Objetivos y limitaciones	90
5.2.2. Fase II: Análisis de datos y Requisitos	94
5.2.3. Fase III: Diseño de la solución	97
5.2.4. Fase IV: Simulación de la estructura de red y Equipos Propuestos	162
CAPITULO VI: Costos y Beneficios	174
6.1. Análisis de Costos y Beneficios.....	174
6.2. Beneficios.....	176
CAPITULO VII: Conclusiones	178
CAPITULO IX: Referencias Bibliográficas.....	181
ANEXOS.....	183

V

INDICE DE ILUSTRACIONES

Ilustración 1: Organigrama de la Clínica (Millenium, 2016)	18
Ilustración 2: Esquema de la Red Actual de la Clínica Millenium	22
Ilustración 3: Análisis de la red inalámbrica – Clínica Millenium utilizando la herramienta Acrylic Wifi Professional.....	23
Ilustración 4: Resultado de encuesta 01	26
Ilustración 5: El modelo TCP/IP con algunos protocolos	50
Ilustración 6: Los desarrolladores de shareware poseen su propia asociación.....	60
Ilustración 7: En el sitio oficial del proyecto GNU (www.gnu.org)	61
Ilustración 8: Logo del Sistema Operativo Ubuntu	63
Ilustración 9: Dial-Access network usando RADIUS.....	73
Ilustración 10: Estructura de una VLAN	80
Ilustración 11: Segmentación VLAN.....	81
Ilustración 12: Puertos Troncale	84
Ilustración 13: Esquema de la Red Actual de la Clínica	92
Ilustración 14: Gabinete de red.....	99
Ilustración 15: Aire de Expansión Directa	99
Ilustración 16: Extintor ABC.....	99
Ilustración 17: UPS.....	99
Ilustración 18: PDU de 12 receptáculos	99
Ilustración 19: Diseño del centro de datos propuesto.....	100
Ilustración 20: Ejemplo de etiquetado de red	101
Ilustración 21: Plano Primera Planta	106
Ilustración 22: Plano Segunda Planta	107
Ilustración 23: Plano Tercera Planta.....	108
Ilustración 24: Plano Cuarta Planta	109
Ilustración 25: Cable categoría 6a.....	110
Ilustración 26: Roseta doble.....	110
Ilustración 27: Conector RJ-45 Hembra	110
Ilustración 28: Conector RJ-45 Macho	110
Ilustración 29: Interacción entre usuario, cliente RADIUS y servidor RADIUS-LDAP.....	112
Ilustración 30: Secuencia de autenticación y autorización RADIUS	117
Ilustración 31: Diseño lógico Firewall.....	117
Ilustración 32: Diseño Lógico. Arquitectura de autenticación propuesta	118
Ilustración 33: Diseño Lógico propuesto	119
Ilustración 34: Servidor SLDAP Asignar contraseña administrador	126
Ilustración 35: Servidor SLDAP configuración inicial.....	126
Ilustración 36: Servidor SLDAP configuración inicial.....	127
Ilustración 37: Servidor SLDAP configuración inicial.....	127
Ilustración 38: Servidor SLDAP configuración inicial.....	127
Ilustración 39: Servidor SLDAP configuración inicial.....	128
Ilustración 40: Servidor SLDAP configuración inicial.....	128
Ilustración 41: Servidor SLDAP configuración inicial.....	128
Ilustración 42: Servidor LDAP servicios básicos	129
Ilustración 43: Servidor LDAP configuración archivo ldap.conf por defecto	129

Ilustración 44: Servidor LDAP configuración archivo ldap.conf	130
Ilustración 45: Servidor Freeradius estado del servidor	132
Ilustración 46: Servidor Freeradius archivo clients.conf	132
Ilustración 47: Servidor Freeradius archivo eap.conf	133
Ilustración 48: Servidor Freeradius archivo radiusd.conf - A	134
Ilustración 49: Servidor Freeradius archivo radiusd.conf por defecto	134
Ilustración 50: Servidor Freeradius archivo radiusd.conf B.....	135
Ilustración 51: Servidor Freeradius archivo ldap por defecto.....	135
Ilustración 52: Servidor Freeradius archivo ldap.....	136
Ilustración 53: Servidor Freeradius archivo default A por defecto	137
Ilustración 54: Servidor Freeradius archivo default A	137
Ilustración 55: Servidor Freeradius archivo default B por defecto	137
Ilustración 56: Servidor Freeradius archivo default B	138
Ilustración 57: Servidor Freeradius archivo inner-tunnel A por defecto	138
Ilustración 58: Servidor Freeradius archivo inner-tunnel A	138
Ilustración 59: Servidor Freeradius archivo inner-tunnel B por defecto	139
Ilustración 60: Servidor Freeradius archivo inner-tunnel B	139
Ilustración 61: Servidor Freeradius archivo inner-tunnel C por defecto	139
Ilustración 62: Servidor Freeradius archivo inner-tunnel C	140
Ilustración 63: Comprobación de conectividad FreeRADIUS con autenticación LDAP ...	140
Ilustración 64: Menú Principal JXplorer.....	143
Ilustración 65: Ventana de conexión a un servidor LDAP	143
Ilustración 66: Datos para la conexión al servidor LDAP mediante JXplorer	144
Ilustración 67: Menú del servidor LDAP JXplorer – grupos registrados	144
Ilustración 68: Menú del servidor LDAP JXplorer – usuarios registrados	145
Ilustración 69: Configuraciones previas para usar securityW2 1.....	145
Ilustración 70: Configuraciones previas para usar securityW2 2.....	146
Ilustración 71: Configuraciones previas para usar securityW2 3.....	146
Ilustración 72: Configuraciones previas para usar securityW2 4.....	146
Ilustración 73: Configuraciones previas para usar securityW2 5.....	147
Ilustración 74: Configuraciones previas para usar securityW2 6.....	147
Ilustración 75: Configuraciones previas para usar securityW2 7.....	148
Ilustración 76: Configuraciones para usar securityW2 1	148
Ilustración 77: Configuraciones para usar securityW2 2	148
Ilustración 78: Configuraciones para usar securityW2 3	149
Ilustración 79: Configuraciones para usar securityW2 4	149
Ilustración 80: Configuraciones para usar securityW2 5	149
Ilustración 81: Verificación de conexión a la red inalámbrica	150
Ilustración 82: Configuración para la conexión a la red inalámbrica en SO Android 1	150
Ilustración 83: Configuración para la conexión a la red inalámbrica en SO Android 2	151
Ilustración 84: Configuración para la conexión a la red inalámbrica en SO Android 3	151
Ilustración 85: Configuración para la conexión a la red inalámbrica en SO Android 4	151
Ilustración 86: Verificación de la conexión a la red inalámbrica en SO Android	152
Ilustración 87: Instalación del plug-in PGINA - A.....	152
Ilustración 88: Acuerdo de Licencia Plug-in PGINA.....	153
Ilustración 89: Selección destino de instalación del Plug-in PGINA	153
Ilustración 90: Creación del atajo para el Plug-in PGINA.....	153
Ilustración 91: Icono de escritorio del Plug-in PGINA.	154

Ilustración 92: Instalación del Plug-in PGINA.....	154
Ilustración 93: Fin de la instalación y ejecución del Plug-in PGINA	154
Ilustración 94: Plug-in PGINA menú principal	155
Ilustración 95: Plug-in PGINA pestaña Plugin selection por defecto	155
Ilustración 96: Plug-in PGINA pestaña Plugin selection correcta	156
Ilustración 97: Plug-in PGINA pestaña Plugin Settings por defecto.....	156
Ilustración 98: Plug-in PGINA pestaña Plugin Settings.....	157
Ilustración 99: Plug-in PGINA pestaña Plugin Order por defecto	157
Ilustración 100: Plug-in PGINA pestaña Plugin Order correcta	158
Ilustración 101: Plug-in PGINA pestaña Simulation por defecto	158
Ilustración 102: Plug-in PGINA pestaña Simulation. Prueba de un usuario LDAP	159
Ilustración 103: Panel de control Usuario de escritorio	159
Ilustración 104: Carpeta de Opciones de Seguridad Local - Usuario de escritorio.....	160
Ilustración 105: Directivas de Seguridad Local - Usuario de escritorio.....	160
Ilustración 106: Habilitar Directivas de Seguridad Local - Usuario de escritorio	161
Ilustración 107: Simulación de la red propuesta.....	162
Ilustración 108: Router CISCO 800 series	165
Ilustración 109: Switch CISCO 2960-L 48 puertos	168
Ilustración 110: TP-Link TL-WR843N.....	170
Ilustración 111. CISCO Firewall ASA 5520	171

VI

INDICE DE TABLAS

Tabla 1. Variables Operacionales.....	30
Tabla 2: Zona de autoridad – Tipo de Registro	71
Tabla 3: Cuadro comparativos de metodología de redes.	77
Tabla 4. Recursos Humanos	90
Tabla 5: Direcciones IP actuales.	93
Tabla 6: Computadores existentes en la Clínica.....	93
Tabla 7: Impresoras existentes en la Clínica	94
Tabla 8: Protocolos de autenticación.....	94
Tabla 9: Servidor de Base de Datos.....	95
Tabla 10. Firewall o Cortafuegos.....	96
Tabla 11: Infraestructura para la simulación del control de acceso	97
Tabla 12: Etiquetado de red.....	103
Tabla 13: Puntos de datos para equipos y dispositivos intermediarios.....	104
Tabla 14: Puntos de dato de cableado backbone.	105
Tabla 15. Configuraciones Servidor LDAP	113
Tabla 16. Configuración NAS	114
Tabla 17. Configuración para habilitar la autenticación mediante LDAP	114
Tabla 18. Grupos Organizativos	115
Tabla 19. Usuario LDAP.....	116
Tabla 20. Directivas de seguridad del Firewall.....	121
Tabla 21. Directivas de seguridad de Switches.....	121
Tabla 22: Direccionamiento IP propuesto.	122

Tabla 23: Creación de VLANS.....	123
Tabla 24: Asignación de VLANS.....	124
Tabla 25: Comparativa Empresas fabricantes de equipos de red.....	163
Tabla 26: Comparación de Routers CISCO	165
Tabla 27: Datos técnicos Router CISCO 800 series.	168
Tabla 28: Datos técnicos Switch CISCO 2960-L.....	169
Tabla 29: Datos técnicos TP-LINK TL-WR843N.....	171
Tabla 30. Datos técnicos Firewall CISCO ASA 5520	172
Tabla 31: Hardware y materiales	174
Tabla 32. Costos de los Softwares utilizados.....	174
Tabla 33: Recursos Humanos	175
Tabla 34: Resumen de Costos	175
Tabla 35. Flujo de Caja	175
Tabla 36. Tasa de referencia.....	175
Tabla 37. Valor Actual Neto	176
Tabla 38. Evaluación Económica	176

CAPITULO I: Datos Generales de la Organización

CAPITULO I: Datos Generales de la Organización

1.1. Descripción de la Organización

Número de RUC: 20163138400 - FAMIDENT S.A.C.
Nombre Comercial: CLÍNICA MILLENIUM
Domicilio: JR. DANIEL ALCIDES CARRION NRO. 151
LAMBAYEQUE – CHICLAYO

1.2. Misión, Visión y Objetivos de la Organización

1.2.1. Misión

Somos la institución privada líder que ofrece servicios de salud integral, con personal especializado altamente competitivo, empleando nuestra moderna infraestructura provista de equipos y tecnología de avanzada. Garantizamos la satisfacción de nuestros usuarios, brindando atención personalizada y de calidad.

1.2.2. Visión

Constituirnos en la institución privada de salud líder del norte del Perú.

1.2.3. Objetivos

Expansión: Con el objetivo de atender mejor a nuestros pacientes y sus familias, tenemos definido un plan de crecimiento a nivel nacional, el cual atenderá las necesidades de un sin número de peruanos.

Eficiencia: Somos conscientes de que debemos cuidar los recursos de nuestra organización, por ello, tenemos definido un modelo de gestión por procesos que hará sostenible la continuidad de nuestra actividad.

Equipo: Somos personas que trabajamos en equipo, convencidos de que nuestro trabajo salva vidas. Juntos construimos día a día un gran lugar para trabajar.

1.3. Estructura Orgánica

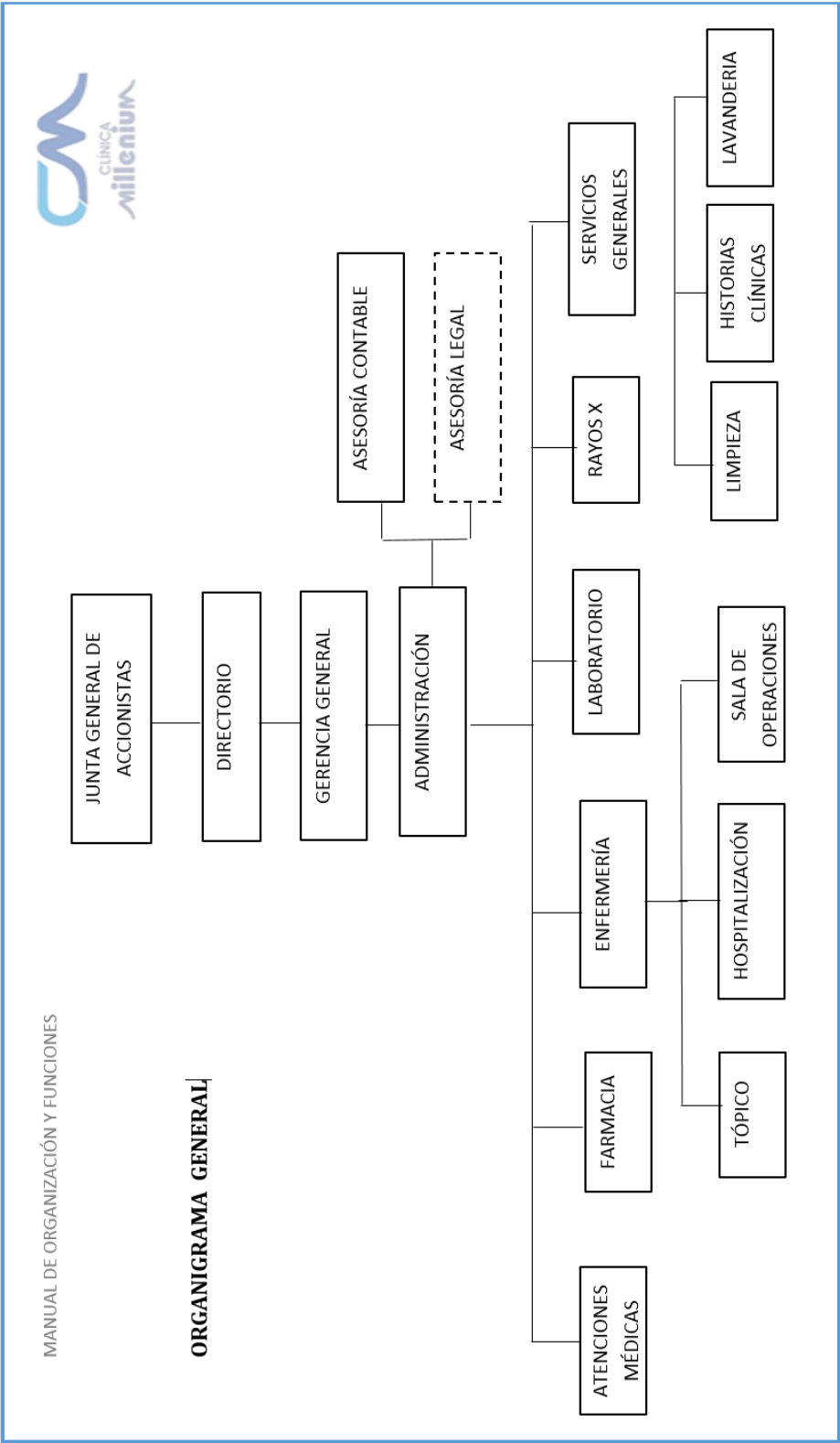


Ilustración 1: Organigrama de la Clínica (Millenium, 2016)

CAPITULO II: Problemática de la Investigación

CAPITULO II: Problemática de la Investigación

2.1. Realidad Problemática

2.1.1. Planteamiento del Problema

Las redes de telecomunicaciones en el sector salud han contribuido en ofrecer una mejor calidad de servicio a los pacientes, disminuyendo considerablemente el tiempo de espera, dando paso a la telemedicina la cual generó la disponibilidad de atención en localizaciones que antes era casi imposible lograr.

Así mismo, al proporcionar tantos beneficios interconectando toda la estructura de una entidad Hospitalaria, se toma a consideración la seguridad en la transferencia de datos de dichas entidades pues esta contiene información privada y esencial para la mejora y el bienestar de quienes son atendidos.

Las Redes Cableadas proporcionan a los usuarios una buena seguridad y la capacidad de mover muchos datos de manera rápida y efectiva, este tipo de conexión trabaja a altas tasas de velocidad y en el proceso de transferencia de datos la velocidad se mantiene, no depende de agentes externos.

Adicionalmente, las redes inalámbricas Wi-Fi se están convirtiendo en el soporte de la movilidad en los entornos hospitalarios, y su despliegue está creciendo a una tasa exponencial. Estas redes no sólo están dando soporte al despliegue en movilidad de sistemas de voz o de la Historia Clínica Electrónica, sino que también están dando soporte a los cientos de dispositivos y aplicaciones médicas móviles, como los sistemas de monitorización de pacientes o de administración de medicamentos. Además, y como ocurre en cualquier otro entorno, las redes WLAN de los hospitales se están viendo saturadas por el uso de portátiles y Tablets para registrar y consultar datos de pacientes, además de los dispositivos personales que empleados y visitas utilizan de forma asidua.

El uso no controlado de estos dispositivos, no sólo por parte de personal facultativo, sino por el público en general, puede poner en peligro tanto la privacidad de la información de los pacientes como la disponibilidad de la propia red para dar servicio en condiciones adecuadas, al sobrepasar la capacidad de dicha red y de los recursos de TI.

El sector de telecomunicaciones en el Perú se encuentra en un proceso de cambio. La rápida expansión de la telefonía móvil, la transición digital, el impulso del gobierno electrónico y la decisión política de universalizar el acceso a servicios de banda ancha, dando oportunidad de crecimiento para la ampliación del acceso a internet. Sin embargo, son pocas las empresas que, a pesar de tener implementado una red de telecomunicaciones moderna, pueda usarse a cabalidad debido a la falencia de seguridad en las redes inalámbricas.

La Clínica Millenium, es una de las instituciones de mayor importancia en la Región Lambayeque, está ubicado en Jr. Daniel A. Carrión N° 151- Chiclayo. Brinda los servicios de atención ambulatoria, hospitalización, cirugía mayor y menor, farmacia y ayuda diagnóstica en laboratorio.

Dentro de su estructura organizativa cuenta con el área de TI, la cual proporciona soporte a los principales servicios y proceso de negocio de la clínica.

La infraestructura tecnológica de la institución está dividida en servicios de telefonía analógica, red de datos a través de red cableada e inalámbrica (sólo algunas áreas específicas) brindando soporte y comunicación a los usuarios.

Ante las exigencias del mundo moderno actual de fortalecer la seguridad y optimizar la velocidad de transferencia de los datos, se debe hacer uso de las tecnologías de información lo que nos conlleva a administrar de manera efectiva los recursos. En tal sentido, se realizó una investigación sobre el estado de la red actual de la institución utilizando la observación como instrumento de recolección de datos, se obtiene el siguiente esquema de red:

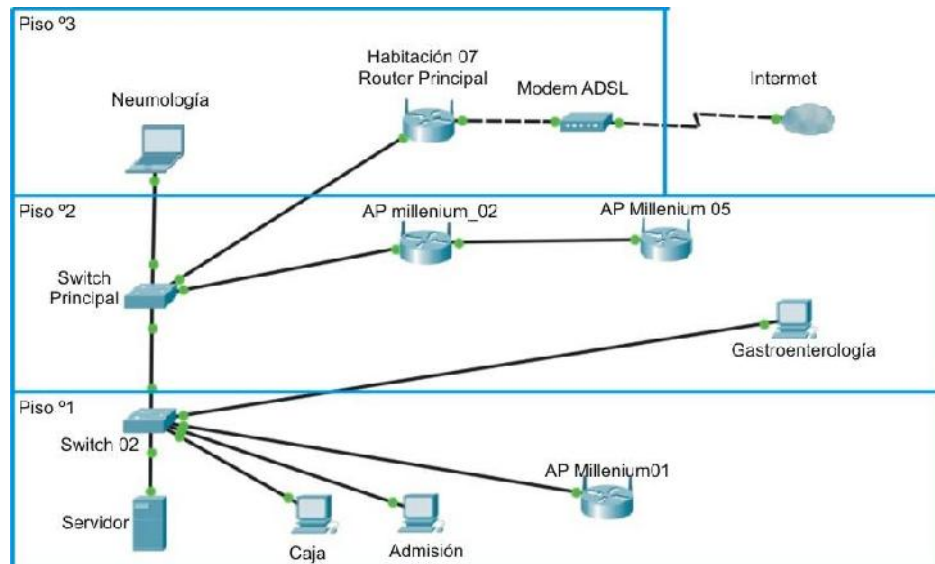


Ilustración 2: Esquema de la Red Actual de la Clínica Millenium

Según lo mostrado en la ilustración 2, entre los principales inconvenientes está la estructura de red inadecuada, El router principal actualmente se localiza en una habitación donde ingresan clientes internos y externos de la Clínica, el switch principal se encuentra en un área donde Médicos atienden según sus agendas correspondientes. A partir del esquema podemos concluir que: Hay una interconexión entre las áreas que no es la más idónea pues se aprecia que el Router principal se encuentra en un área dónde ingresa personal no autorizado y aumenta el riesgo de alguna manipulación y pérdida de información de la Clínica, robo del dispositivo físico, ocasionando pérdida de la conexión a internet, fallos en la red y desconexión de la misma.

Ilustración 3: Análisis de la red inalámbrica – Clínica Millenium utilizando la herramienta Acrylic Wifi Professional

Según lo mostrado en la ilustración 3, y haciendo una comparativa con la encuesta N° 02, podemos notar una falencia en la seguridad a nivel de control de acceso a la red interna y al internet pues en la encuesta se afirma una cantidad menor a los resultados del análisis de red inalámbrica realizados.

Se realizó un análisis general de la situación actual de la red de la Clínica y se detectó lo siguiente:

- Las instalaciones de red cableada no están correctamente estructuradas.
- No cuentan con etiquetado de red, no se tiene noción del esquema de la red cableada actual, por ende, no se identifica en que parte de la red se origina un problema.
- El router principal que provee de internet se encuentra en un área indebida.
- Se realizaron varios empalmes de cableado de red, ocasionando pérdida en la transferencia de datos y caídas de la conexión de red.
- La red inalámbrica sólo provee internet a algunas áreas, pues su localización dentro de la Clínica es incorrecta.
- Cuentan con un sistema de Facturación y control para particulares y convenios, el cual debe estar activo 24x7x365. La caída de este sistema por al menos una hora, genera pérdidas y congelamiento en los procesos dentro de la clínica, alterando el curso de las consultas y transacciones.
- No hay control al acceso de red inalámbrica. Esto genera un uso adicional ocasionando mayor tráfico de red. No se está administrando el acceso, se desconoce que usuarios no autorizados tienen acceso y con qué finalidad han ingresado a la red.

Actualmente esta área no tiene una adecuada gestión referente al uso de la red de telecomunicaciones que posee, este decir, la LAN, WLAN y WAN que da acceso a internet, sin embargo la WLAN está siendo usada con la configuración básica que viene por defecto de fábrica.

Esta situación ocasiona:

- No hay una correcta administración y control del ancho de banda de la WLAN, ocasionando colapsos en el sistema debido al gran tráfico de red.
- Carencia de seguridad para evitar los posibles ataques de acceso a la misma por consecuencia se puede ingresar al servicio de internet de manera no autorizada, debido que cualquier persona que obtenga la contraseña de la WLAN pueda entrar a dicha red, los usuarios propios y ajenos al hospital puedan ingresar sin ningún tipo de control de acceso y esto hace vulnerable a la red del hospital.

Todo esto indica que es posible realizar un estudio respecto a esta situación utilizando lo que nos ofrecen actualmente las nuevas tecnologías, a través del análisis y el diseño, para así ayudar a la solución de estos problemas que afronta dicha institución.

Por esta razón, la hipótesis establecida para la presente investigación propuso el diseño de un sistema de seguridad de red basado en la integración de los servidores RADIUS - LDAP en Linux permitirá fortalecer el acceso de la red de la clínica Millenium Chiclayo.

2.2. Formulación del Problema

¿En qué medida el sistema de seguridad basado en la integración de los servidores RADIUS - LDAP en Linux fortalecerá el acceso a la red de la Clínica Millenium Chiclayo?

2.3. Justificación e Importancia de la Investigación

El presente estudio se justifica debido a que busca reducir las vulnerabilidades de la red, así como mantener el control de acceso de los usuarios a dicha red para evitar saturaciones que perjudiquen la correcta ejecución de las aplicaciones de la institución.

Actualmente no se usa adecuadamente la red cableada, tiene una administración ineficiente por tal motivo se plantea un nuevo diseño de red el cuál que sea escalable, de esta poder compartir grandes cantidades de información a través de distintos programas, base de datos, etc., evitando las saturaciones y caídas inesperadas de la red.

Con un nuevo y correcto diseño de red cableada se puede crear de manera óptima una red inalámbrica que extienda y mejore la red de trabajo.

Debido a lo antes descrito, se orientará a una arquitectura de red con infraestructura cableada e inalámbrica que permitirá la interconexión entre las áreas de la Clínica y que a su vez se realizará un diseño de la integración de los servidores RADIUS – LDAP, los cuales fortalecerán la seguridad de los datos que contiene esta red.

Una red inalámbrica que incluya sistemas médicos críticos exige el mismo nivel de disponibilidad que se espera de una red cableada. La red Wi-Fi hospitalaria debe ser un recurso robusto y totalmente fiable para su uso con las aplicaciones clínicas esenciales. Y hay que conseguir esto al tiempo que se ofrece a usuarios y personal del hospital conectividad de calidad y se mantienen controlados los costes de operación y de inversión en la red. Además, para poder manejar este creciente grado de complejidad, el departamento de sistemas tiene que disponer de visibilidad, seguridad y control sobre toda la red, dispositivos y usuarios críticos, desde el núcleo hasta el extremo, y hacerlo con el menor número de recursos posible.

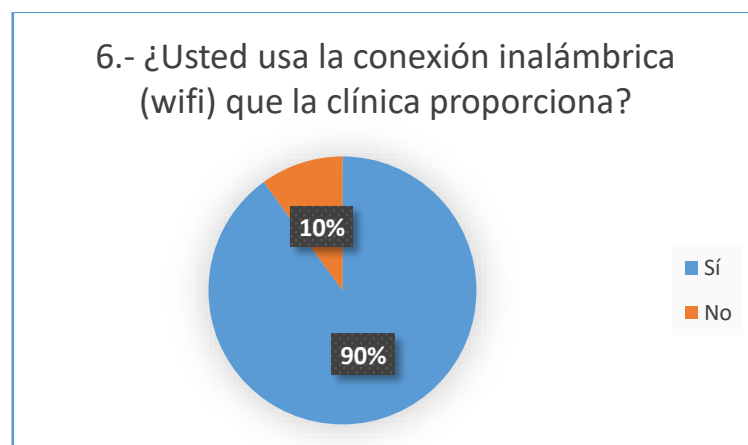


Ilustración 4. Resultado de encuesta 01.

2.3.1. Justificación Social

El personal administrativo y doctores tendrán mayor seguridad al notar que la red de la clínica les provee de un servicio de calidad por consecuencia ellos mejorarán su servicio.

2.3.2. Justificación Económica

Hoy en día las inversiones económicas a mediano y a largo plazo con el objetivo de permanecer en constante actualización sobre los avances tecnológicos y metodologías de encriptación es una inversión que se recupera y beneficia a la institución, pues incrementa la seguridad y agiliza los procesos dentro de una red.

2.3.3. Justificación Tecnológica

Todo ello exige una adaptación de la infraestructura de red y los sistemas de TI de los hospitales. Se requiere más que nunca una conectividad fiable y de alta disponibilidad, capaz de satisfacer las nuevas demandas en las condiciones de servicio adecuadas. Toda esta complejidad de gestión tiene su reflejo en los nuevos estándares en los que trabaja la industria, como el IEC 80001-1, que tienen por objeto gestionar los riesgos de TI en este tipo de entornos críticos. Este estándar en concreto pone los cimientos para que las organizaciones puedan desplegar una red unificada capaz de dar solución a estas nuevas necesidades de conectividad de equipos médicos al tiempo que proporciona un estándar de interoperabilidad para la seguridad de la información médica sensible.

En definitiva, la red está jugando un papel cada vez más protagonista en los entornos hospitalarios, ya es el soporte de gran parte de las nuevas necesidades de servicios de TI, sobre todo la parte inalámbrica por la demanda creciente de movilidad. Y tiene que ser capaz de afrontar este reto al tiempo que garantiza la seguridad y confidencialidad de la información de los pacientes y la capacidad operativa de la clínica.

2.4. Objetivos de la Investigación

2.4.1. Objetivo General

“Diseñar un sistema de seguridad de red basado en la integración de los servidores RADIUS - LDAP en Linux para fortalecer el acceso de la red de la clínica Millenium Chiclayo”

2.4.2. Objetivos Específicos

- Analizar la situación actual de la infraestructura tecnológica de la Clínica Millenium Chiclayo.
- Identificar las vulnerabilidades de seguridad en la red de la Clínica Millenium Chiclayo
- Diseñar un esquema de red de la Clínica Millenium mediante la metodología CISCO.
- Crear usuarios y políticas de control de acceso a la red.
- Simular la instalación e integración de los servidores RADIUS y LDAP.

2.5. Limitaciones de la Investigación

El desarrollo del proyecto de tesis tuvo limitaciones en accesos a los sistemas informáticos que manejan pues consideran que es de uso privado.

CAPITULO III: Marco Metodológico

CAPITULO III: Marco Metodológico

3.1. Tipo de Investigación

Auditoría y Seguridad Informática

3.2. Hipótesis

El diseño de un sistema de seguridad de red basado en la integración de los servidores RADIUS - LDAP en Linux permitirá fortalecer el acceso de la red de la clínica Millenium Chiclayo

3.3. Variables

		Definición	Dimensiones
Variable independiente	Diseño de un sistema de seguridad de red	Un Sistema de seguridad basada en la integración de los servidores RADIUS – LDAP en Linux Ubuntu sirve de herramienta para controlar el acceso que se da mediante la autenticación de usuarios a la red LAN y WLAN, administrarlos y otorgarles permisos para un mejor rendimiento de la red la red inalámbrica.	-Reestructuración de la red
Variable dependiente	Nivel de acceso a la red	Fortalecer el nivel de acceso y reducción de vulnerabilidades, se consigue mediante la autenticación de usuarios y a su vez restringiendo y otorgando permisos a estos.	- Organización - Control

Tabla 1. Variables Operacionales

CAPITULO IV: Marco Teórico

CAPITULO IV: Marco Teórico

4.1. Antecedentes

4.1.1. Antecedentes en el contexto internacional

Antecedente 1:

Tesis: “IMPLEMENTACIÓN DE UN PROTOTIPO DE RED INALÁMBRICA QUE PERMITA ELEVAR LOS NIVELES DE SEGURIDAD A TRAVÉS DE LA AUTENTICACIÓN DE UN SERVIDOR RADIUS PARA LOS USUARIOS QUE ACCEDAN A INTERNET EN EL EDIFICIO FRANCISCO MORAZÁN DE LA UTEC” (San Salvador – El Salvador, 2012)

Conclusión:

El proyecto presentado se ha dedicado a la implementación de un servidor RADIUS que permite la validación y autenticación de usuarios para el mejoramiento de la seguridad de la red inalámbrica del edificio Francisco Morazán de la UTEC.

El aplicar políticas de seguridad no es tarea sencilla; sin embargo, actualmente, se cuenta con herramientas que ayudan a la realización de tan importante tarea, Esta tesis es un ejemplo de ellos.

Antecedente 2:

Tesis: “MODELO DE SEGURIDAD, PARA UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)” (Mexico DF - Mexico, 2013)

Conclusión:

El modelo de seguridad en apoyo a la estructura del Centro de Operaciones de Seguridad contribuye en la administración de la seguridad en forma eficiente, al dotar de los diferentes controles de seguridad que se encuentran dispersos en la red y que alimentan los repositorios de registros e información que utiliza el SOC para la toma de decisiones en la detección y reacción de incidentes.

La restricción en el uso de los activos que se ubican en el SOC mediante el empleo del mecanismo de control de acceso basado en AAA, cumplimenta los objetivos del SOC al resguardar la información de seguridad altamente sensible y de valor para algún atacante.

Antecedente 3:

Tesis: “SEGURIDAD EN REDES INALÁMBRICAS USANDO HERRAMIENTAS DE SOFTWARE LIBRE” (Veracruz - Mexico, 2012)

Conclusión:

Este trabajo demuestra la gran importancia que hoy en día son las redes inalámbricas de área local ya sea para empresas grandes, pequeñas o de uso personal, proporcionando cada una de sus ventajas; movilidad, escalabilidad, fácil instalación y costo bajo facilitando conectividad en áreas de distancia corta y proporcionando la facilidad de trabajo sin tener que estar conectado bajo un cable. Considerando la gran ventaja que presta una red inalámbrica de área local, también se consideran desventajas en cuanto a la seguridad de la misma. Un factor muy importante por el cual surge la problemática de seguridad, es por la gran cantidad de demanda que hoy en día presenta esta tecnología.

Antecedente 4:

Tesis: “IMPLEMENTACIÓN DE UN CLIENTE RADIUS EN LINUX” (Quito - Ecuador, 2012)

Conclusión:

El sistema planteado reúne los requisitos de ser un sistema de uso simple.

Desde el punto de vista del usuario, pero reúne la complejidad suficiente dentro de sus procesos internos, para ser una solución lo suficientemente segura. Todos los procesos adicionales que se realizarán dentro del sistema de seguridad, son totalmente transparentes para el usuario, es decir el usuario no se percatará que dentro del sistema se realizan verificaciones adicionales de seguridad.

4.1.2. Nacionales

Antecedente 1:

Tesis: “DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN Y WLAN CONSISTENTE DE CONTROL DE ACCESO MEDIANTE SERVIDORES AAA” (Lima - Perú, 2012)

Conclusión:

Afirma que, se comprobó que los protocolos AAA RADIUS Y TACACS+ tienen diferentes características en el manejo de autenticación y autorización. El protocolo RADIUS maneja ambos servicios de manera combinada, mientras que el protocolo TACACS+ los ofrece como servicios independientes. A pesar de ello fueron implementados en una misma red y coexisten para brindar una red con sistema de control de acceso robusto. Así mismo al culminar con la implementación del presente proyecto se pudo concluir que gracias al servidor RADIUS, un usuario inalámbrico puede autenticarse e ingresar a la red; asimismo, el servidor TACACS+, teniendo como base el nivel de privilegio del, usuario, permite a este ingresar o no a los equipos de red para realizar configuraciones en los equipos.

4.2. Base Teórica

4.2.1. Autenticación

“Ya sabemos que unos requerimientos primordiales de los sistemas informáticos que desempeñan tareas importantes son los mecanismos de seguridad adecuados a la información a la información que se intenta proteger; el conjunto de tales mecanismos ha de incluir al menos un sistema que permita identificar a las entidades (elementos pasivos, como ficheros o capacidad de cómputo), mediante procesos tan simples como una contraseña o tan complejos como un dispositivo analizador de patrones retinales.

Los sistemas que habitualmente utilizamos los humanos para identificar a una persona, como el aspecto físico o la forma de hablar, son demasiado complejos para una computadora; el objetivo de los sistemas de identificación de usuarios no suele ser **identificar** a una persona, sino **autenticar** que esa persona es quien dice ser realmente. Aunque como humanos seguramente ambos términos nos parecerán equivalentes, para un ordenador existe una gran diferencia entre ellos; imaginemos una potencia sistema de identificación estrictamente hablando, por ejemplo, uno biométrico basado en el reconocimiento de la retina; una persona miraría a través del dispositivo lector, y el sistema sería capaz de decidir si es un usuario válido, y en ese caso decir de quién se trata; esto es identificación. Sin embargo, lo que habitualmente hace el usuario es introducir su identidad (un número, un nombre de usuario...) además de mostrar sus retinas ante el lector; el sistema en este caso no tiene que identificar a esa persona, sino autenticarlo: comprobar los parámetros de la retina que está leyendo con los guardados en una base de datos para el usuario que la persona dice ser: estamos reduciendo el problema de una población potencialmente muy elevada a un grupo de usuarios más reducido, el grupo de usuarios del sistema que necesita autenticarlos.

Los métodos de autenticación se suelen dividir en tres categorías, en función de lo que utilizan para la verificación de identidad: (a) algo que el usuario sabe, (b) algo que éste posee, y (c) una característica física del usuario o un acto involuntario del mismo. Esta de cada uno de estos tipos de autenticación: un password (Unix) o passphrase (PGP) es algo que el usuario conoce y el resto de personas no, una tarjeta de identidad es algo que el usuario lleva consigo, la huella dactilar es una característica física del usuario, y un acto involuntario podría considerarse que se produce al firmar (al rubricar la firma no se piensa en el diseño de cada trazo individualmente). Por supuesto, un sistema de autenticación puede (y debe, para incrementar su fiabilidad) combinar mecanismos de diferente tipo, como en el caso de una tarjeta de crédito junto al PIN a la hora de utilizar un cajero automático

o en el de un dispositivo generador de claves para el uso de One Time Passwords.

Cualquier sistema de identificación (aunque les llamemos así, recordemos que realmente son sistemas de autenticación) ha de poseer unas determinadas características para ser viable; obviamente, ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo de 10^{-4} en los sistemas seguros), económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto) y ha de soportar con éxito cierto tipo de ataques (por ejemplo, imaginemos que cualquier usuario puede descifrar el password utilizado en el sistema de autenticación de Unix en tiempo polinomial; esto sería inaceptable). Aparte de estas características tenemos otra, no técnica sino humana, pero quizás la más importante: un sistema de autenticación ha de ser aceptable para los usuarios, que serán al fin y al cabo los recursos de la Universidad, consistente en un dispositivo que fuera capaz de realizar un análisis de sangre a un usuario, y así comprobar que es quien dice ser; seguramente sería barata y altamente fiable, pero nadie aceptaría dar un poco de sangre cada vez que desee consultar su correo

a. Sistemas basados en algo conocido: contraseñas

El modelo de autenticación más básico consiste en decidir si un usuario es quien dice ser simplemente basándonos en una prueba de conocimiento que a priori sólo ese usuario puede superar; y desde Alí Babá y su “Ábrete, Sésamo” hasta los más modernos sistemas Unix, esa prueba de conocimiento no es más que una contraseña que en principio es secreta. Evidentemente, esa aproximación es la más vulnerable a todo tipo de ataque, pero también la más barata, por lo que se convierte en la técnica más utilizada en entornos que no precisan de una alta seguridad, como es el caso de los sistemas Unix en redes normales (y en general en todos los sistemas operativos en redes de seguridad media – baja); otros entornos en los que se suele aplicar este modelo de autenticación son las aplicaciones que requieren de alguna identificación de usuarios, como el software de cifrado PGP o el escáner de seguridad NESSUS. También se utiliza como

complemento a otros mecanismos de autenticación, por ejemplo, en el caso del Número de Identificación Personal (PIN) a la hora de utilizar cajeros automáticos.

En todos los esquemas de autenticación basados en contraseñas se cumple el mismo protocolo: las entidades (generalmente dos) que participan en la autenticación acuerdan una clave, clave que han de mantener en secreto si desean que la autenticación sea fiable. Cuando una de las partes desea autenticarse ante otra se limita a mostrarle su conocimiento de esa clave común, y si ésta es correcta se otorga el acceso a un recurso. Lo habitual es que existan unos roles preestablecidos con una entidad activa que desea autenticarse y otra pasiva que admite o rechaza a la anterior (en el modelo del acceso a sistemas Unix, tenemos al usuario y al sistema que le permite o niega la entrada).

Como hemos dicho, este esquema es muy frágil: basta con que una de las partes no mantenga la contraseña en secreto para que toda la seguridad del modelo se pierda; por ejemplo, si el usuario de una máquina Unix comparte su clave con un tercero, o si ese tercero consigue leerla y rompe su cifrado (por ejemplo, como veremos luego, mediante un ataque de diccionario), automáticamente esa persona puede autenticarse ante el sistema con éxito con la identidad de un usuario que no le corresponde.” (Villalón Huerta, 2012)

b. Autenticación Clásica

“En el sistema Unix Habitual cada usuario posee un nombre de entrada al sistema o *login* y una clave o *password*; ambos datos se almacenan generalmente en el fichero `/etc/passwd`. Este archivo contiene una línea por usuario (aunque hay entradas que no corresponden a usuarios reales, como veremos a continuación) donde se indica la información necesaria para que los usuarios puedan conectar al sistema y trabajar en él, separando los diferentes campos mediante ‘;’. Por ejemplo, podemos encontrar entradas parecidas a la siguiente:

```
Toni:LEgPN8jqSCHCg:1000:100:Antonio  
Villalon,,,:/export/home/toni:/bin/sh
```

En primer lugar, aparecen el *login* del usuario y su clave cifrada; a continuación, tenemos dos números que serán el identificador de usuario y el de grupo respectivamente. El quinto campo, denominado GECOS es simplemente información administrativa sobre la identidad real del usuario, como su nombre, teléfono o número de despacho. Finalmente, los dos últimos campos corresponden al directorio del usuario (su \$HOME inicial) y al Shell que le ha sido asignado.

Al contrario de lo que mucha gente cree, Unix no es capaz de distinguir a sus usuarios por su nombre de entrada al sistema. Para el sistema operativo lo que realmente distingue a una persona de otra (o al menos a un usuario de otro) es el UID del usuario en cuestión; el *login* es algo que se utiliza principalmente para comodidad de las personas (obviamente es más fácil acordarse de un nombre de entrada como *toni* que de un UID como 2643, sobre todo si se tienen cuentas en varias máquinas, cada una con un UID diferente). Por tanto, si en `/etc/passwd` existen dos entradas con un mismo UID, para Unix se tratará del mismo usuario, aunque tengan un *login* y un *password* diferente: así, si dos usuarios tienen asignado el UID 0, ambos tendrán privilegios de superusuario, sin importar el *login* que utilicen. Esto es especialmente aprovechado por atacantes que han conseguido privilegios de administrador en una máquina: pueden añadir una línea a `/etc/passwd` mezclada entre todas las demás, con su nombre de usuario normal, pero con el UID 0; así garantizan su entrada al sistema como administradores en caso de ser descubiertos, por ejemplo, para borrar huellas. Como a simple vista puede resultar difícil localizar la línea insertada especialmente en sistemas con un gran número de usuarios, para detectar las cuentas con privilegio en la máquina podemos utilizar la siguiente orden:

```
Anita:~# awk -F: '$3==0 {print $1}' /etc/passwd
root
anita:~#
```

En el fichero de claves van a existir entradas que no corresponden a usuarios reales, sino que son utilizadas por ciertos programas o se trata de cuentas mantenidas por motivos de compatibilidad con otros sistemas; típicos

ejemplos de este tipo de entradas son *1p*, *uucp* o *postmaster*. Estas cuentas han de estar bloqueadas en la mayoría de casos, para evitar que alguien pueda utilizarlas para acceder a nuestro sistema: sólo han de ser accesibles para el *root* mediante la orden *su*. Aunque en su mayoría cumplen esta condición, en algunos sistemas estas cuentas tienen claves por defecto o, peor, no tienen claves, lo que las convierte en una puerta completamente abierta a los intrusos; es conveniente que, una vez instalado el sistema operativo, y antes de poner a trabajar la máquina, comprobemos que están bloqueadas, o que en su defecto que tienen claves no triviales. Algunos ejemplos de cuentas sobre lo que hay que prestar especial atención son *root*, *guest*, *1p*, *demos*, *4dGifts*, *tour*, *nuucp*, *games* o *postmaster*; es muy recomendable consultar los manuales de cada sistema concreto, y chequear periódicamente la existencia de cuentas sin clave o cuentas que deberían permanecer bloqueadas y no lo están.

Para cifrar las claves de acceso de sus usuarios, el sistema operativo Unix emplea un criptosistema irreversible que utiliza la función estándar de C *crypt* (3), basada en el algoritmo DES. Esta función toma como la clave de ocho primeros caracteres de la contraseña elegida por el usuario (si la longitud de ésta es menor, se completa con ceros) para cifrar un bloque de texto en claro de 64 bits puestos a cero; para evitar que dos *Passwords* iguales resulten en un mismo texto aleatoria para cada usuario, basada en un campo formado por un número de 12 bits (con lo que conseguimos 4096 permutaciones diferentes) llamado *salt*. El cifrado resultante se vuelve a cifrar utilizando la contraseña del usuario de nuevo como clave, y permutando con el mismo *salt*, repitiéndose el proceso 25 veces. El bloque cifrado final, de 64 bits, se concatena con dos bits de ruido, obteniendo 66 bits que se hacen representables en 11 caracteres de 6 bits cada uno y que, junto con el *salt*, pasan a constituir el campo *password* del fichero de contraseñas, usualmente */etc/passwd*. Así los dos primeros caracteres de este campo estarán constituidos por el *salt* y los 11 restantes por la contraseña cifrada:

Toni:LEgPN8jqSCHCg:1000:100:Antonio
Villalon,,,:/export/home/toni:/bin/sh

SALT: LE

PASSWORD CIFRADO: Gpn8JSCHCg

Como hemos dicho antes, este criptosistema es irreversible. Entonces, ¿cómo puede un usuario conectarse a una máquina Unix? El proceso es sencillo: el usuario introduce su contraseña, que se utiliza como clave para cifrar 64 bits a 0 basándose en el *salt*, leído en */etc/passwd*, de dicho usuario. Si tras aplicar el algoritmo de cifrado el resultado se corresponde con lo almacenado en los últimos 11 caracteres del campo *password* del fichero de contraseñas, la clave del usuario se considera válida y se permite el acceso. En caso contrario se le deniega y se almacena en un fichero el intento de conexión fallido.

c. Mejora de la seguridad

Problemas del modelo clásico

Los ataques de texto cifrado escogido constituyen la principal amenaza al sistema de autenticación Unix; a diferencia de lo que mucha gente no cree, no es posible descifrar una contraseña, pero es muy fácil cifrar una palabra junto a un determinado *salt*, y comparar el resultado de la cadena almacenada en el fichero de claves. De esta forma, un atacante leerá el fichero */etc/passwd* (este fichero ha de tener permiso de lectura para todos los usuarios si queremos que el sistema funcione correctamente), y mediante un programa adivinador (o *crackeador*) como Crack o John the Ripper cifrará todas las palabras de cualquier idioma o campo de la sociedad – historia clásica, deporte, cantantes de rock...), comparando el resultado obtenido en este proceso con la clave cifrada del fichero de contraseñas; si ambos coinciden, ya ha obtenido una clave para acceder al sistema de forma no autorizada. Este proceso se puede, pero no se suele hacer en la máquina local, ya que en este caso hay bastantes posibilidades de detectar el ataque: desde modificar el ataque en código de la función *crypt* (3) para que alerte al administrador cuando es invocada repetidamente (cada vez que el adivinador cifra una palabra utiliza esa función) hasta simplemente darse

cuenta de una carga de CPU excesiva (los programas adivinadores suelen consumir un tiempo de procesador considerable). Lo habitual es que el atacante transfiera una copia de archivo a otro ordenador y realice el proceso en esta otra máquina; ni siquiera se tiene que tratar de un servidor Unix con capacidad de cómputo: existen muchos programas adivinadores que se ejecutan en un PC normal, bajo MS – DOS o Windows. Obviamente, este segundo es mucho más difícil de detectar, ya que se necesita una auditoría de los programas que ejecuta el usuario (y utilidades como cp o ftp no suelen llamar la atención del administrador). Esta auditoría la ofrecen muchos sistemas Unix (generalmente en los ficheros de *log* /var/adm/pacct o /var/adm/acct), pero no se suele utilizar por los excesivos recursos que puede consumir, incluso en sistema pequeños; obviamente, no debemos fiarnos nunca de los archivos históricos de órdenes del usuario (como \$HOME/.sh_history o \$HOME/.bash_history), ya que el atacante los puede modificar para ocultar sus actividades, sin necesidad de ningún privilegio especial.

Contraseñas aceptables

La principal forma de evitar este tipo de ataque es utilizar *Passwords* que no sean palabras de los ficheros *diccionario* típicos: combinaciones de minúsculas y mayúsculas, números mezclados con texto, símbolos como &, \$ o %, etc. Por supuesto, hemos de huir de claves simples como *internet* o *Beatles*, nombres propios, combinaciones débiles como *Pepito1* o *qwerty*, nombres de lugares, actores, personajes de libros, deportistas... Se han realizado numerosos estudios sobre cómo evitar este tipo de *Passwords* en los usuarios, y también se han diseñado potentes herramientas para lograrlo, como Npasswd o Passwd+. Es bastante recomendable instalar alguna de ellas para ‘obligar’ a los usuarios utilizar contraseñas aceptables (muchos Unices ya las traen incorporadas), pero no conviene confiar toda la seguridad en nuestro sistema a estos programas. Como norma, cualquier administrador deberá ejecutar con cierta periodicidad algún programa adivinador, tipo *Crack*, para comprobar sus usuarios no han elegidos contraseñas débiles (a pesar del uso de Npasswd o Passwd+): se puede

tratar de claves generadas antes de instalar estas utilidades o incluso de claves asignadas por el propio *root* que no han pasado por el control de estos programas.

Por último, es necesario recordar que para que una contraseña sea aceptable, obligatoriamente ha de cumplir el principio **KISS**, que hablando de *password* está claro que no puede significar '*Keep it simple, Stupid!*' sino '**Keep it SECRET, stupid!**'. La contraseña más larga, la más difícil de recordar, la que combina más caracteres no alfabéticos... pierde toda su robustez si su propietario la comparte con otras personas.

Shadow Password

Otro método cada día más utilizado para proteger contraseñas de los usuarios del denominado *Shadow Password* u oscurecimiento de contraseñas. La idea básica de este mecanismo es impedir que los usuarios sin privilegios puedan leer el fichero donde se almacenan las claves cifradas; en el punto anterior hemos comentado que el fichero sigue siendo legible para todos los usuarios, pero a diferencia del mecanismo tradicional, las claves cifradas no se guardan en él, sino en el archivo `/etc/shadow`, que sólo el *root* puede leer. En el campo correspondiente a la clave cifrada de `/etc/shadow` no aparece esta sino un símbolo que indica a determinados programas (como `/bin/login`) que han de buscar claves en `/etc/shadow`, generalmente una `x`:

```
toni:x:1000:100:Antonio Villalon,,,:/export/home/toni:/bin/sh
```

El aspecto de `/etc/shadow` es en cierta forma similar al de `/etc/passwd` que ya hemos comentado: existe una línea por cada usuario del sistema, en la que se almacena su *login* y su clave cifrada. Sin embargo, el resto de campos de este fichero son diferentes; corresponden a información que permite implementar otro mecanismo para proteger las claves de los usuarios, el envejecimiento de contraseñas o *Agning Password*, del que hablaremos a continuación:

```
Toni:LEgPN8jqSCHCg:10322:0:99999:7:::
```

Desde hace un par de años, la gran mayoría de Unices del mercador incorporan este mecanismo; si al instalar el sistema operativo las claves aparecen almacenadas en `/etc/passwd` podemos comprobar si existe la orden **pwconv**, que convierte un sistema clásico a uno oscurecido. Si no es así, o si utilizamos un Unix antiguo que no posee el mecanismo de *Shadow Password*, es muy conveniente que consigamos el paquete que lo implementa (seguramente se tratará de un fichero `shadow.tar.gz` que podemos encontrar en multitud de servidores, adecuado a nuestro clon de Unix) y lo instalemos en el equipo. Permitir que todos los usuarios lean las claves cifradas ha representado durante años, y sigue representando, uno de los mayores problemas de seguridad de Unix; además unas de las actividades preferidas de piratas novatos es intercambiar ficheros de claves de los sistemas a los que acceden y *crackearlos*, con los que es suficiente una persona que lea nuestro fichero para tener en poco tiempo una colonia de intrusos en nuestro sistema.” (Villalón Huerta, 2012)

4.2.2. Autorización

“Hasta ahora hemos gestionado el acceso de los usuarios a nuestro router o red, esto sería la primera “A” (Authentication) de AAA, el ¿Quién accede? Ahora vamos a empezar con la segunda “A” (Authorization), que se centra en los privilegios de esos usuarios que se conectan a dicha red o router. La metodología de funcionamiento es similar, se crean listas, esta vez de autorización, y se especifica el tipo de autorización y el método, es el comando que usamos para crear una lista de autorización. Dentro de los posibles tipos de autorización podemos elegir entre *console*, *exec* y *network*. El tipo *console* lo usamos para activar los privilegios de los usuarios que se conectan mediante la consola. Estos privilegios, de los que hasta ahora estoy hablando, son relativos al control el router mediante su línea de comandos. Por último, el tipo *network* se usa para activar esos privilegios de usuario que se conectan a la red, normalmente median PPP u otros métodos. Teniendo la lista de autenticación configurada, nuestros clientes podían loguearse dentro de la red, o acceder al router siempre que su usuario estuviera dado de alta en la base de datos (local o RADIUS), pero si uno de esos usuarios

tenía privilegios de súper usuario, o necesitaba adquirir una dirección IP específica al conectarse a la red, no recibiría esos privilegios o aspectos especiales relativos a su usuario. Para que eso suceda necesitamos crear la lista de autorización que es como el router concede el uso de esos privilegios a esos usuarios que los poseen. Estos son unos ejemplos de lista de autorización:

- ***aaa authorization exec default group radius local:*** Lista de autorización que concederá privilegios a los usuarios que se conecten al Shell del router mediante una línea virtual (vty). Es la lista *default*, por lo tanto, se aplicará a todos aquellos interfaces que no formen parte de una lista de autorización específica. Primero se tratará de autorizar a esos usuarios mediante un servidor RADIUS y en caso de fallo se procederá usando la base de datos de usuarios local del router.
- ***aaa Authorization network default group radius local if-authenticated:*** Lista de autorización que concederá privilegios a los usuarios que se conecten a la red. Es la lista *default*, por lo tanto, se aplicará a todas aquellas conexiones que no formen parte de una lista de autorización específica. Primero se tratará de autorizar a esos usuarios mediante un servidor RADIUS y en caso de fallo se procederá usando la base de datos de usuarios local del router. Al final hemos añadido el parámetro *if-authenticated*, que hace que solo se proceda a la autorización si previamente el usuario ha sido autenticado
- ***aaa authorization network default group radius local if-authenticated:*** Lista de autorización que concederá privilegios a los usuarios que se conecten a la red. Es la lista *default*, por lo tanto, se aplicará a todas aquellas conexiones que no formen parte de la lista de autorización específica. Primero se tratará de autorizar a esos usuarios mediante un servidor RADIUS y en caso de fallo se procederá usando la base de datos de usuarios local del router. Al final hemos añadido el parámetro *if-authenticated*, que hace que solo

se proceda a la autorización si previamente el usuario ha sido autenticado.

4.2.3. Accounting

La última “A” significa Accounting, que consiste en llevar un registro sobre los recursos que consumen esos usuarios que acceden a la red, o que se conectan a la Shell del router, por ejemplo. Dentro de estos registros podemos ver a qué hora accedieron, cuanta información transmitieron, como se conectaron, etc...

Al igual que en la autenticación y en la autorización, en Accounting tenemos que crear unas listas que tienen la misma estructura, donde especificaremos el tipo, la lista a usar y el método por el cual se lleva a cabo la autorización. Esta es su estructura: *aaa Accounting [tipo_accounting] [lista_accounting] [tipo_registro] [método1] [método 2]*.

La única diferencia que podemos observar con respecto a las listas anteriores es que, en el caso de Accounting, tenemos un nuevo parámetro, el tipo de registro. El router tiene la posibilidad de crear un registro cuando un usuario inicia sesión en la red y/o cuando este cierra la sesión, en este parámetro *tipo_registro* podemos hacer que el router grabe ese registro con cada inicio y fin de sesión dándole el valor *Start-stop* o sólo cuando el usuario cierra la sesión. Para esto último el parámetro sería *stop-only*. Al igual que en los anteriores casos, si utilizamos la lista *default*, esta será aplicada automáticamente en todos los interfaces que no formen parte de la otra lista de Accounting. Estos son unos ejemplos de listas accounting:

aaa accounting exec default Start-stop group radius: Crea registros relativos al inicio de sesión en la shell del router cuando los usuarios inician y cierran la sesión. Estos registros se crean en un servidor RADIUS.

aaa accounting network default Start-stop group radius: Crea registros relativos a la conexión de usuarios a la red mediante PPP. Estos registros son creados con cada conexión y desconexión del usuario y son guardados en un servidor RADIUS.

aaa accounting resource default stop-only group radius: Crea un registro complete con el cierre de session de usuarios en la red.” (Marqués, 2016)

4.2.4. Modelo de referencia TCP/IP

“Pasemos ahora del modelo de referencia OSI al modelo de referencia que se utiliza en la más vieja de todas las redes de computadoras de área amplia: ARPANET y su sucesora, Internet. Aunque más adelante veremos una breve historia de ARPANET, es conveniente mencionar ahora unos cuantos aspectos de esta red. ARPANET era una red de investigación patrocinada por el DoD (Departamento de Defensa de Estados Unidos, del inglés U.S. Department of the Defense). En un momento dado llegó a conectar cientos de universidades e instalaciones gubernamentales mediante el uso de líneas telefónicas rentadas.

Cuando después se le unieron las redes de satélites y de radio, los protocolos existentes tuvieron problemas para interactuar con ellas, de modo que se necesitaba una nueva arquitectura de referencia. Así, casi desde el principio la habilidad de conectar varias redes sin problemas fue uno de los principales objetivos de diseño. Posteriormente esta arquitectura se dio a conocer como el Modelo de referencia TCP/IP,

Debido a sus dos protocolos primarios. Este modelo se definió por primera vez en Cerf y Kahn (1974); después se refinó y definió como estándar en la comunidad de Internet (Braden, 1989). Clark (1988) describe la filosofía de diseño detrás de este modelo. Debido a la preocupación del DoD de que alguno de sus valiosos hosts, enrutadores y puertas de enlace de inter redes pudieran ser volados en pedazos en cualquier momento por un ataque de la antigua Unión Soviética, otro de los objetivos principales fue que la red pudiera sobrevivir a la pérdida de hardware de la subred sin que se interrumpieran las conversaciones existentes. En otras palabras, el DoD quería que las conexiones permanecieran intactas mientras las máquinas de origen y de destino estuvieran funcionando, Incluso aunque algunas de las máquinas o líneas de transmisión en el trayecto dejaran de funcionar en forma repentina. Además, como se tenían en mente aplicaciones con

requerimientos divergentes que abarcaban desde la transferencia de archivos hasta la transmisión de voz en tiempo real, se necesitaba una arquitectura flexible.

a. La capa física

La capa física se relaciona con la transmisión de bits puros a través de un canal de transmisión. Los aspectos de diseño tienen que ver con la acción de asegurarse que cuando uno de los lados envíe un bit 1 el otro lado lo reciba como un bit 1, no como un bit 0. En este caso las preguntas típicas son: ¿qué señales eléctricas se deben usar para representar un 1 y un 0?, ¿cuántos nanosegundos dura un bit?, ¿la transmisión puede proceder de manera simultánea en ambas direcciones?, ¿cómo se establece la conexión inicial y cómo se interrumpe cuando ambos lados han terminado?, ¿cuántos pines tiene el conector de red y para qué sirve cada uno? Los aspectos de diseño tienen que ver con las interfaces mecánica, eléctrica y de temporización, así como con el medio de transmisión físico que se encuentra bajo la capa física.

b. La capa de enlace

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa sin conexión que opera a través de distintas redes. La capa más baja en este modelo es la capa de enlace; ésta describe qué enlaces (como las líneas seriales y Ethernet clásica) se deben llevar a cabo para cumplir con las necesidades de esta capa de interred sin conexión. En realidad, no es una capa en el sentido común del término, sino una interfaz entre los hosts y los enlaces de transmisión. El primer material sobre el modelo TCP/IP tiene poco que decir sobre ello.

c. La capa de interred

Esta capa es el eje que mantiene unida a toda la arquitectura. Su trabajo es permitir que los hosts inyecten paquetes en cualquier red y que viajen de manera independiente hacia el destino (que puede estar en una red distinta). Incluso pueden llegar en un orden totalmente diferente al orden en que se enviaron, en cuyo caso es responsabilidad de las capas más altas volver a ordenarlos, si se desea una entrega en orden. Tenga en cuenta que aquí utilizamos “interred” en un sentido genérico, aunque esta capa esté presente en la Internet.

La analogía aquí es con el sistema de correos convencional (lento). Una persona puede dejar una secuencia de cartas internacionales en un buzón en un país y, con un poco de suerte, la mayoría de ellas se entregarán a la dirección correcta en el país de destino. Es probable que las cartas pasen a través de una o más puertas de enlace de correo internacionales en su trayecto, pero esto es transparente a los usuarios. Además, los usuarios no necesitan saber que cada país (es decir, cada red) tiene sus propias estampillas, tamaños de sobre preferidos y reglas de entrega.

La capa de interred define un formato de paquete y un protocolo oficial llamado IP (Protocolo de Internet, del inglés Internet Protocol), además de un protocolo complementario llamado ICMP (Protocolo de Mensajes de Control de Internet, del inglés Internet Control Message Protocol) que le ayuda a funcionar. La tarea de la capa de interred es entregar los paquetes IP a donde se supone que deben ir.

Aquí el ruteo de los paquetes es sin duda el principal aspecto, al igual que la congestión (aunque el IP no ha demostrado ser efectivo para evitar la congestión).

d. La capa de transporte

Por lo general, a la capa que está arriba de la capa de interred en el modelo TCP/IP se le conoce como capa de transporte; y está diseñada para permitir que las entidades pares, en los nodos de origen y de destino, lleven a cabo una conversación, al igual que en la capa de transporte de OSI. Aquí se definieron dos protocolos de transporte de extremo a extremo. El primero, TCP (Protocolo de Control de la Transmisión, del inglés Transmission Control Protocol), es un protocolo confiable orientado a la conexión que permite que un flujo de bytes originado en una máquina se entregue sin errores a cualquier otra máquina en la interred. Este protocolo segmenta el flujo de bytes entrante en mensajes discretos y pasa cada uno a la capa de interred. En el destino, el proceso TCP receptor vuelve a ensamblar los mensajes recibidos para formar el flujo de salida. El TCP también maneja el control de flujo para asegurar que un emisor rápido no pueda inundar a un receptor lento con más mensajes de los que pueda manejar.

El segundo protocolo en esta capa, UDP (Protocolo de Datagrama de Usuario, del inglés User Datagram Protocol), es un protocolo sin conexión, no confiable para aplicaciones que no desean la asignación de secuencia o el control de flujo de TCP y prefieren proveerlos por su cuenta. También se utiliza mucho en las consultas de petición-respuesta de una sola ocasión del tipo cliente-servidor, y en las aplicaciones en las que es más importante una entrega oportuna que una entrega precisa, como en la transmisión de voz o video. En la figura 1 se muestra la relación entre IP, TCP y UDP. Desde que se desarrolló el modelo, el IP se ha implementado en muchas otras redes.

e. La capa de aplicación

El modelo TCP/IP no tiene capas de sesión o de presentación, ya que no se consideraron necesarias. Las aplicaciones simplemente incluyen cualquier función de sesión y de presentación que requieran. La experiencia con el modelo OSI ha demostrado que esta visión fue correcta: estas capas se

utilizan muy poco en la mayoría de las aplicaciones.

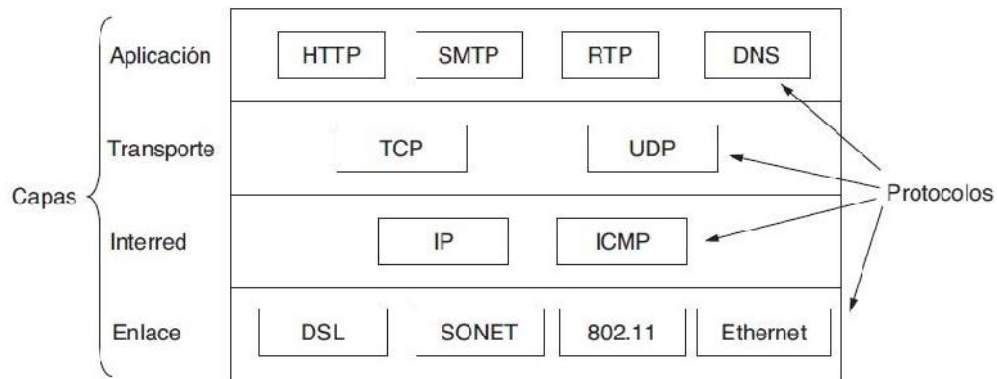


Ilustración 5: El modelo TCP/IP con algunos protocolos.

Encima de la capa de transporte se encuentra la capa de aplicación. Ésta contiene todos los protocolos de alto nivel. Entre los primeros protocolos están el de terminal virtual (TELNET), transferencia de archivos (FTP) y correo electrónico (SMTP). A través de los años se han agregado muchos otros protocolos. En la ilustración 4 se muestran algunos de los más importantes que veremos más adelante: el Sistema de nombres de dominio (DNS) para resolución de nombres de hosts a sus direcciones de red; HTTP, el protocolo para recuperar páginas de la World Wide Web; y RTP, el protocolo para transmitir medios en tiempo real, como voz o películas.” (Tanenbaum, 2012)

4.2.5. Seguridad en redes Inalámbricas

“La seguridad es una de las principales preocupaciones de las empresas que están interesadas en implementar redes inalámbricas. Afortunadamente, tanto el conocimiento de los usuarios sobre la seguridad como las soluciones ofrecidas por los proveedores de tecnología están mejorando. Las redes inalámbricas actuales incorporan funciones completas de seguridad, y cuando estas redes cuentan con una protección adecuada, las compañías pueden aprovechar con confianza las ventajas que ofrecen.

"Los proveedores están haciendo un gran trabajo para mejorar las funciones de seguridad, y los usuarios están obteniendo conocimiento de la seguridad inalámbrica", afirma Richard Web, analista de orientación para redes de área local inalámbricas (LAN) de Infonetics Research. "Sin embargo, las amenazas aún se consideran importantes, y los proveedores siempre necesitan tener en cuenta la percepción inamovible de que las redes LAN son inseguras".

De hecho, la seguridad es el principal obstáculo para la adopción de redes LAN inalámbricas. Y esta preocupación no es exclusiva de las compañías grandes. En lo que respecta a la conexión de redes inalámbricas, "la seguridad sigue siendo la preocupación nº 1 de las compañías de todos los tamaños", afirma Julie Ask, directora de investigaciones de Júpiter Research" (Seguridad en redes inalámbricas – Cisco 2015).

a. Encriptación y Autenticación

"La encriptación es una medida de seguridad utilizada al momento de almacenar y/o transmitir información sensible, para que ésta no pueda ser obtenida con facilidad por terceros, esta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación.

Algunos de los usos más comunes de la encriptación son la transmisión y almacenamiento de información sensible como contraseñas, números de tarjetas de crédito, números de identificación legal, reportes administrativo-contables y conversaciones privadas, entre otros.

La mayoría de los métodos de encriptación utilizan una clave como parámetro variable en las mencionadas fórmulas matemáticas de forma que a pesar de que un intruso las conozca, no le sea posible descifrar el criptograma si no conoce la clave, la cual solo se encuentra en posesión de las personas que pueden tener acceso a claves, una privada que se utiliza

para la encriptación y otra pública para la desencriptación. En algunos métodos la clave pública no puede efectuar la desencriptación o descifrado, sino solamente comprobar que el criptograma fue encriptado o cifrado usando la clave privada correspondiente y no ha sido alterado o modificado desde entonces.

b. Encriptación WEP

Una encriptación WEP (Wired Equivalent Privacy o Privacidad Equivalente a Cableado) es un tipo de cifrado, implementado en el protocolo de conexión Wifi 802.11, que se encarga de cifrar la información que vamos a transmitir entre dos puntos de forma que solo le sea posible tener acceso a ellos e interpretarlos a aquellos puntos que tengan la misma clave.

En general, un router Wifi o un Access Point solo va a permitir el acceso a aquellos terminales que tengan la misma clave de encriptación WEP.

Esta clave puede ser de tres tipos

- Clave WEP de 64 bits. - 5 Caracteres o 10 dígitos hexadecimales ("0 a 9" "A - F", precedidos por la cadena "0x").
- Clave WEP de 128 bits. - 13 Caracteres o 26 dígitos hexadecimales ("0 a 9" "A - F", precedidos por la cadena "0x").
- Clave WEP de 256 bits. - 29 Caracteres o 58 dígitos hexadecimales ("0 a 9" "A - F", precedidos por la cadena "0x").

La que más suele usar es la de 128 bits, que ofrece un buen nivel de protección sin ser excesivamente larga y complicada.

La encriptación WEP de 256 bits no es soportada por muchos dispositivos. Una clave de encriptación WEP se puede descifrar (existen programas para ello), pero para esto es necesario un tráfico ininterrumpido de datos durante un tiempo determinado (por cierto, bastantes datos y bastante tiempo).

Evidentemente, cuanto mayor sea el nivel de encriptación y más complicada sea la clave más difícil va a ser de descifrar.

No se tarda lo mismo (a igualdad volumen de datos y tiempo) en descifrar la clave de una encriptación WEP de 64 bits que una de 128 bits, no existiendo además entre ambos una relación aritmética, es decir, que no se tarda el doble en descifrar una clave de encriptación WEP de 128 bits que una de 64 bits.

A pesar de que es posible descifrar estas claves de encriptación, no debemos pensar que sea fácil ni rápido. Una buena clave de encriptación WEP de 128 bits (por no decir una de 256 bits) puede llegar a ser prácticamente indescifrable si nos hemos asegurado de que sea lo suficientemente complicada.

c. Encriptación WPA

Una encriptación WPA (Wireless Protected Access) de este tipo actúa de diferente forma y es bastante más segura. El mayor inconveniente es que no son muchos los dispositivos Wifi que la soportan. Puede ser de dos tipos:

- Basada en servidores de autenticación (normalmente servidores Radius (Remote Authentication Dial-In User)), en la que es el servidor de autenticación el encargado de distribuir claves diferentes entre los usuarios. En un principio la encriptación WPA se creó para ser utilizada en este sistema.
- Este tipo de encriptación no solo es utilizado por las conexiones Wifi, sino también por otro tipo de conexiones que requieren autenticación. Suele ser el empleado entre otros los proveedores de servicios de Internet (ISP). Es un sistema sumamente seguro, aunque algo excesivo para nuestra conexión Wifi.

d. La encriptación WPA-PSK (Wireless Protected Access Pre-Share Key).

Este tipo de encriptación Utiliza un tipo de algoritmo denominado RC4, también empleado en las encriptaciones WEP, con una clave de 128 bits y un vector de inicialización de 48 bits, en vez de un vector de inicialización de 24 bits, que es el utilizado por la encriptación WEP.

A esto hay que añadirle el uso del protocolo TKIP (Temporal Key Integrity Protocol) que cambia la clave de encriptación dinámicamente, a medida que utilizamos esa conexión. Si unimos ambos sistemas obtenemos un sistema casi imposible de violar (y digo casi por imposible no hay casi nada).

Como ya hemos visto, una clave de 128 bits está compuesta por una cadena de 13 caracteres o 26 dígitos hexadecimales ("0 - 9" "A - F"), a lo que si usamos la posibilidad de usar y mezclar tanto mayúsculas y minúsculas se tiene alto número de posibilidades.

e. Encriptación WPA2 o 802.11i

Aunque la seguridad que se obtiene con una encriptación WPA es sumamente alta, y la que alcanzamos con una encriptación WPA2, es altísima, no todos los dispositivos Wifi admiten este tipo de encriptación, que además presenta una serie de inconvenientes.

El estándar 802.11i elimina muchas de las debilidades de sus predecesores tanto en lo que autenticación de usuarios como a su robustez de los métodos de encriptación se refiere. Y lo que consigue en el primer caso gracias a su capacidad para trabajar en colaboración con 802.1x, y en el segundo, mediante la incorporación de encriptación Advanced Encryption Standard (AES).

Aparte de incrementar de manera más que significativa la seguridad de los entornos WLAN, también reduce considerablemente la complejidad y el tiempo de roaming de los usuarios de un punto de acceso a otro.

Funcionamiento

Cuando una estación inalámbrica solicita abrir una sesión con el punto de acceso, entre ambos extremos se establece una clave denominada Pairwise Master Key (PMK). Para ello se utiliza típicamente el estándar LAN y WLAN 802.1x, que permite al responsable de seguridad aplicar un método de autenticación tan potente como desee, desde las simples combinaciones usuario/contraseña hasta certificados digitales. Se trata de un mecanismo de autenticación de usuario basado en plataforma RADIUS (o cualquier otro servidor de autenticación TACAS+) y en el protocolo Extensible Authentication Protocol (EAP). EL servidor RADIUS retorna la PMK al punto de acceso, y entonces, éste y la estación intercambian una secuencia de cuatro mensajes, denominada “four-way handshake” (algo así como saludo o reconocimiento de cuatro vías).

Durante el proceso “four-way handshake”, se utilizan la PMK y diversos valores generados aleatoriamente tanto desde la estación como desde el punto de acceso, renovándose varias veces durante la sesión para securizar el proceso de pacto de una nueva clave, denominada Pairwise Transient Key (PTK). Ésta se compone a su vez de tres subclaves: una para firmar los cuatro mensajes que intervendrán en el proceso, otra para asegurar los paquetes de datos transmitidos entre los dispositivos implicados y una tercera para encriptar la llamada “clave de grupo”, que será enviada desde el punto de acceso a la estación y que permitirá a aquel difundir tráfico multicast a toso los clientes a él asociados, sin tener que enviar a cada uno de ellos un mismo paquete de forma diferente.

Proceso

A lo largo del proceso, estación y punto de acceso negocian también el tipo de encriptación que utilizarán para cada conexión resultando dos cifras. Una de ellas es la clave de grupo ya mencionada; la otra, denominada cifra o clave pairwise (reconocimiento de pareja), se utilizará para las transmisiones

de datos en modo unicast que sólo afectan al punto de acceso 802.11i permite la negociación de cualquier cifra de encriptación, aunque la tecnología de referencia para la especificación sea AES con clave de 128 bits en modo CCM (Counter with CBC-MAC).

En un entorno puro, AES será utilizado normalmente tanto para la cifra de pareja como grupo. Sin embargo, en caso de que el punto de acceso dota de soporte de la norma dependan tanto dispositivo 802.11i aporta hay que descartar también su capacidad para acelerar la itinerancia o roaming entre puntos de acceso. Con WPA era necesario que la estación realizara la autenticación 802.1x completa cada vez que se asociaba a un nuevo punto de acceso. Ahora, cuando un cliente wireless retorna a un punto de acceso con el que ya está autenticado, puede reutilizar la PMK acordada con anterioridad, omitiendo el proceso 802.11x y pasando directamente al diálogo four-handshake. Además, la estación puede pre autenticarse en un punto de acceso al que tiene intención de itinerar, sin perder su asociación con el de origen.

Finalmente, el estándar incluye la técnica de roaming rápido conocida informalmente como Opportunistic Key Caching o Proactive Key Caching. Si se hace múltiples puntos de acceso compartan claves PMK, la estación puede itinerar entre ellos y acceder a puntos que no haya visitado antes reutilizando la PMK establecida con el punto de acceso al que hubiera estado asociada con anterioridad.

f. Encriptación 802.1x

El estándar 802.1x está diseñado para mejorar la seguridad de las redes de área local inalámbricas (WLAN) que siguen el estándar IEE 802.11. 802.1x Proporciona una autenticación para redes LAN inalámbricas, lo que permite a un usuario ser autenticado por una autoridad central.

Es una LAN inalámbrica con 802.1x, un usuario (conocido como el suplicante) genera las solicitudes de acceso a un punto de acceso (conocido

como el autenticador). El punto de acceso obliga al usuario (en realidad, el usuario del software de cliente) no autorizado en un estado que permite al cliente enviar sólo un mensaje de inicio EAP. El punto de acceso EAP devuelve un mensaje solicitando identidad de usuario. El cliente devuelve la identidad, que se transmite por el punto de acceso al servidor de autenticación, que utiliza un algoritmo para autenticar el usuario y devuelve un aceptar o rechazar el mensaje de vuelta al punto de acceso. Aceptar la hipótesis de una se ha recibido, el punto de acceso cambia el estado del cliente a ser autorizado y el tráfico normal ya podrá circular.

El autenticador no tiene por qué ser una máquina inteligente, por lo que pequeños APs podrán utilizar este estándar 802.1x.

La adopción de 802.11i supondrá hacer frente a las actualizaciones de firmware de los puntos de acceso y estaciones. En caso de que el hardware haya quedado obsoleto para el soporte de la nueva norma, habrá que comprar puntos de acceso capaces de tratar AES, dado que, pese a que 802.11i puede operar con cualquier otra técnica de encriptación, el soporte de esta especificación es precisamente su principal ventaja sobre WPA.

Será necesario instalar servidores de autenticación y de autoridades de certificados si no se dispone de ellos, y, por supuesto, añadir no sólo uno, sino dos protocolos más a la red, dado que, como se ha dicho, 802.11i gestiona la parte de encriptación de la seguridad WLAN, pero es también una tecnología bastante reciente, todavía brilla por su ausencia en la mayoría de las organizaciones.

g. EAP (Extensible Authentication Protocol)

La mayoría de los suministradores utilizan EAP como medio de comunicar peticiones de acceso entre cliente y punto de acceso. Pero este tipo de paquetes transportan sólo peticiones; el protocolo no describe cómo gestionar la autenticación misma. En consecuencia, cada fabricante ha optado por alguna de las extensiones propietarias que definen la tecnología

sobre la que se soportará otra gestión, dando lugar a una auténtica sopa de acrónimos referidos todos ellos a implementaciones acordes con EAP pero, en ocasiones, incompatibles entre sí.” (Delgado Ortiz, Seguridad en Redes Inalámbricas, 2010)

4.2.6. Protocolos de confidencialidad e integridad de datos

“Los Protocolos de confidencialidad e integridad de datos han pasado por un proceso evolutivo desde TKIP incorporado en el protocolo de encriptación WAP hasta el protocolo CCMP incorporado en el protocolo de encriptación WAP2.

TKIP (Temporal Key Integrity Protocol): Protocolo de integridad de clave temporal, surgió como una actualización (Wi-Fi CERTIFIED nombra esta actualización como WAP) para reforzar los sistemas WEP, sin tener que cambiar el antiguo hardware de red. Por ello, al igual que WEP, se basa en el algoritmo de encriptación RC4, lo que acarrea limitaciones de seguridad que son remediadas con la desconexión de 60 segundos y establecimiento de nuevas claves cuando se produzcan más de 2 fallas de MIC por minuto. Corrige las siguientes vulnerabilidades de WEP:

- Integridad de mensaje: Lo logra usando un nuevo control de integridad del mensaje MIC basado en el algoritmo Michael de Niels Ferguson con 20 bits de seguridad, que impide la modificación de los datos dentro de un paquete mientras es transmitido.
- Reutilización de claves de inicialización: Incluye nuevas reglas de selección y va incrementando su valor, evitando su reutilización, genera una nueva clave cada 10000 paquetes o 10 Kbytes de información transmitida.
- Gestión de claves: Aplica el algoritmo “hash” al vector de inicialización para la distribución y modificación de claves.

Ahora el vector de inicialización es encriptado y repartido por distintas ubicaciones del paquete.

WRAP (Wireless Robust Authenticated Protocol): Basado en el algoritmo de encriptación AES, fue el primer protocolo elegido por el estándar IEEE 802.11i, pero se abandonó por motivos de propiedad intelectual y posibles licencias.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol): A diferencia de TKIP, este protocolo no nació para acomodarse al hardware WEP, por ello tiene un nuevo diseño basado en el algoritmo de encriptación de bloques AES (cuenta con un contador extra inicializado en 1 y se incrementa en cada bloque). Además, utiliza el método de autenticación de 14 mensajes CBC – MAC (Cipher Block Chaining) para producir un MIC. Usa una clave única, pero con diferentes vectores de inicialización, el vector es incrementado en cada fragmento del paquete. La cabecera CCMP no viaja encriptada pero los datos si, incluido el vector.” (pucp, 2015)

4.2.7. Sistemas Operativos Linux

“¿Qué es software libre?

El Software Libre (nótense las mayúsculas) es un concepto que no es nuevo. La idea principal detrás de estas palabras es la libertad de compartir la información. Actualmente, existen varias modalidades de desarrollo y distribución de software, que son:

- **Software propietario:** estos programas y aplicaciones suelen estar desarrollados por empresas que licencian el código fuente del programa y no permiten su redistribución. Cuando una persona adquiere un sistema propietario, generalmente sólo obtiene una versión pre compilada de ese código fuente, con permiso para ser usada en “n” cantidad de computadoras. Si se lo quiere utilizar en un número mayor de computadoras, se debe pagar por cada

licencia un precio fijado por la empresa. Además, al no obtener el código fuente, el usuario está imposibilitado de modificar el programa o ver cómo funciona internamente. De más está decir que es ilegal copiar un programa de este tipo a un amigo o a un familiar.

- **Shareware:** ésta es una modalidad de desarrollo y distribución que tuvo mucho éxito a finales de los '80 y en los '90. La idea detrás del shareware es la de “probar antes de comprar”. Generalmente, estos programas no dejan de ser propietarios, pero se distribuye una versión reducida (o con límite de uso temporal) por los BBS y CDs de revistas para que la gente pueda probarlos. Si le gusta, puede pagar un precio por la versión completa, la cual tampoco incluye el código fuente (generalmente). La versión shareware es de libre distribución, la versión completa, no.

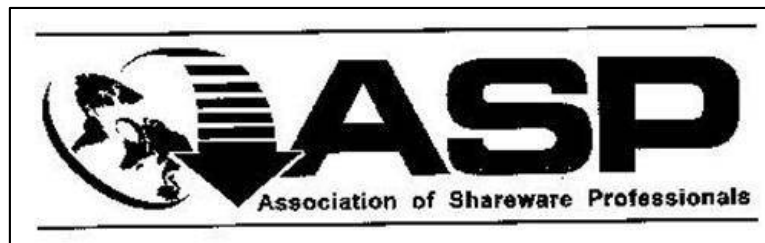


Ilustración 6: Los desarrolladores de shareware poseen su propia asociación.

Fuente: <http://www.trademarkia.com/asp-association-of-shareware-professionals-76693777.html>

- **Freeware:** en conjunto con el shareware, se desarrolló el freeware. Aquí las cosas son un poco mejores para el usuario final, ya que un programa que es freeware es un programa que está completo, y puede ser utilizado y distribuido libremente. El problema es que estos programas generalmente no tienen la calidad de uno propietario y de Software Libre. En los programas freeware tampoco se incluye el código fuente, por

lo que éstos sufren también las limitaciones mencionadas en las otras modalidades.

- **Software Libre:** y, finalmente, llegamos al Software Libre. El punto máximo de libertad tanto para el desarrollador como para el usuario. Para que un programa sea Software Libre, debe cumplir con cuatro requisitos básicos. El primero de ellos es que el programa pueda ser utilizado sin ningún tipo de limitación. El segundo requisito es que pueda ser distribuido libremente y copiado a cuantas computadoras sea necesario. El tercero es muy sencillo: el programa siempre debe estar acompañado del código fuente (o de una carta al usuario en donde se ofrezca un acceso a él). Este requisito es muy importante, ya que al disponer del código fuente, Los usuarios pueden hacerle modificaciones y, así, adecuarlo mejor a sus necesidades. El último punto, en realidad, no es un requisito: un programa que es Software Libre se puede vender. Incluso se puede vender una versión modificada de un programa de Software Libre. Siempre y cuando se respeten los nombres de los autores originales y los tres puntos anteriores, no hay ninguna restricción para hacer algo de dinero con un programa de software Libre.



Ilustración 7: En el sitio oficial del proyecto GNU (www.gnu.org).

Fuente: <https://www.gnu.org/distros/screenshot.html>

¿Qué es GNU/Linux?

Muchos querrán saltar esta sección alegando que no estarían leyendo este libro si no supieran lo que es GNU/Linux. En realidad, esta sección es más importante de lo que parece.

GNU/Linux es el primer sistema operativo basado en UNIX que es 100% Software Libre. Si bien anteriormente había otros sistemas operativos de libre distribución (como MINIX), éstos no eran totalmente Software Libre, ya que eran regidos por licencias más restrictivas.

GNU/Linux es un proyecto que ya lleva 20 años en desarrollo, y lo estará por muchos más, ya que se asienta sobre una base de cientos de programadores de todas partes del mundo. Muchas veces me preguntan si no es posible que “el que hace Linux un día se vuelva rebelde y quiera hacer que su sistema sea propietario”. La respuesta es, obviamente, negativa. No existe una persona “que hace Linux”. GNU/Linux es un conjunto de componentes desarrollados por muchas personas que trabajan en muchos proyectos. No es un único paquete (aunque muchos de ustedes lo hayan instalado como tal). Es prácticamente imposible parar un proyecto de estas magnitudes.

Hablando técnicamente, GNU/Linux es un sistema operativo de software libre basado en UNIX, que cumple las normas POSIX. Su base es un núcleo monolítico llamado Linux (a secas), desarrollado originalmente por Linus B. Torvalds a principios de la década de los noventa. Su estructura general es la típica de cualquier sistema UNIX (núcleo – intérprete de comandos – aplicaciones), aunque actualmente debe de ser el más desarrollado de ellos. Cuenta con una interfaz gráfica llamada Xfree86 (versión libre del sistema de ventanas Xwindow original del MIT) y con muchas aplicaciones para realizar las más diversas tareas, desde procesamiento de textos hasta montaje de servidores de red, pasando por aplicaciones multimedia y juegos.” (Facundo Arena, 2011)

a. Sistema Operativo Ubuntu

“¿Qué es Ubuntu?”

Ubuntu es un sistema operativo desarrollado por la comunidad que es perfecto para laptops, computadoras de escritorio y servidores. Ya sea que lo utilices en el hogar, en la escuela o en el trabajo, Ubuntu contiene todas las aplicaciones que puedas necesitar, desde procesadores de texto y aplicaciones de email, hasta software para servidor web y herramientas de programación.

Ubuntu es y siempre será libre de costo. No pagas por una licencia de uso. Puedes descargar, usar y compartir Ubuntu con tus amigos, familiares, escuela o negocios libremente.

Se publica un nuevo lanzamiento de la versión de escritorio y servidor cada seis meses. Esto significa que siempre tendrás las más recientes aplicaciones que el mundo del open source te puede ofrecer.

Ubuntu está diseñado pensando en la seguridad. Consigues actualizaciones de seguridad libremente por lo menos 18 meses en la versión de escritorio y servidor. Con la versión con Long Term Support (LTS) tienes soporte por tres años en la versión de escritorio, y cinco años en la versión de servidor. No se requiere de pagos extra por la versión LTS, ponemos lo mejor de nuestro trabajo disponible a todos en los mismos términos libres. Actualizaciones a la nueva versión de Ubuntu son y siempre serán libres de costo.” (Ubuntu_Mexico, 2015)



*Ilustración 8: Logo del Sistema Operativo Ubuntu.
Fuente: <http://pcwallart.com/linux-ubuntu-wallpaper-2.html>*

4.2.8. Protocolos RADIUS y LDAP

a. RADIUS

“El protocolo RADIUS que significa en sus siglas en Ingles (Remote Authentication Dial In User Service).

Este puerto ha tenido muchas confusiones por la asignación del puerto.

El despliegue rápido de RADIUS se realiza mediante el puerto 1645, el cual entra en conflicto con el protocolo "DATAMETRICS", pero originalmente el puerto asignado a RADIUS es el 1812 oficialmente.

¿Qué es RADIUS?

RADIUS es un protocolo UDP de autenticación y autorización, para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Sus principales características son:

- **Cliente / Servidor**

Modelo Network Access Server (NAS).

Funciona como un cliente de RADIUS. El cliente es responsable de pasar la información del usuario a los servidores RADIUS designados, y luego actuar sobre la respuesta que se devuelve.

- **Red de Seguridad**

Las transacciones entre el cliente y el servidor RADIUS se autentican a través de la utilización de un secreto compartido, que nunca se envían a través de la red. Además, todas las contraseñas de usuario se envían cifrados entre el cliente y el servidor RADIUS, para eliminar la posibilidad de que alguien husmeando en una red no segura podría determinar la contraseña de un usuario.

- **Mecanismos de autenticación flexible.**

El servidor RADIUS puede apoyar una variedad de métodos para autenticar a un usuario. Cuando se proporciona con el nombre de

usuario y la contraseña original dado por el usuario, que puede soportar PPP PAP o CHAP, inicio de sesión UNIX, y otros mecanismos de autenticación.

- **Protocolo Extensible**

Todas las transacciones se componen de atributo de longitud variable Relación longitud-3-tuplas. Nuevos valores de los atributos se pueden añadir sin perturbar las implementaciones existentes del protocolo.

Estas son las 4 características principales de RADIUS, sus funciones principales y características.

RADIUS permite una autenticación segura, basada en cliente/servidor, o servidor/servidor, las autenticaciones que realiza son mediante puertos seguros, un claro ejemplo del uso de este protocolo es el conectarse al internet.

Los ISP's (Internet Service Provided), usan este protocolo para mediante el ADSL-Modem enviar la información del usuario que quiere conectarse a sus servidores.

El protocolo presenta conflictos con Norton-Symantec al momento de instalar su antivirus, según lo que ya eh probado, hay que deshabilitar este protocolo para poder instalar este programa.” (RADIUS_1812, 2015)

b. LDAP

“LDAP (Protocolo compacto de acceso a directorios) es un protocolo estándar que permite administrar directorios, esto es, acceder a bases de información de usuarios de una red mediante protocolos TCP/IP.

Las bases de información generalmente están relacionadas con los usuarios, pero, algunas veces, se utilizan con otros propósitos, como el de administrar el hardware de una compañía.

El objetivo del protocolo LDAP, desarrollado en 1993 en la Universidad de Michigan, fue reemplazar al protocolo DAP (utilizado para acceder a los servicios de directorio X.500 por OSI) integrándolo al TCP/IP. Desde 1995, DAP se convirtió en LDAP independiente, con lo cual se dejó de utilizar sólo para acceder a los directorios tipo X500. LDAP es una versión más simple del protocolo DAP, de allí deriva su nombre Protocolo compacto de acceso a directorios.

Presentación de LDAP

El protocolo LDAP define el método para acceder a datos en el servidor a nivel cliente, pero no la manera en la que se almacena la información.

El protocolo LDAP actualmente se encuentra en su 3era versión y el IETF (Grupo de Trabajo de Ingeniería de Internet) lo ha estandarizado. Por lo tanto, existe una RFC (petición de comentarios) para cada versión de LDAP que constituye un documento de referencia:

- RFC 1777 para LDAP v.2
- RFC 2251 para LDAP v.3

LDAP le brinda al usuario métodos que le permiten:

- Conectarse
- Desconectarse
- Buscar información
- Comparar información
- Insertar entradas
- Cambiar entradas
- Eliminar entradas

Asimismo, el protocolo LDAP (en versión 3) ofrece mecanismos de cifrado (SSL, etc.) y autenticación para permitir el acceso seguro a la información almacenada en la base.” (CMM, 2015)

4.2.9. Servidor de Dominios

a. Bind (Berkeley Internet Name Domain)

“BIND (acrónimo de Berkeley Internet Name Domain) es una implementación del protocolo DNS y provee una implementación libre de los principales componentes del Sistema de Nombres de Dominio, los cuales incluyen:

- Un servidor de sistema de nombres de dominio (named).
- Una biblioteca resolutoria de sistema de nombres de dominio.
- Herramientas para verificar la operación adecuada del servidor DNS (bind-utils).

El Servidor DNS BIND es ampliamente utilizado en la Internet (99% de los servidores DNS) proporcionando una robusta y estable solución.

b. DNS (Domain Name System)

DNS (acrónimo de Domain Name System) es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombres de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. El DNS nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección IP.

Los Servidores DNS utilizan TCP y UDP en el puerto 53 para responder las consultas. Casi todas las consultas consisten de una sola solicitud UDP desde un Cliente DNS seguida por una sola respuesta UDP del servidor. TCP interviene cuando el tamaño de los datos de la respuesta excede los 512 bytes, tal como ocurre con tareas como transferencia de zonas.

c. NIC (Network Information Center)

NIC (acrónimo de Network Information Center o Centro de Información sobre la Red) es una institución encargada de asignar los nombres de dominio en Internet, ya sean nombres de dominios genéricos o por países, permitiendo

personas o empresas montar sitios de Internet mediante a través de un ISP mediante un DNS. Técnicamente existe un NIC por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país.

Por ejemplo: NIC México es la entidad encargada de gestionar todos los dominios con terminación .mx, la cual es la terminación correspondiente asignada a los dominios de México.

d. FQDN (Fully Qualified Domain Name)

FQDN (acrónimo de Fully Qualified Domain Name o Nombre de Dominio Plenamente Calificado) es un Nombre de Dominio ambiguo que especifica la posición absoluta del nodo en el árbol jerárquico del DNS. Se distingue de un nombre regular porque lleva un punto al final. Como ejemplo: suponiendo que se tiene un dispositivo cuyo nombre de anfitrión es «maquina1» y un dominio «dominio.com», el FQDN sería «maquina1.dominio.com.», de modo define de modo único al dispositivo mientras que pudieran existir muchos anfitriones llamados «maquina1», solo puede haber uno llamado «maquina1.dominio.com.». La ausencia del punto al final definiría que se pudiera tratar tan solo de un prefijo, es decir «maquina1.dominio.com» pudiera ser de un dominio más largo como «maquina1.dominio.com.mx».

La longitud máxima de un FQDN es de 255 bytes, con una restricción adicional de 63 bytes para cada etiqueta dentro del nombre del dominio. Solo se permiten los caracteres A-Z de ASCII, dígitos y el carácter «-». No se distinguen mayúsculas y minúsculas.

Desde 2004, a solicitud de varios países de Europa, existe el estándar IDN (acrónimo de Internationalized Domain Name) que permite caracteres no-ASCII, codificando caracteres Unicode dentro de cadenas de bytes dentro del conjunto normal de caracteres de FQDN. Como resultado, los límites de longitud de los nombres de dominio IDN dependen directamente del contenido mismo del nombre.

e. Componentes de un DNS

Los DNS operan a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

- **Clientes DNS**

Son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres. Básicamente preguntan por la dirección IP que corresponde a un nombre determinado.

- **Servidores DNS**

Son servicios que contestan las consultas realizadas por los Clientes DNS. Hay dos tipos de servidores de nombres:

Servidor Maestro (o primario) Obtiene los datos del dominio a partir de un fichero hospedado en el mismo servidor.

Servidor Esclavo (o secundario) Al iniciar obtiene los datos del dominio a través de un servidor un Servidor Maestro, realizando un proceso denominado transferencia de zona.

Un gran número de problemas de operación de servidores DNS se atribuyen a las pobres opciones de servidores secundarios para la zona de DNS. De acuerdo al RFC 2182, el DNS requiere que al menos tres servidores existan para todos los dominios delegados (o zonas). Una de las principales razones para tener al menos tres servidores para cada zona es permitir que la información de la zona misma esté disponible siempre y forma confiable hacia los Clientes DNS a través de Internet cuando un servidor DNS de dicha zona falle, no esté disponible y/o esté inalcanzable.

Contar con múltiples servidores también facilita la propagación de la zona y mejoran la eficiencia del sistema en general la brindar opciones a los Clientes DNS si acaso encontraran dificultades para realizar una consulta en un Servidor DNS. En otras palabras: tener múltiples servidores para una zona permite contar con redundancia y respaldo del servicio.

Con múltiples servidores, por lo general uno actúa como Servidor Maestro o Primario y los demás como Servidores Esclavos o Secundarios. Correctamente configurados y una vez creados los datos para una zona, no será necesario copiarlos a cada Servidor Esclavo o Secundario, pues éste se encargará de transferir los datos de manera automática cuando sea necesario.

Los Servidores DNS responden dos tipos de consultas:

Consultas Iterativas (no recursivas): El cliente hace una consulta al Servidor DNS y este le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas locales. Si no es posible dar una respuesta, la consulta se reenvía hacia otro Servidor DNS repitiéndose este proceso hasta encontrar al Servidor DNS que tiene la Zona de Autoridad capaz de resolver la consulta.

Consultas Recursivas: El Servidor DNS asume toda la carga de proporcionar la una respuesta completa para la consulta realizada por el Cliente DNS. El Servidor DNS desarrolla entonces Consultas Iterativas separadas hacia otros Servidores DNS (en lugar de hacerlo el Cliente DNS) para lograr la respuesta.

- **Zonas de Autoridad**

Permiten al Servidor Maestro o Primario cargar la información de una zona. Cada Zona de Autoridad abarca al menos un dominio y posiblemente sus sub-dominios, si estos últimos no son delegados a otras zonas de autoridad.

La información de cada Zona de Autoridad es almacenada de forma local en un fichero en el Servidor DNS. Este fichero puede incluir varios tipos de registros:

TIPO DE REGISTRO	DESCRIPCIÓN
A (Address)	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPv4 de 32 bits
AAAA	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPV6 de 128 bits.
CNAME (Canonical Name)	Registro de nombre canónico que hace un nombre sea alias de otro. Los dominios con alias obtienen los subdominios y registros DNS del dominio original.
MX (Mail Exchanger)	Registro de servidor de correo que sirve para definir una lista de servidores de correo para un dominio, así como la prioridad entre éstos.
PTR (Pointer)	Registro de apuntador que resuelve direcciones IPV4 hacia el nombre de anfitriones. Es decir, hace lo contrario al registro A. Se utiliza en zonas de Resolución Inversa.
NS (Name Server)	Registro de servidor de nombres que sirve para definir una lista de servidores de nombres con autoridad para un dominio.
SOA (Start of Authority)	Registro de Inicio de autoridad que especifica el Servidor DNS Maestro (o primario) que proporcionará la información con autoridad acerca de un dominio de Internet, dirección de correo electrónico del administrador, número de serie del dominio y parámetros de tiempo para a zona.
SVR (services)	Registro de servicios que especifica al administrador insertar texto arbitrariamente en un registro DNS. Este tipo de registro es muy utilizado por los servidores de listas negras DNSBL (DNS – based Blackhole List) para la filtración de Spam. Otro ejemplo de uso son las VPN, donde suele requerirse un registro TXY para definir una llave que será utilizada por los clientes.

Tabla 2: Zona de autoridad – Tipo de Registro

Las zonas que se pueden resolver son:

Zonas de Reenvío

Devuelven direcciones IP para las búsquedas hechas para nombres FQDN (Fully Qualified Domain Name). En el caso de dominios públicos, la responsabilidad de que exista una Zona de Autoridad para cada Zona de Reenvío corresponde a la autoridad misma del dominio, es decir, y por lo general, quien esté registrado como autoridad del dominio tras consultar una base de datos WHOIS. Quienes compran dominios a través de un NIC (por ejemplo: www.nic.mx) son quienes se hacen cargo de las Zonas de Reenvío, ya sea a través de su propio Servidor DNS o bien a través de los Servidores DNS de su ISP.

Salvo que se trate de un dominio para uso en una red local, todo dominio debe ser primero tramitado con un NIC como requisito para tener derecho legal a utilizarlo y poder propagarlo a través de Internet.

Zonas de Resolución Inversa

Devuelven nombres FQDN (Fully Qualified Domain Name) para las búsquedas hechas para direcciones IP.

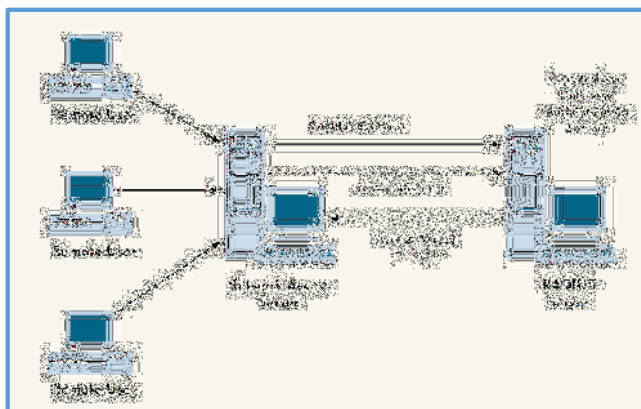
En el caso de segmentos de red públicos, la responsabilidad de que exista de que exista una Zona de Autoridad para cada Zona de Resolución Inversa corresponde a la autoridad misma del segmento, es decir, y por lo general, quien esté registrado como autoridad del segmento tras consultar una base de datos WHOIS.

Los grandes ISP, y en algunos casos algunas empresas, son quienes se hacen cargo de las Zonas de Resolución Inversa.” (Dueñas, 2012)

4.2.10. Servidor RADIUS y LDAP

a. Servidor RADIUS

“Es un protocolo ampliamente usado en el ambiente de redes, para dispositivos tales como routers, servidores y switches entre otros. Es utilizado para proveer autenticación centralizada, autorización y manejo de cuentas de acceso inalámbrico.



*Ilustración 9: Dial-Access network usando RADIUS.
Fuente: <http://www.tech-faq.com/radius-server.html>*

Características:

Los sistemas embebidos generalmente no pueden manejar un gran número de usuarios con información diferente de autenticación. Requiere una gran cantidad de almacenamiento.

- RADIUS facilita una administración centralizada de usuarios. Si se maneja una enorme cantidad de usuarios, continuamente cientos de ellos son agregados o eliminados a lo largo del día y la información de autenticación cambia continuamente. En este sentido, la administración centralizada de usuarios es un requerimiento operacional.
- Debido a que las plataformas en las cuales RADIUS es implementado son frecuentemente sistemas embebidos, hay oportunidades limitadas para soportar protocolos adicionales.

Algún cambio al protocolo RADIUS deberá ser compatible con clientes y servidores RADIUS pre-existent.

- Un cliente RADIUS envía credenciales de usuario e información de parámetros de conexión en forma de un mensaje RADIUS al servidor. Éste autentica y autoriza la solicitud del cliente y envía de regreso un mensaje de respuesta. Los clientes RADIUS también envían mensajes de cuentas a servidores RADIUS.

Los mensajes RADIUS son enviados como mensajes UDP (User Datagram Protocol). El puerto UDP 1812 es usado para mensaje de autenticación RADIUS y, el puerto UDP 1813, es usado para mensaje de cuentas RADIUS. Algunos servidores usan el puerto UDP 1645 para mensajes de autenticación y, el puerto 1646, para mensajes de cuentas. Esto último debido a que son los puertos que se usaron inicialmente para este tipo de servicio.

Índice RFC RADIUS

RFC-2058 –Remote Authentication Dial-In User Server (RADIUS)

RFC-2059 – RADIUS Accounting

RFC2548 – Microsoft Vendor – Specific RADIUS Attributes

RFC 2618 – RADIUS Authentication Client MIB

RFC 2619 – RADIUS Authentication Server MIB

RFC 2620 – RADIUS Accounting Client MIB

RFC 2621 – RADIUS Accounting Server MIB

RFC 2809 – Compulsory Tunneling via RADIUS

RFC 2865 – Remote Authentication Dial-In User Service (obsoleto RFC 2138; actualizado por RFC 2868)

RFC 2866 – RADIUS Accounting (Obsoleto RFC 2139; actualizado por RFC 2867)

RFC 2867 – RADIUS Accounting Modifications for Tunner Protocol Support

RFC 2868 – RADIUS Attributes for Tunneling Support

RFC 2869 – RADIUS Extensions

b. Servidor LDAP

“¿Qué es LDAP?

LDAP (“Lightweight Directory Access Protocol”, «Protocolo Ligero de Acceso a Directorios») es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio. Se usó inicialmente como un front-end o interfaz final para X.500, pero también puede usarse con servidores de directorio únicos y con otros tipos de servidores de directorio.

¿Qué es un servicio de directorio?

Un directorio es como una base de datos, pero en general contiene información más descriptiva y más basada en atributos. La información contenida en un directorio normalmente es leída mucho más de lo que se escribe. Como consecuencia los directorios no implementan normalmente los complicados esquemas para transacciones o esquemas de reducción (rollback) que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos. Por contra, las actualizaciones en un directorio son usualmente cambios sencillos de «todo o nada», si es que se permiten en algo.

Los directorios están afinados para proporcionar una respuesta rápida a operaciones de búsqueda o consulta. Pueden tener la capacidad de replicar información de forma amplia, con el fin de aumentar la disponibilidad y la fiabilidad, y a la vez reducir el tiempo de respuesta. Cuando se duplica (o se replica) la información del directorio, pueden aceptarse inconsistencias temporales entre la información que hay en las réplicas, siempre que finalmente exista una sincronización.

Existen muchas maneras distintas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos

de información, establecer requisitos diferentes para hacer referencias a la información, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados, etc. Algunos servicios de directorio son locales, proporcionando servicios a un contexto restringido (por ejemplo, el servicio de finger en una única máquina). Otros servicios son globales, proporcionando servicio en un contexto mucho más amplio.

¿Cómo funciona LDAP?

El servicio de directorio LDAP se basa en un modelo cliente-servidor. Uno o más servidores LDAP contienen los datos que conforman el árbol del directorio LDAP o base de datos troncal. El cliente ldap se conecta con el servidor LDAP y le hace una consulta. El servidor contesta con la respuesta correspondiente, o bien con una indicación de dónde puede el cliente hallar más información (normalmente otro servidor LDAP). No importa con qué servidor LDAP se conecte el cliente: siempre observará la misma vista del directorio; el nombre que se le presenta a un servidor LDAP hace referencia a la misma entrada a la que haría referencia en otro servidor LDAP. Es ésta una característica importante de un servicio de directorios universal como LDAP.” (LDAP_LINUX, 2015)

Ventajas en el uso de LDAP:

“Un directorio LDAP destaca sobre los demás tipos de bases de datos por las siguientes características:

- Es muy rápido en la lectura de registros
- Permite replicar el servidor de forma muy sencilla y económica
- Muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente
- Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas
- Usa un sistema jerárquico de almacenamiento de información.
- Permite múltiples directorios independientes
- Funciona sobre TCP/IP y SSL

- La mayoría de aplicaciones disponen de soporte para LDAP
- La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.” (Servidor_LDAP, 2015)

4.2.11. Metodología de Redes

METODOLOGÍA	DESCRIPCIÓN
METODOLOGÍA DESARROLLADA POR EL INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA INEI	Esta consiste en cuatro etapas y se enfocan principalmente en LANs de corta capacidad.
METODOLOGÍA ELABORADA POR JAMES MCCABE	Orientada a redes que se encuentran en campus, se realiza en cuatro fases.
TOP-DOWN NETWORK DESIGN – CISCO	Se asocia a las necesidades del negocio y a la tecnología disponible. Basado en cuatro Fases
METODOLOGÍA CISCO PDIOO	Se enfoca en cuatro fases y se detalla de manera robusta las necesidades a nivel empresarial, sin embargo está encaminado a redes WAN.

Tabla 3: Cuadro comparativos de metodología de redes.

Para el proyecto de tesis se utilizará la metodología CISCO Top-Down Network Design pues está orientada a optimizar el ancho de banda y por su modelo Jerárquico evita que los dispositivos se comuniquen con demasiados dispositivos similares y facilita la escalabilidad.

Es una metodología que propone cuatro Fases, para el diseño de redes

- I. Fase1** : Análisis de Negocios Objetivos y limitaciones
- II. Fase2** : Análisis de Datos y Requisitos
- III. Fase3** : Diseño de la Solución
- IV. Fase4** : Simulación de la estructura de red y equipos propuestos

I. Fase de Análisis de Negocio, Objetivos y Limitaciones

En esta fase se identificará los objetivos y restricciones del negocio, y los objetivos y restricciones técnicos del cliente.

Analizar los objetivos del negocio

- Conocer línea de negocio y el mercado del cliente
- Estructura organizacional la empresa
- Conocer sus proveedores
- Filiales, Oficinas remotas
- Determinar la autoridad responsable para la aceptación del Diseño de Red propuesto
- Identificar los cambios que el proyecto generaría

II. Análisis de Datos y Requisitos

En esta fase se diseñará la topología de red, el modelo de direccionamiento y nombramiento, y se seleccionará los protocolos de bridging, switching y routing para los dispositivos de interconexión. El diseño lógico también incluye la seguridad y administración de la red.

III. Diseño de la Solución

Esta fase implica en seleccionar las tecnologías y dispositivos específicos que darán satisfacción a los requerimientos técnicos de acuerdo al diseño lógico propuesto (LAN / WAN)

1. Selección de Tecnologías y dispositivos para la red del Campus

- Diseño del Cableado Estructurado
- Tecnologías LAN: ATM, Fast Ethernet, Giga Ethernet
- VoIP
- Switch
- Router
- Bridge
- Inalámbrico
- Radio enlaces
- Otros

2. Selección de Tecnologías y dispositivos para la red Empresarial

- Tecnología de acceso remoto
- Línea de Suscripción Digital (DSL)
- Red Privada Virtual (VPN)
- Línea Dedicada
- Acceso Satelital
- Otros

IV. Simulación de la estructura de red y equipos propuestos

Cada sistema es diferente; la selección de métodos y herramientas de prueba correctos, requiere creatividad, ingeniosidad y un completo entendimiento del sistema a ser evaluado.

Implementación de un Plan de Pruebas

1. Prueba del Diseño de la red

- Usar pruebas de los fabricantes
- Construir un prototipo de pruebas
- Herramientas de prueba de diseño de redes
- Un escenario de prueba del Diseño de red
- La prueba debe incluir análisis de performance y de fallas:
 - Prueba de aplicación de tiempo de respuesta
 - Prueba de Rendimiento
 - Prueba de la Disponibilidad
 - Prueba de Regresión

2. Optimización del Diseño de la red

- Optimización del uso del ancho de Banda con Tecnología IP Multicast
- Reduciendo el Delay de la serialización.
- Optimización de la performance de la red para QoS

- Cisco Internetwork Operating System Features for
- Optimizing Network

3. Documentación de la red

- Respondiendo a la propuesta de los requerimientos del cliente
- Los contenidos de los documentos del Diseño de la Red” (Metodologia Redes, 2016)

4.2.12. Redes Privadas Virtuales – VLAN

“Los grupos de trabajo en una red, creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o hub traen como consecuencia directa, que estos grupos de trabajo compartan el ancho de banda disponible y los dominios del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

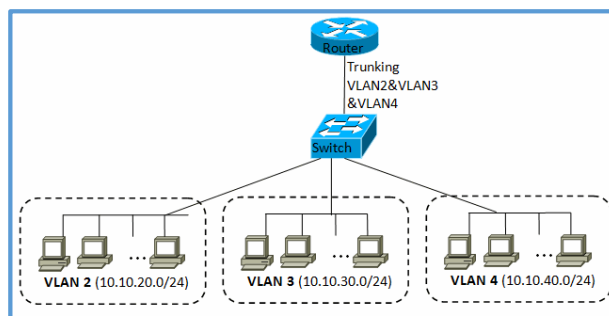


Ilustración 10: Estructura de una VLAN.

Fuente: <http://wiki.mikrotik.com/images/9/9a/Image12005.jpeg>

Una VLAN es una lógica de red de área local (LAN) que se extiende más allá de una sola LAN tradicional a un grupo de segmentos de LAN, habida cuenta de configuraciones específicas. Debido a que una VLAN es una entidad lógica, su creación y configuración se realiza completamente en software.

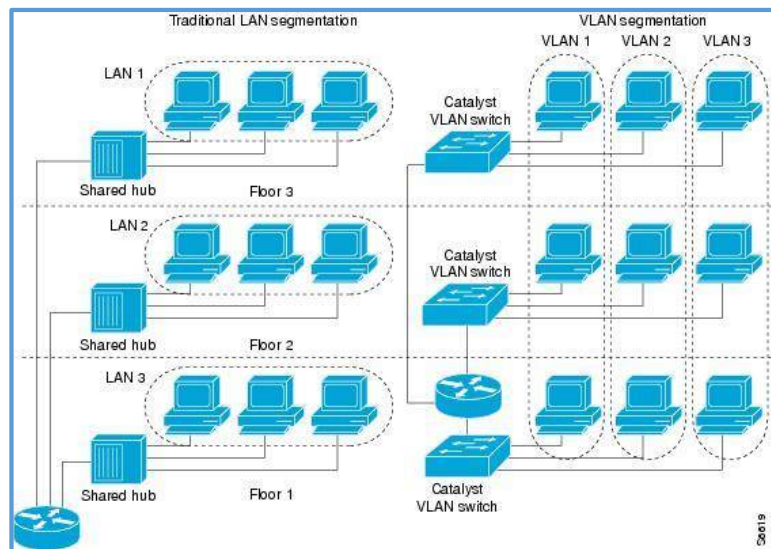


Ilustración 11: Segmentación VLAN.

Fuente: http://www.cisco.com/c/dam/en/us/td/i/Other/Software/S6501-7000/s6619.ps/_jcr_content/renditions/s6619.jpg

Las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de “broadcast”.

La principal diferencia con la agrupación física, como se ha mencionado, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma.

Los usuarios pueden, así, “moverse” a través de la red, manteniendo su pertenencia al grupo de trabajo lógico.

Identificación de VLAN

Dado que una VLAN es un concepto de software. La identificación es el proceso utilizado para garantizar que los miembros de la VLAN estén debidamente configurados en un agrupamiento lógico y se diferencien de otra VLAN. Con el identificador, las tramas tienen la debida VLAN ID en su origen a fin de que puedan ser debidamente procesadas, ya que pasan a través de la red.

La VLAN ID se utiliza para permitir la conmutación y encaminamiento de la información que un equipo transmite; a su vez realiza las decisiones apropiadas, que se definen en la configuración de VLAN.

Beneficios

Esquematizando los puntos en que las redes virtuales benefician a las redes actuales:

- **Movilidad:** Como hemos visto, el punto fundamental de las redes virtuales es el permitir la movilidad física de los usuarios dentro de los grupos de trabajo.
- **Dominios lógicos:** Los grupos de trabajo pueden definirse a través de uno o varios segmentos físicos o, en otras palabras, los grupos de trabajo son independientes de sus conexiones físicas, ya que están contruidos como dominios lógicos.
- **Control y conversación del ancho de banda:** Las redes virtuales pueden restringir los broadcast a los dominios lógicos donde han sido generados. Además, añadir usuarios a un determinado dominio o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros.
- **Conectividad:** Los modelos con funciones de routing nos permiten interconectar diferentes conmutadores y expandir las redes virtuales a través de ellos, incluso aunque estén situados en lugares geográficos diversos.
- **Seguridad:** Los accesos desde y hacia los dominios lógicos, pueden ser restringidos, en función de las necesidades específicas de cada red, proporcionando un alto grado de seguridad.
- **Protección de la Inversión:** Las capacidades VLAN están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado, sino más bien los evitan, facilitando las reconfiguraciones de la red sin costes adicionales.
- **Diseños tradicionales de uso de red routers para crear dominios de difusión y limitar las emisiones entre múltiples subredes:** Esto evita que emitan las inundaciones en las grandes redes de consumo de recursos, no intencional o causar denegaciones de servicio.

Desventajas:

Lamentable, la tradicional metodológica de diseño de redes tiene algunos defectos en su diseño.

Geographic Focus – los diseños tradicionales de red se centran en ubicaciones físicas de los equipos y personal para hacer frente segmento de LAN y colocación. Debido a esto, hay algunos inconvenientes importantes:

- Segmento de red físicamente separado para las organizaciones no pueden formar parte del mismo espacio de direcciones. Cada ubicación física debe abordarse con independencia, y ser parte de su propio dominio de difusión. Esto puede obligar al personal a estar situados en una zona céntrica, o tener más tiempo de latencia o déficit de conectividad.
- Las deslocalizaciones de personal y departamentos pueden llegar a ser difícil, especialmente si la ubicación original conserva sus segmentos de red. Reubicado equipo tendrá que ser reconfigurada basados en la nueva configuración de la red.

Una VLAN solución puede aliviar tanto de estos inconvenientes al permitir el mismo dominio de difusión para extender más allá de un único segmento.

Tipos de VLAN:

VLAN estáticas

Los puertos del switch están ya pre asignados a las estaciones de trabajo. Se configura por una cantidad “n” de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN.

Ventajas:

- Facilidad de movimientos y cambios
- Microsegmentación y reducción del dominio de Broadcast.
- Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones

Desventajas

- Administración: Un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que está conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

Puertos troncales

La comunicación que se hace entre switches para interconectar VLANs utiliza un proceso llamado Trunking. El protocolo VLAN Trunk Protocol (VTP) es el que utiliza para esta conexión, el VTP puede ser utilizado en todas las líneas de conexión, con versiones propietarias como ISL (CISCO), ATM LANE o versiones estandarizadas, IEEE 802.1Q y IEEE 802.3ad.

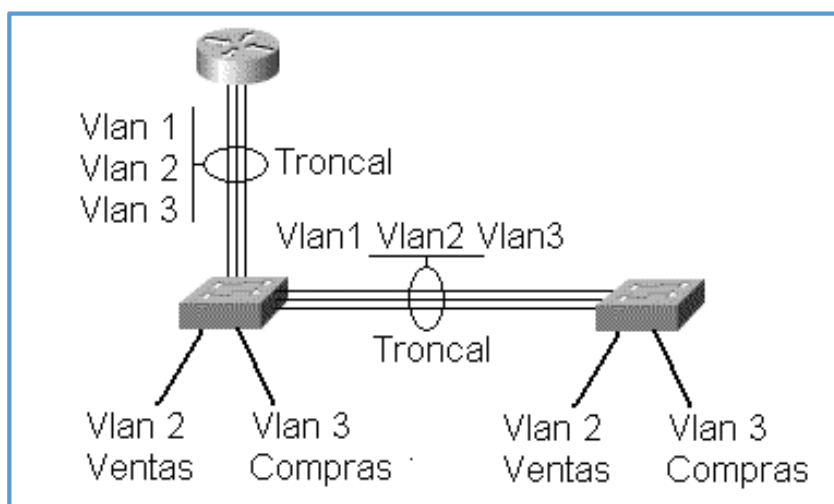


Ilustración 12: Puertos Troncales.

Fuente: <http://aprenderedes.com/wp-content/uploads/2007/02/troncal1.bmp>

Configuraciones de VLAN

La terminología utilizada entre los distintos fabricantes de hardware cuando se trata de VLANs. Debido a esto a menudo existe confusión en la aplicación del tiempo. Los siguientes son algunos detalles, y algunos ejemplos para ayudarle en la definición de VLANs para que su confusión no sea un problema.

Cisco VLAN terminología

Usted necesita algunos detalles para definir una VLAN en la mayoría de los equipos CISCO. Lamentablemente, debido a CISCO adquiere a veces las tecnologías que utilizan para llenar sus conmutación, enrutamiento y

seguridad de las líneas de productos, convenciones de nombres no siempre son coherentes.

Vlan ID – La VLAN ID es un valor exclusivo que asigne a cada VLAN en un único dispositivo.

Con el enrutamiento de CISCO o de conmutación dispositivo que ejecute IOS, su rango es de 1 – 4096. Al definir una VLAN que suelen utilizar la sintaxis “VLAN x” donde x es el número al que desea asignar a la VLAN ID. VLAN 1 está reservado como una VLAN 1 por defecto.

VLAN Nombre – El nombre de VLAN es un texto basado en el nombre que utiliza para identificar su VLAN, tal vez para ayudar al personal técnico en la comprensión de su función. La cadena de usar puede ser entre 1 y 32 caracteres de longitud.

Private VLAN – Cuando se configura una VLAN de CISCO como privada – VLAN, esto significa que los puertos que son miembros de la VLAN no pueden comunicarse directamente entre sí por defecto. Normalmente todos los puertos que son miembros de una VLAN pueden comunicarse directamente sí del mismo modo que sería capaz de haber sido miembro de un segmento de red estándar. VLANs privadas se crean para mejorar la seguridad en una red donde hosts que coexisten en la red no puede ni debe confiar en los demás. Esta es una práctica común de utilizar la Web en granjas o en entornos de alto riesgo, cuando la comunicación entre máquinas de la misma subred no es necesaria.

VLAN modos – en CISCO IOS, sólo hay dos modos de una interfaz puede operar en “modo de acceso” y “modo de troncal”. Modo de acceso es para fines dispositivos o aparatos que no requieren múltiples VLANs. El modo Troncal se utiliza el modo de transmitir múltiples VLANs a otros dispositivos de red, o para finales de los dispositivos que tienen necesidad de pertenencia a múltiples VLANs a la vez. Si se está preguntando qué modo utilizar, el modo es probablemente “el modo de acceso”

CISCO VLAN implementaciones

Al definir una VLAN en un dispositivo CISCO, usted necesita un VLAN ID, un nombre de VLAN, los puertos de miembros. En condiciones normales segmento de red en configuraciones de routers, interfaces individuales o grupos de interfaces (llamados canales) se asignan las direcciones IP.

Cuando usted usa VLANs, las interfaces son miembros de VLANs y no tienen direcciones IP individuales, y en general no tienen listas de acceso se aplica a ellos. Estas características son generalmente reservadas para las interfaces VLAN.” (Delgado Ortiz, Seguridad en Redes Inalámbricas, 2010)

4.3. Concepto y definiciones

❖ AAA:

En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: autenticación, autorización y contabilización (en inglés, Authentication, Authorization and Accounting). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

AAA se combina a veces con auditoria, convirtiéndose entonces en AAAA.
(Secur-IT @C.R.S., 2016)

❖ AP:

AP (Access Point traducido significa punto de acceso). Se trata de un dispositivo utilizado en redes inalámbricas de área local (WLAN - Wireless Local Area Network), una red local inalámbrica es aquella que cuenta con una interconexión de computadoras relativamente cercanas, sin necesidad de cables, estas redes funcionan a base de ondas de radio específicas. El Access Point entonces se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.
(InformaticaModerna, 2016)

❖ Ancho de Banda:

Bandwidth en inglés. Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información.

Se mide en millones de bits por segundo (Mbps). Una buena analogía es una autopista. Mientras más carriles tenga la calle, mayor cantidad de tráfico podrá transitar a mayores velocidades. El ancho de banda es un concepto muy parecido. Es la cantidad de información que puede transmitirse en una conexión durante una unidad de tiempo elegida. (web, 2016)

❖ Autenticación:

Proceso de identificación de un equipo o usuario. El estándar 802.11 define dos métodos de autenticación: open system y shared key. (GamaInternet, 2016)

❖ Clave de Encriptación:

Conjunto de caracteres que se utilizan para encriptar y desencriptar la información que se quiere mantener en privado. El tipo de clave y la forma de emplearla depende del algoritmo de encriptación que se utilice. (GamaInternet, 2016)

❖ Cliente, o dispositivo cliente:

Cualquier equipo conectado a una red y que solicita servicios (ficheros, impresión, etc.) de otro miembro de la red. (GamaInternet, 2016)

❖ Hot Spot:

También conocidos como lugares de acceso público, un Hot Spot es un lugar donde se puede acceder a una red Wireless pública, ya sea gratuita o de pago. Pueden estar en cibercafés, aeropuertos, centros de convenciones, hoteles, y otros lugares de encuentro, para proporcionar acceso a su red o a Internet a los visitantes o invitados. (GamaInternet, 2016)

❖ Intranet:

Red de área local de ordenadores en la que se aplican los métodos y tecnologías de Internet, como el protocolo TCP/IP. (Real Academia de Ingeniería, 2016)

❖ Linux:

Es un sistema operativo de software libre (no es propiedad de ninguna

persona o empresa), por ende no es necesario comprar una licencia para instalarlo y utilizarlo en un equipo informático. Es un sistema multitarea, multiusuario, compatible con UNIX, y proporciona una interfaz de comandos y una interfaz gráfica, que lo convierte en un sistema muy atractivo y con estupendas perspectivas de futuro. (Definición de Linux, 2016)

❖ QoS (Quality of Services):

Un conjunto de normas y mecanismos para la transmisión de datos de control de calidad. (Microsoft, 2016)

❖ SSID, Service Set Identification:

Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos Wireless se puedan comunicar, deber tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red Wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad. Dependiendo de si la red Wireless funciona en modo Ad-Hoc o en modo Infraestructura, el SSID se denomina ESSID o BSSID. (GamaInternet, 2016)

CAPITULO V: Desarrollo de la Propuesta

CAPÍTULO V: Desarrollo de la Propuesta

5.1. Recursos Humanos

La implementación del presente proyecto fue realizada por los siguientes colaboradores:

CARGO	NOMBRES	FUNCIÓN
Tesista	Osmar Ricardo Albuja Moreno	Desarrollar el Proyecto
Asesor Especialista	Roger Alarcón García	Asesorar durante el desarrollo del proyecto
Gerente de la Clínica Millenium	Víctor Loayza Carbajal	Identificar, evaluar, administrar la información solicitada para el desarrollo del proyecto

Tabla 4. Recursos Humanos

5.2. Metodología CISCO Top-Down Network Design

5.2.1. Fase I: Análisis de Negocios Objetivos y limitaciones

Datos Empresariales

- Rubro de la empresa: Salud Privada
- Razón Social: CLÍNICA MILLENIUM
- Fecha de Creación: 01 de marzo del año 1993
- Dirección: JR. Daniel A. Carrión N° 151 – Chiclayo
- Referente al cableado de red en la clínica, está implementada con cable de red categoría 5e en una topología estrella.
- Los dispositivos intermediarios de la red actual son: 01 Switch de 16 puertos básico, 01 Access Point TP-Link TL-WR743ND, 01 Access Point TP-Link TL-WA500G, 01 Modem ADLS Router convencional que ha sido reutilizado como un Access Point y 01 Modem ADSL Router convencional proporciona el servicio de Internet, otorgado por el IPS.
- El servicio de internet se trata de una línea ADSL de velocidad 4 Mbps y el ISP actualmente es movistar.

La clínica, debido al raudo avance tecnológico y la mejora continua en la telecomunicación, se ve obligada a optar por tecnología como fuente de desarrollo, considerando los sistemas de seguridad que protegen a las empresas.

Actualmente la clínica, necesita de una red de datos que funcione de manera cabal e ininterrumpida con acceso a datos dentro de la misma como a internet. Por estos motivos el diseño propuesto tiene una lista de objetivos que afectará al diseño de la red:

- Crear relaciones y accesos de información a un nuevo nivel, como fundamento para un modelo organizacional de red.
- Ofrecer nuevos servicios a los usuarios
- Obtener más ventajas competitivas frente a otras organizaciones que tienen el mismo rubro de negocio.

Análisis de los Objetivos y Limitaciones Técnicas

Teniendo en consideración que la Clínica posee una red inestable pues no se realizado una implementación de cableado estructurado anteriormente, los equipos de cómputo no están configurados correctamente a lo que nivel de seguridad se refiere, se sugiere el siguiente análisis.

Confidencialidad

Protección de la información ante interceptaciones no autorizadas

Facilidad de Uso

El acceso es sencillo y fácil, los usuarios podrán acceder en todo momento según los permisos otorgados respectivamente.

Adaptabilidad

Indicará si el diseño es flexible, y puede ser adaptado ante algún cambio pues las tecnologías y sistemas de información mejoran velozmente.

Caracterizar y Graficar la red Existente

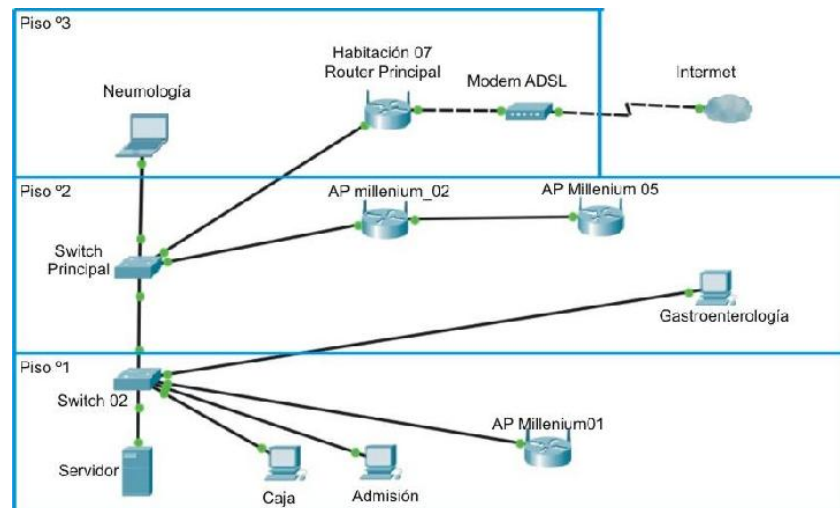


Ilustración 13: Esquema de la Red Actual de la Clínica. Millenium (Propia, 2016)

Según lo mostrado en la ilustración 1, uno de los principales inconvenientes es que hay estructura de red inadecuada, El router principal actualmente se localiza en una habitación donde entra clientes internos y externos de la Clínica, el switch principal se encuentra en un área donde Médicos atienden según sus agendas correspondientes. A partir del esquema podemos concluir que: Hay una interconexión entre las áreas que no es la más idónea pues se aprecia que el Router principal se encuentra en un área dónde ingresa personal no autorizado y aumenta el riesgo de alguna manipulación y pérdida de información de la Clínica, robo del dispositivo físico, ocasionando pérdida de la conexión a internet, fallos en la red y desconexión de la misma.

Direccionamiento IP actual

La clínica actualmente está compuesta por una sola red 192.168.1.0 – (Clase C) con máscara /24 y la distribución es mediante DHCP a excepción de:

Nº	ÁREA	DIRECCIÓN IP	MÁSCARA DE SUBRED
1	Servidor	192.168.1.10	255.255.255.0
2	Admisión	192.168.1.16	255.255.255.0
3	Neumología	192.168.1.11	255.255.255.0
4	Gastroenterología	192.168.1.33	255.255.255.0
5	Traumatología	192.168.1.35	255.255.255.0
6	Farmacia	192.168.1.34	255.255.255.0

Tabla 5: Direcciones IP actuales.

Se hace mención que, en el caso de áreas como Gastroenterología y Neumología los usuarios poseen equipos de cómputo personales (Laptops) y no se cuentan como parte de la institución.

Descripción Física de los Equipos que usan en la Clínica

La Clínica cuenta con 07 equipos de cómputo, impresoras 2. A continuación, presentamos la siguiente tabla con las computadoras existentes.

ÁREA	Nº PC'S	PROCESADOR	FUNCIÓN
Admisión	01	Intel Corei3 2.6 GHz	Registrar citas médicas, informe de los servicios médicos y consultar los horarios de doctores.
Farmacia	01	Intel Corei3 2.6 GHz	Registro y pago de consultas, productos y servicios médicos.
Gastroenterología	01	Intel Core2Duo 2.53 GHz	Consultorio de Médico Gastroenterólogo
Traumatología	01	Intel Corei3 2.6	Consultorio de Médico Traumatólogo
Servidor	01	POWER7	Administrar y controlar los servicios informáticos de la clínica

Tabla 6: Computadores existentes en la Clínica.

ÁREA	Nº IMPRESORAS	MODELO
Admisión	01	EPSON-L355
Farmacia	01	EPSON-LX 350

Tabla 7: Impresoras existentes en la Clínica

Diseñando una topología lógica aumentaremos la probabilidad de encontrar objetivos de un cliente para escalabilidad, adaptabilidad e interpretación.

5.2.2. Fase II: Análisis de datos y Requisitos

a. Análisis y selección de las herramientas para la autenticación

1. PROTOCOLO DE AUTENTICACIÓN

PROTOCOLOS DE AUTENTICACIÓN			
	RADIUS	TACACS	DIAMENTER
Descripción	Desarrollado para permitir el despliegue de acceso por servicios dial-up (PPP), soporta los servicios NAS	Propietario y desarrollado por Cisco. Provee un punto control centralizado para la autenticación	Su soporte sólo se especifica para Accounting.
Características	Autentica y autoriza para transferir datos de configuración entre dos servidores. Su uso principal es para acceder a la red.	Separa la autenticación y autorización. Uso primario es de administración de la red.	Se utiliza de la mano con una aplicación DMT, cada aplicación depende del protocolo base sobre el servidor para acceder a la red.

Tabla 8: Protocolos de autenticación

Se escogerá el protocolo RADIUS pues se adapta a las exigencias de la red de clínica, permite llevar el control al acceso, generando confiabilidad y mayor seguridad. Aumenta la productividad y soporta los nuevos avances multimediales.

2. BASE DE DATOS

SERVIDOR DE BASE DE DATOS			
	LDAP	MYSQL	PostgreSQL
Descripción	<p>Un servidor LDAP es utilizado para procesar consultas y actualizaciones a un directorio de información LDAP.</p> <p>Un directorio de información LDAP es un tipo de base de datos, pero no es una base de datos relacional.</p>	<p>Es un sistema de gestión de bases de datos relacional, sin embargo carece de elementos considerados esenciales tales como integridad referencial y transacciones.</p>	<p>Es un Sistema de gestión de bases de datos relacional orientado a objetos y libre.</p>
Características	<ul style="list-style-type: none"> • Rápido en la lectura de registros muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente. • Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas • La mayoría de aplicaciones disponen de soporte para LDAP 	<ul style="list-style-type: none"> • Amplio subconjunto del lenguaje SQL. Algunas extensiones son incluidas igualmente. • Disponibilidad en gran cantidad de plataformas y sistemas. • Tradicionalmente en aplicaciones web de lectura mayormente, usualmente escritas en PHP, donde la principal preocupación es la optimización de consultas sencillas. 	<ul style="list-style-type: none"> • Permite que mientras un proceso escribe en una tabla, otros accedan a la misma tabla sin necesidad de bloqueos. • Posee excelentes funciones con las que puedes indexar elementos y hacer búsquedas avanzadas en formato JSON.

Tabla 9: Servidor de Base de Datos

Debido a que el proyecto está enfocado a fortalecer el acceso a la red de la clínica, LDAP cumple los requisitos para estar dentro de la arquitectura AAA. Será usado para fortalecer el proceso de autenticación que en este caso será con RADIUS.

LDAP es considerada como una base de datos y está basado en directorios pues son conjuntos de objetos con atributos organizados en una manera lógica y jerárquica.

Realiza operaciones de lectura muy rápidas, esto se debe a la naturaleza de los datos almacenados en los directorios, las lecturas son más comunes que las escrituras.

3. FIREWALL

FIREWALL			
	CISCO	HP	PANDA SECURITY
Descripción	Proporcionan la visibilidad de red necesaria, alta protección contra amenazas y malware avanzado y mayor automatización para reducir costos y complejidad.	Permite una protección de red escalable, incluye tecnologías GRE, L2PT.	El objetivo del Firewall perimetral Panda es impedir que se realicen conexiones entre la red corporativa e Internet que estén fuera de la política de seguridad de la compañía.
Características	<ul style="list-style-type: none"> • Visibilidad contra granulares • Sistema de prevención de intrusiones (IPS) • Protección contra malware avanzado 	<ul style="list-style-type: none"> • Firewall virtual avanzado • Protección de seguridad comprehensiva. 	<ul style="list-style-type: none"> • Protección contra intrusos • Bloqueos • Definición de reglas

Tabla 10. Firewall o Cortafuegos

Para complementar la seguridad en la red se elegirá un firewall CISCO. Permitirá equilibrar la eficacia de la seguridad con la productividad. Con esta solución la red de la clínica reforzará el monitoreo de seguridad y estará previendo amenazas avanzadas tales como malwares.

c. Softwares para la simulación del control de acceso a la red.

En la siguiente tabla se mencionan los softwares para la simulación del control de acceso a la red:

SOFTWARE	DESCRIPCIÓN
VMWare Workstation versión 10	Software de virtualización
Ubuntu Server versión 14.04 TLS	Sistema operativo en Linux para el uso de servidores.
FreeRADIUS	Servidor que usa protocolos de autenticación y autorización para aplicaciones de acceso a la red o movilidad
SLADP	Servidor de directorio LDAP que se ejecuta en distintas plataformas.

Packet Tracer versión 7	Potente programa de simulación de red para describir conceptos técnicos y diseño de sistemas de redes.
JXplorer	Navegador LDAP de código abierto. Se trata de un cliente compatible con las normas de uso general LDAP que se puede utilizar para leer y buscar en un directorio LDAP. JXplorer es una pieza completamente funcional del software con la integración de avanzados niveles de seguridad (en este caso RADIUS) y apoya a las partes más difíciles del protocolo LDAP.
SecureW2	Es un programa que permite conectarse mediante la autenticación TTLS PAP para Windows. Se instalan en las laptops que se conectarán a la red inalámbrica, nos permitirá conectarnos al servidores integrados RADIUS-LDAP mediante un usuario y contraseña.
Plug-in PGINA	PGINA es un plug-in para LDAP que proporciona servicios utilizando un servidor LDAP como la fuente primaria de datos. Proporciona soporte para el cifrado SSL y la conmutación por error a uno o más servidores alternativos.

Tabla 11: Infraestructura para la simulación del control de acceso

Para simular la integración de los servidores RADIUS-LDAP se instaló una máquina virtual configurada con Sistema Operativo Ubuntu Server 14.04 TLS en Linux, la instalación se explica en el anexo 1 y las configuraciones se las máquinas virtuales en los anexos 2 y 3 correspondientemente.

5.2.3. Fase III: Diseño de la solución

1. Diseño Físico Propuesto de la arquitectura de red

1.1. Centro de datos

Ubicación

Se ha previsto que el centro de datos se ubicará en la cuarta planta de la clínica; lugar amplio y seguro para la administración de la red telemática. Se cumplen las normas ANSI/TIA 942.

Estructura

El espacio físico propuesto del Centro de Datos de la clínica tendrá un espacio de 2.44 metros de largo, 4.10 metros de ancho, 3 metros de altura

dónde se almacenarán los equipos de red, rack de telecomunicaciones, sistema de electricidad, etc.

Sistema de Puesta a Tierra






Este sistema consiste en realizar una conexión eléctrica intencional con el sistema físico al suelo.

Las definiciones están establecidas de acuerdo a las normas IEEE Std. 81-1983, ASTM G57-06 y EIA/TIA 607.

Se colocará una barra de conexión a tierra TGB que refiere al sistema de puesta a tierra.

- Cada equipo o gabinete ubicado en dicha sala debe tener su TGB montada en la parte superior trasera.
- El conductor que une el TGB con el TBB debe ser cable 6 AWG.
- Además, se debe procurar que este tramo sea lo más recto y corto posible.
- Hecha de cobre y sus dimensiones mínimas 6 mm. de espesor y 50 mm. de ancho. Su longitud puede variar, de acuerdo a la cantidad de cables que deban conectarse a ella y de las futuras conexiones que tendrá.
- Aislada mediante aisladores poliméricos (h=50 mm mínimo)

Elementos a considerar en el centro de datos:

<p>Gabinete de red</p>	 <p><i>Ilustración 14: Gabinete de red.</i> Fuente: http://www.satranet.com/satra/images/gabinetes1.jpg</p>
<p>Sistema de aire acondicionado</p>	 <p><i>Ilustración 15: Aire de Expansión Directa.</i> Fuente: http://www.apc.com/resource/images/salestools/500/Front_Left/2BAF4ED4F3308DF885257B0C0055F79B_SLIE_94QLLQ_f_v_500x500.jpg</p>
<p>Extintor</p>	 <p><i>Ilustración 16: Extintor ABC.</i> Fuente: http://fotos.infoinfo.com.pe/extintores_peru/136568_12319</p>
<p>Sistema de alimentación ininterrumpida (UPS)</p>	 <p><i>Ilustración 17: UPS.</i> Fuente: https://www.bhphotovideo.com/images/images1000x1000/APC_smc1500_Smart_UPS_C_1500VA_with_887781.jpg</p>
<p>Equipo de distribución de energía (PDU)</p>	 <p><i>Ilustración 18: PDU de 12 receptáculos.</i> Fuente: http://www.leviton.com/OA_HTML/ibcGetAttachment.jsp?cltemId=ltbY6ihObCqVw4zmwszVOA</p>

1.2. Diseño del Centro de Datos

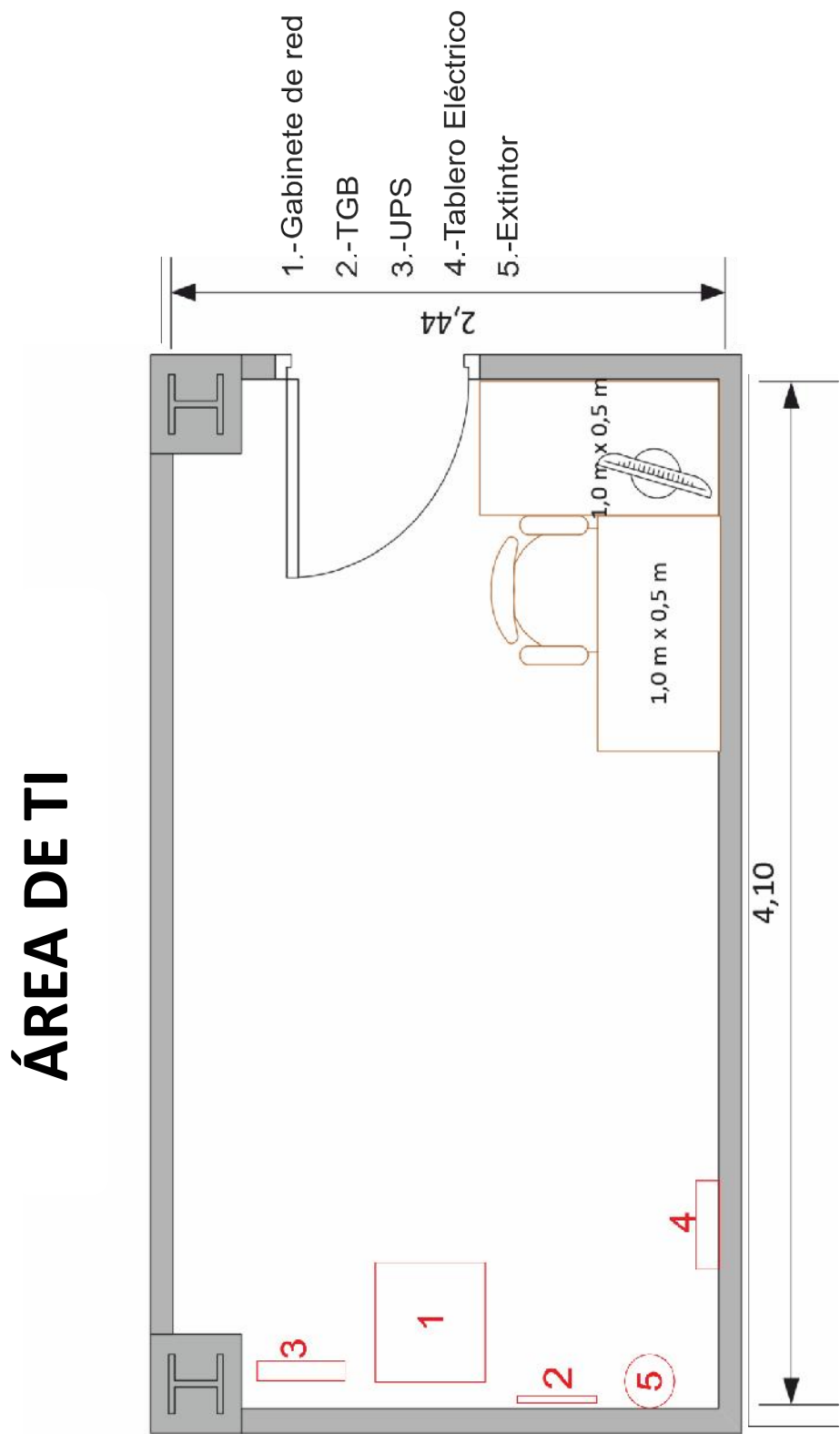


Ilustración 19: Diseño del centro de datos propuesto.

1.3. Reestructuración de Cableado

Para la propuesta se solicitó autorización para hacer las mediciones de todas los ambientes que posee la clínica y así esclarecer las necesidades que se pretenden cubrir.

La clínica no cumple con las especificaciones adecuadas ni dispositivos intermediarios para una red estable.

A partir de ello creamos un plano del edificio, y determinamos la ubicación de las áreas de trabajo las cuáles se muestran en las ilustraciones 21, 22, 23 y 24.

Adicionalmente se diseña la localización de los dispositivos intermediarios, puntos de datos, punto de toma corriente para los equipos de cómputo.

Por lo tanto, para el óptimo funcionamiento de la integración de los servidores RADIUS-LDAP se rediseñará la red cumpliendo con los estándares correspondientes.

1.3.1. Reglas para el etiquetado

La información del rotulado se debe presentar en etiquetas individuales, adhesivas y autolaminadas.

Los extremos de cada cable y las rosetas o conectores a los que llegan irán timbrados con un código único, uniforme e inequívoco que incluirá el número del armario, la planta, el número del conjunto de rosetas y número del conector, separados por guiones. El etiquetado será idéntico en ambos extremos del cable.



Ilustración 20: Ejemplo de etiquetado de red.

Fuente:http://megaenlinea.com/html/product_images/uploaded_images/idxpert-utp-1.jpg

Simbología:

Px: Planta Número “x”

Ax: Área “x”

Bkx: Backbone de planta “x”

CTx: Caja de Comunicaciones “x”

PRIMERA PLANTA	
Área	Nomenclatura de etiquetado
Switch	BK1 – CT1 – P1
Farmacia	P1 – A1-D1
	P1 – A1-D2
Admisión	P1 – A2-D3
	P1 – A2-D4
Access Point	P1- BK1-AP1
SEGUNDA PLANTA	
Área	Nomenclatura de etiquetado
Switch	BK2 – CT1 – P2
Access Point	P2- BK2 – AP2
TERCERA PLANTA	
Área	Nomenclatura de etiquetado
Switch	BK3 – CT1 – P3
Access Point	P3 – BK3 – AP3
CUARTA PLANTA	
Área	Nomenclatura de etiquetado
Switch	BK4 – CT1 – P4
Sistemas	P4 – A3 – D5
	P4 – A3 – D6

	P4 – A3 – D7
Gerente	P4 – A4 – D8
	P4 – A4 – D9
Reuniones	P4 – A5 – D10
Administrador	P4 – A6 – D11
	P4 – A6 – D12
	P4 – A6 – D13
Secretaria	P4 – A7 – D14
	P4 – A7 – D15
	P4 – A7 – D16

Tabla 12: Etiquetado de red.

1.3.2. Cableado horizontal:

Para aplicar la norma ANSI/TIA/EIA-569-A de recorridos y espacios de telecomunicaciones en edificios comerciales sobre cómo enrutar el cableado se propone considerar los siguientes “puntos de red” para el caso de los equipos de cómputo y puntos para los Access points distribuidos en las cuatro plantas de la clínica. El tipo de cable propuesto es UTP categoría 6.

PRIMERA PLANTA		
Área	Cantidad de Puntos de red	Cable UTP (metros)
Farmacia	02	58
Admisión	02	15
Access Point	01	01
Subtotal	05	74
SEGUNDA PLANTA		
Área	Cantidad de Puntos de red	Cable UTP (metros)
Access Point	01	01
Subtotal	01	01

TERCERA PLANTA		
Área	Cantidad de Puntos de red	Cable UTP (metros)
Access Point	01	1
Subtotal	06	1
CUARTA PLANTA		
Área	Cantidad de Puntos de red	Cable UTP (metros.)
Reuniones	01	9
Gerente	02	20
Sistemas	03	39
Administrador	03	100
Secretaria	03	60
Subtotal	12	227
Total	24	303

Tabla 13: Puntos de datos para equipos y dispositivos intermediarios.

1.3.3. Cableado vertical (Backbone)

Prosiguiendo con la normativa de cableado estructurado, se expone los siguientes “puntos de red” para el caso de los switches distribuidos en las cuatro plantas de la clínica los cuales proporcionarán interconexión al cuarto de telecomunicaciones. El tipo de cable propuesto es UTP categoría 6.

PRIMERA PLANTA		
Área	Cantidad de Puntos de red	Cable UTP (metros)
Switch Primera Planta	01	30
SEGUNDA PLANTA		
Área	Cantidad de Puntos de red	Cable UTP (metros)
Switch Segunda Planta	01	25
TERCERA PLANTA		
Área	Cantidad de Puntos de red	Cable UTP (metros)
Switch Tercera Planta	01	20
CUARTA PLANTA		
Área	Cantidad de Puntos de red	Cable UTP (metros.)

Switch Cuarta Planta	01	10
Total	04	85

Tabla 14: Puntos de dato de cableado backbone.

1.3.4. Diseño del Cableado Estructurado de la Clínica

En el siguiente diseño se detallan la ubicación de los puntos de datos para la conexión de todas las áreas de la clínica.

Se ha considerado colocar un switch por cada piso y anclado en la parte superior del pasillo tal como se muestran en las figuras 21, 22, 23, 24 debido a que actualmente todos los ambientes de la clínica son cuartos para pacientes, consultorios y centro de operaciones médicas.

El total de puntos de red estimados es de 28 y la cantidad aproximada en cable UTP es de 303 metros en cableado Horizontal y 85 metros en Backbone, resultando un total de 390 metros.

El cableado horizontal se realizará de una sola tirada entre la toma de telecomunicaciones y el Switch de acceso de la planta que se encuentre, la finalidad es evitar empalmes y puntos de transición.

Planos de la Primera Planta

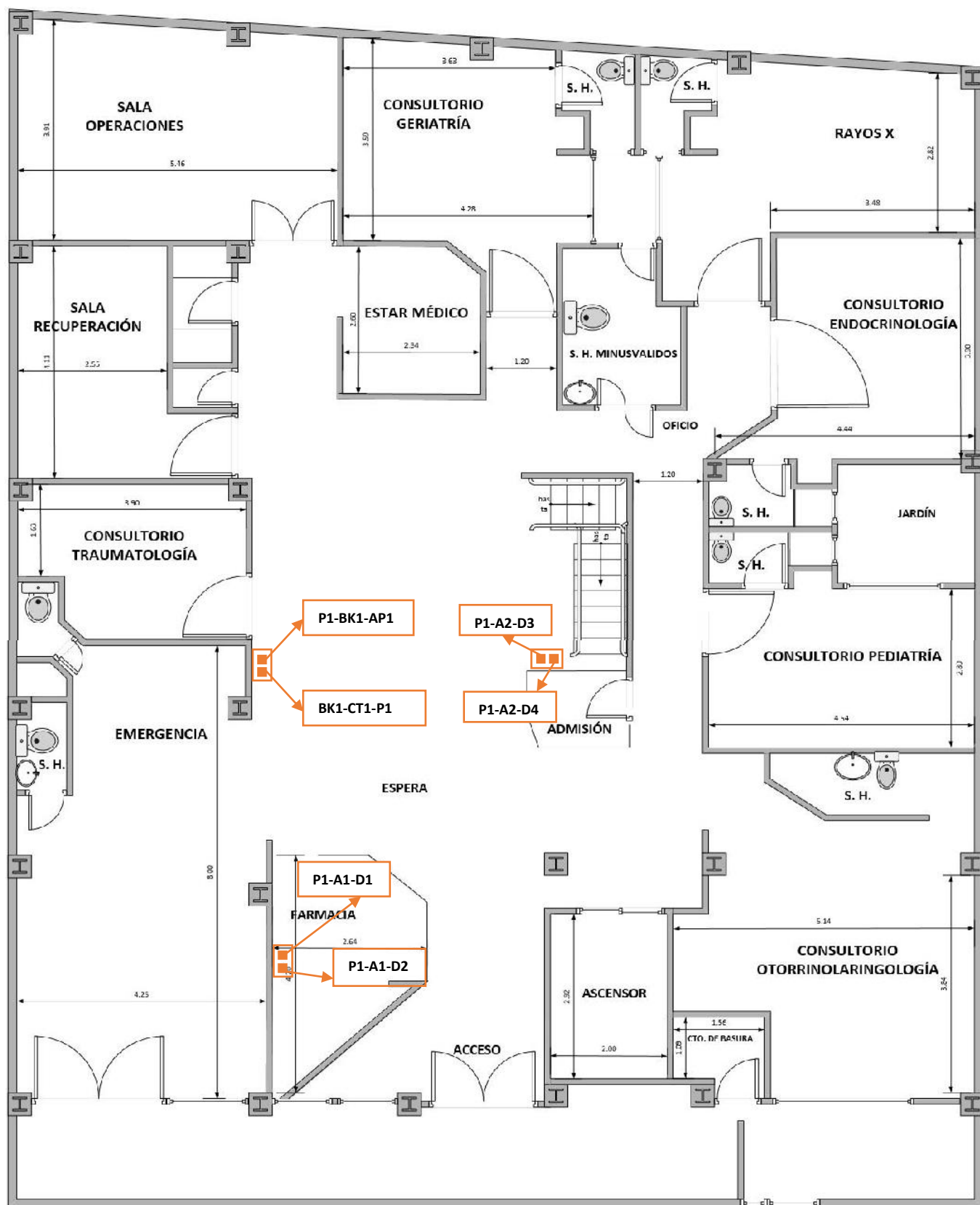


Ilustración 21: Plano Primera Planta.

Planos de la Segunda Planta

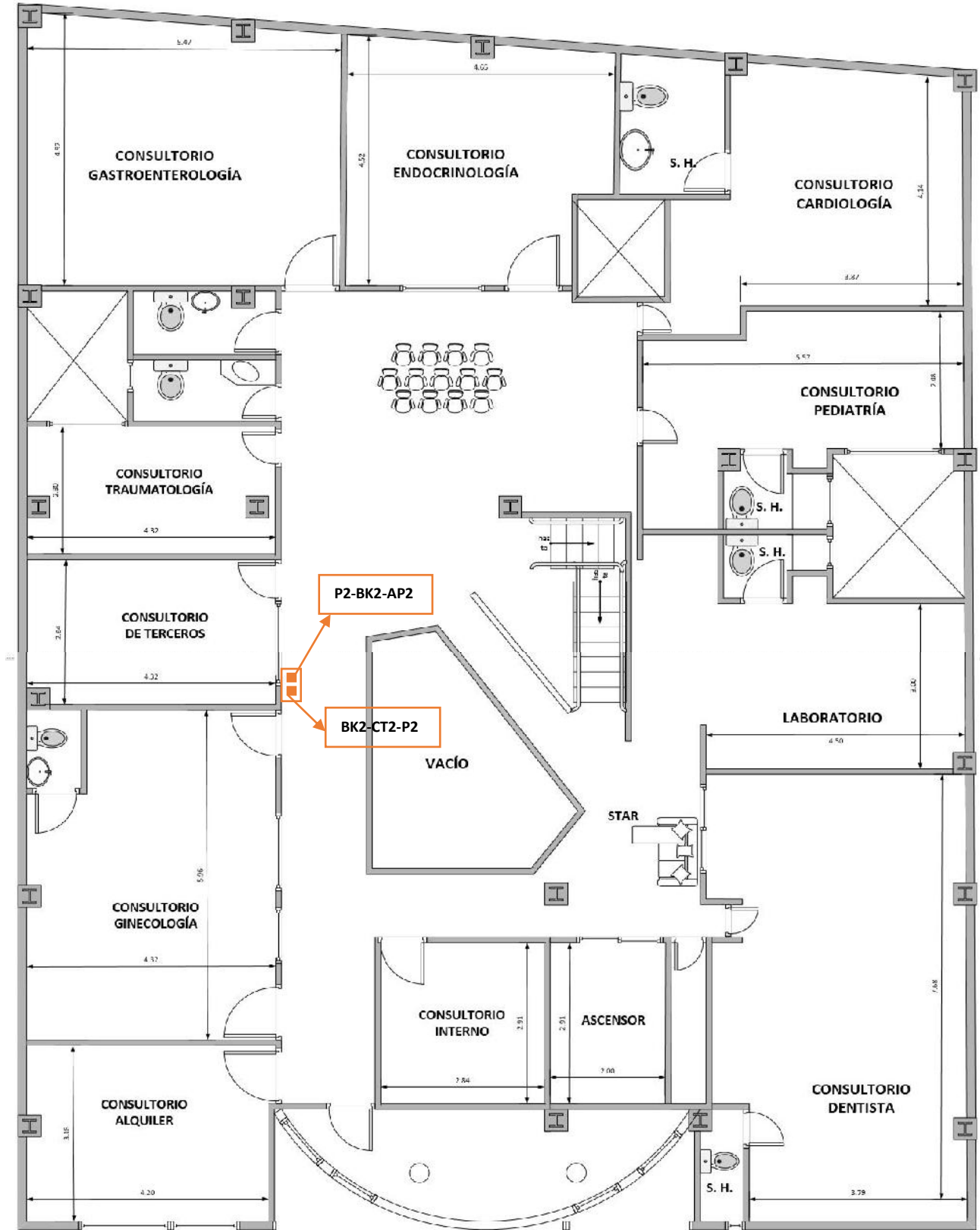


Ilustración 22: Plano Segunda Planta.

Planos de la Tercera Planta

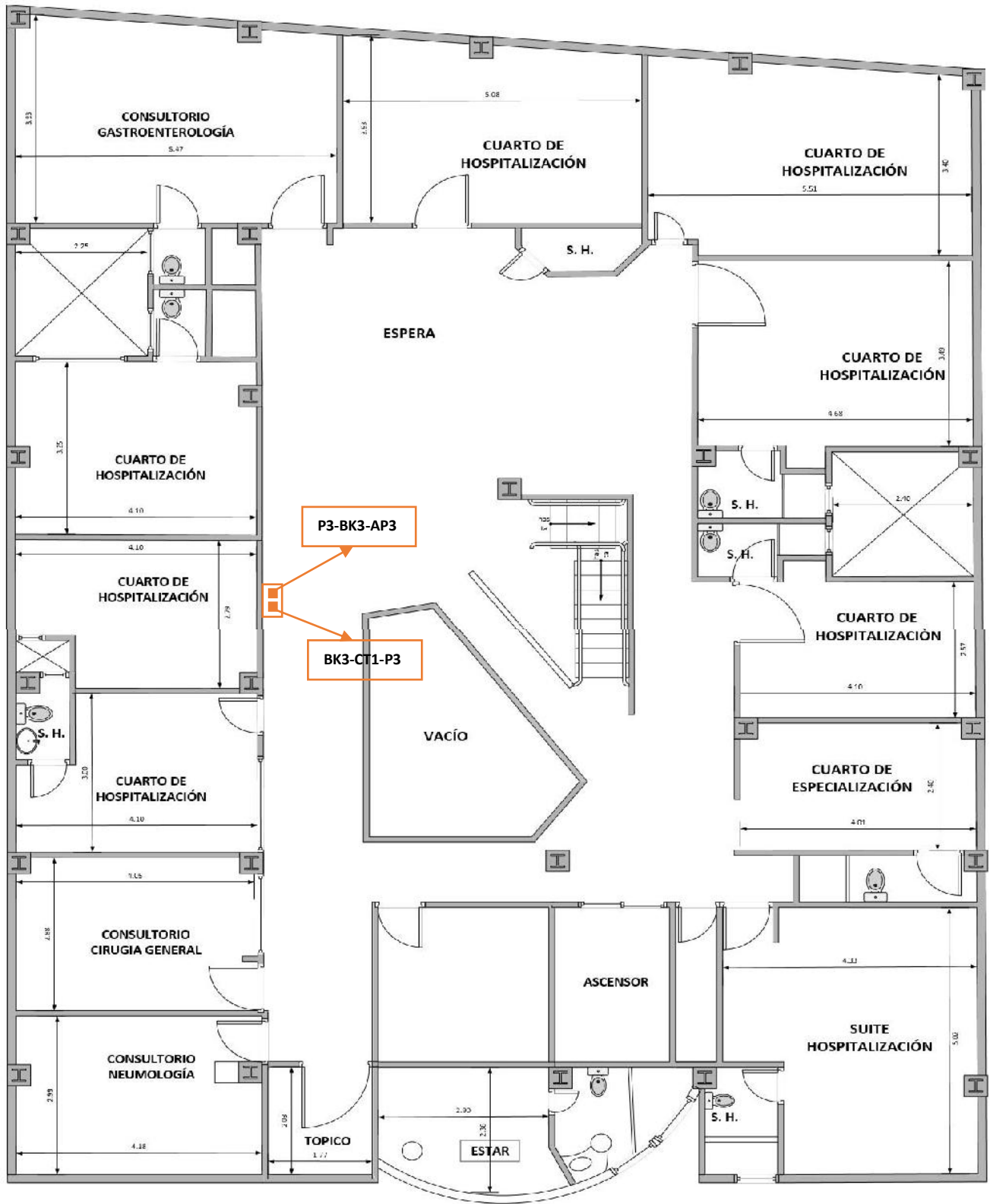


Ilustración 23: Plano Tercera Planta.

Planos de la Cuarta Planta

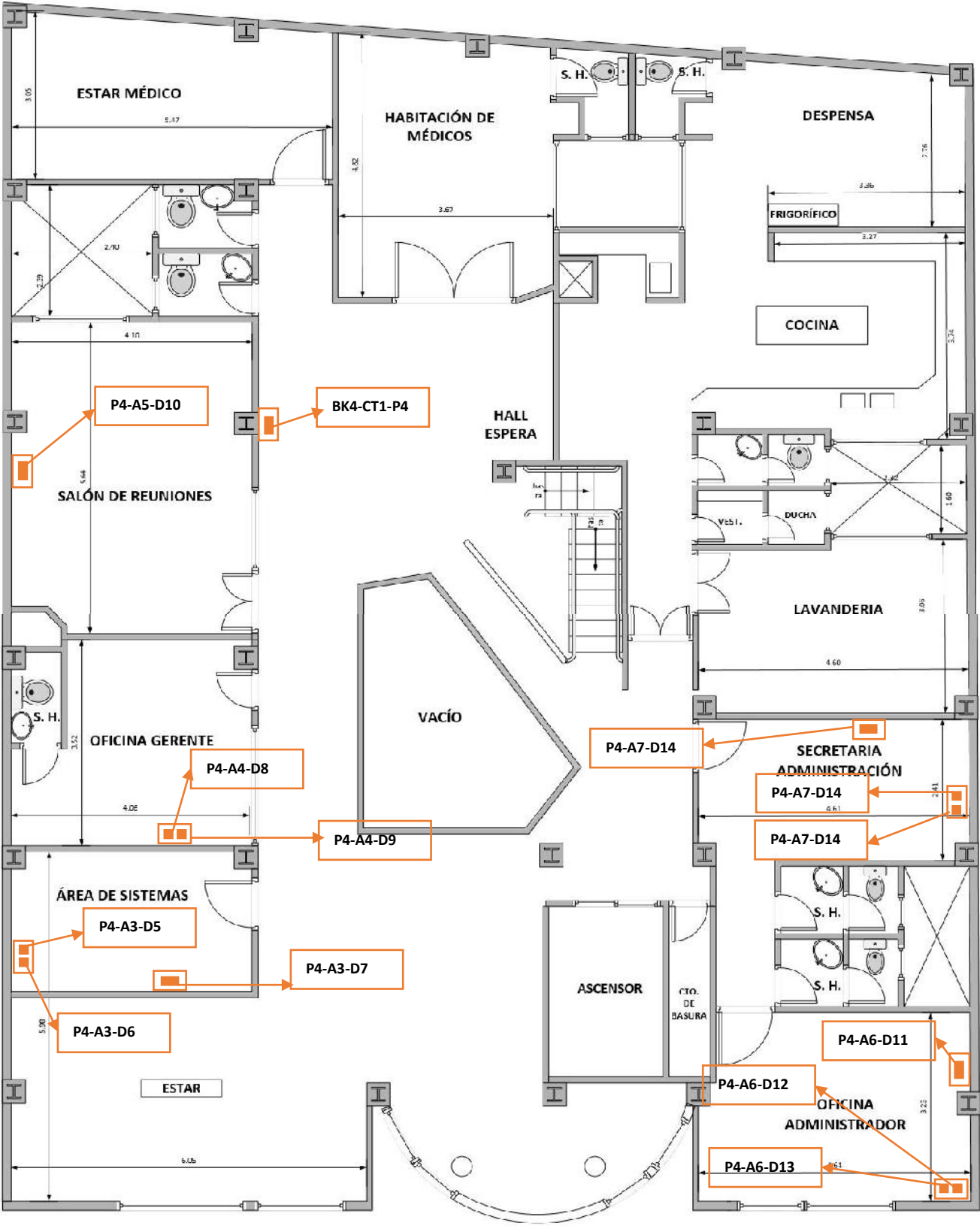
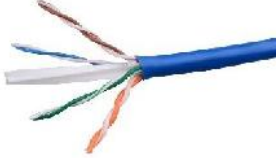





Ilustración 24: Plano Cuarta Planta.

Las tomas de telecomunicaciones estarán implementadas por:

<p>Cable UTP Categoría 6</p>	 <p><i>Ilustración 25: Cable categoría 6a.</i> Fuente: http://www.computadoresbogota.com/articulos/activos/imagenes/Powest_-_Cable_Cat_6A.jpg</p>
<p>Rosetas (caja toma datos):</p>	 <p><i>Ilustración 26: Roseta doble.</i> Fuente: http://imagen.xtremmedia.com/A029037_0_1.jpeg</p>
<p>Conectores RJ-45 Hembra</p>	 <p><i>Ilustración 27: Conector RJ-45 Hembra.</i> Fuente: https://img.pccomponentes.com/articles/4/48306/digitus-keystone-jack-rj45-hembra-cat-6-1.jpg</p>
<p>Conectores RJ-45 Macho</p>	 <p><i>Ilustración 28: Conector RJ-45 Macho.</i> Fuente: http://3.bp.blogspot.com/-oymYczf7x4U/T0JTKu5uf8I/AAAAAAAAAeM/PIZOB4QfsEY/s1600/Konektor+RJ45.jpg</p>

Se aplica también la norma ANSI/TIA/EIA-606-A pues es vital para el buen funcionamiento de su cableado estructurado de la clínica, ya que habla sobre la identificación de cada uno de los subsistemas basado en etiquetas, códigos y colores, con la finalidad de que se puedan identificar cada uno de los servicios

que en algún momento se tengan que habilitar o deshabilitar. Esto es muy importante, ya que en la documentación que se debe entregar al usuario final, la norma dice que se tendrá que especificar la forma en que está distribuida la red, por dónde viaja, qué puntos conecta.

El Programa de Sistemas de Marcación y Etiquetado evalúa el rendimiento físico de las etiquetas tomando en cuenta los requisitos de la norma ANSI/UL 969, que es la norma de seguridad de los sistemas de marcación y etiquetado.

2. Diseño Lógico Propuesto de la arquitectura de red

El siguiente informe detalla el diseño del sistema de seguridad

a) El usuario de la clínica inicia la autenticación PPP, acontecimiento realizado en el nivel de enlace de datos, segunda capa del modelo OSI, es el responsable de establecer una conexión directa entre el usuario y el Access point “APx” de configuración RADIUS, el cual realiza la labor de dispositivo intermediario.

a) Usuario:

- La selección e identificación de la red inalámbrica está bajo el protocolo 802.1X
- Envía el nombre de usuario y la contraseña encriptada al cliente RADIUS.
- Espera la respuesta del cliente RADIUS, esta procederá dependiendo de los parámetros de servicios agrupados con Aceptar o Rechazar.
- Si la solicitud es aceptada, el cliente RADIUS le proporciona una dirección IP que le permitirá ingresar a la red de la clínica.

El NAS para la red inalámbrica será el Access point. Este pedirá que ingrese el nombre de usuario y la contraseña (en caso de Protocolo de autenticación de contraseña PAP)

b) Access Point:

- Funciona como NAS (Servidor de Acceso a la red), como un cliente para el servidor RADIUS – LDAP.
- Se activa el servicio de autenticación mediante RADIUS.
- Se registra la dirección IP del servidor RADIUS – LDAP. Evento realizado en el nivel de Red, tercera capa del modelo OSI. Proporcionará la conectividad.
- Se activa el sistema de seguridad WPA-WPA2 para reforzar la seguridad de la red inalámbrica. Este utiliza un algoritmo de encriptación de cifrado AES (Estándar de encriptación avanzada).
- Se ingresa la clave compartida (Shared Secret) para la conexión con el servidor RADIUS – LDAP desde este dispositivo. Esta clave no se envía nunca a través de la red. Actividad indispensable para que el cliente RADIUS inicie la comunicación con el servidor RADIUS – LDAP.
- El tipo de conexión se realiza mediante el protocolo PAP, subprotocolo usado por la autenticación del protocolo PPP, validando el acceso al sistema y a los recursos del servidor RADIUS – LDAP. Los paquetes RADIUS son “encapsulados” dentro del campo de datos de UDP en el puerto 1812. Evento realizado en el nivel de Transporte, cuarta capa del modelo OSI.
- Si es la solicitud es aceptada, éste asignará una dirección IP al usuario otorgando el ingreso a la red de la clínica. Caso contrario envía un mensaje de fallo en la autenticación.

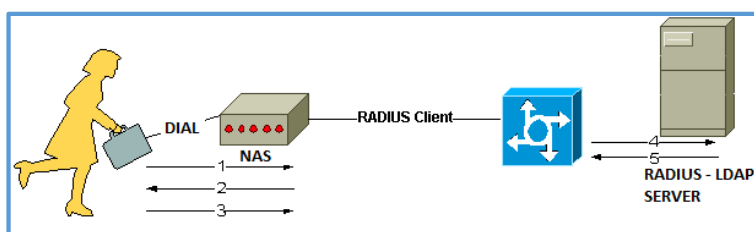


Ilustración 29. Interacción entre usuario, cliente RADIUS y servidor RADIUS-LDAP.

c) Servidor LDAP

Al finalizar la instalación de manera automática, debemos actualizar la configuración por defecto con los siguientes parámetros:

CONFIGURACIÓN	DESCRIPCIÓN
Contraseña administrador	admin123admin
Nombre de dominio DNS	millenium.com
Nombre de la Organización	Millenium
Motor de base de datos	HDB
Protocolo LDAPv2	Desactivado

Tabla 15. Configuraciones Servidor LDAP

El protocolo LDAPv2 se desactiva pues actualmente se cuenta con el protocolo LDAPv3 (RFC 2251), éste aborda algunas de las limitaciones de LDAPv2 y permite agregar funciones al protocolo sin requerir cambios en el protocolo.

Las configuraciones del servidor se aprecian desde la ilustración 33 hasta la 43.

d) Servidor DNS

Para la implementación del servicio DNS en el dominio, se habilitó el rol de servidor DNS en el equipo servidor a través de la consola de administración del servidor, incluida en el servidor LDAP.

LDAP maneja un servidor DNS de tipo primario local, lo utiliza como BIND, de tal forma LDAP funciona como backend.

Una vez instalado el servidor, se estableció el nombre de dominio DNS, se utiliza para construir el DN base del directorio LDAP:

millenium.com

e) Servidor RADIUS

Se realizó la siguiente configuración:

CONFIGURACIÓN PARA EL NAS	DESCRIPCIÓN
Asignación de IP	192.168.1.1
Secretname	admin123admin
Shortname	Apradius

Tabla 16. Configuración NAS

CONFIGURACIÓN PARA HABILITAR LA AUTENTICACIÓN MEDIANTE LDAP	DESCRIPCIÓN
Default_eap_type	peap
Puerto	1812
Asignación IP servidor (server)	192.168.1.200
Identity	cn=admin,dc=millenium,dc=com
Contraseña	admin123admin
Basedn	dc=millenium,dc=com

Tabla 17. Configuración para habilitar la autenticación mediante LDAP

- **Server:** Nombre del servicio LDAP o alternativamente la IP donde se encuentra el servidor.
- **Identity:** Se refiere al usuario con privilegios de administrador o globales en el servidor LDAP y dominio de búsqueda.
- **Password:** Contraseña del usuario con privilegios de administrador.
- **basedn:** Es la ruta donde se busca el usuario en el servidor LDAP

Desde la ilustración 44 hasta la 62 se detalla la configuración señalada.

f) Grupos y Usuarios en el servidor LDAP

Realizada la integración de los servidores RADIUS-LDAP, ya podemos crear los grupos y usuarios que tendrán el acceso correspondiente a la red. Para tal labor, se cargarán unas plantillas con formato *ldif*, las cuales contienen los registros de los grupos y posteriormente los usuarios, asignándoles un grupo ya existente.

Primero se carga la plantilla con los grupos organizativos, que comprenden:

GRUPO ORGANIZATIVO
Sistema
Administrativos
Doctores

Tabla 18. Grupos Organizativos

- Sistema: Usuarios encargados de la administración de la red telemática de la clínica, servidores.
- Administrativos: Usuarios que utilizan el servidor para los registros de consulta médica, venta de medicamentos.
- Doctores: Usuarios que pertenecen al área médica y ofrecen sus servicios.

Para el registro de usuarios se consideró lo siguientes parámetros:

- Como regla base no se usarán datos que se asocien a la persona. Jamás incluir los nombres propios ni de familiares, tampoco poner números que tengan que ver con la persona, como año de nacimiento, terminación de teléfono, dirección o fechas.
- La contraseña debe tener un mínimo de 8 caracteres
- La primera letra hace referencia al grupo organizacional donde se encuentra
- La segunda letra se obtiene concatenando la primera letra del nombre del usuario
- Finalmente se añade el primer apellido del usuario.
- Se utilizará en una misma contraseña dígitos, letras y caracteres especiales.
- Se alternarán las letras aleatoriamente mayúsculas y minúsculas.

USUARIO	CONTRASEÑA
Screyes	c351c4F1
Avloayza	v003v75J
Avhidalgo	h923h01P
Dssuarez	d461d88R
Dplopez	p571p96L

Tabla 19. Usuario LDAP

El registro mediante plantillas LDIF de los grupos y usuarios de la Clínica se estima desde la ilustración 63 hasta la 67.

g) Servidores integrados RADIUS – LDAP

El servidor RADIUS – LDAP recibe las solicitudes de autenticación de los usuarios, la autenticación del usuario, y luego regresar toda la información de configuración necesaria para el cliente para conceder el servicio al usuario (eventos realizados en la capa de Transporte, cuarta capa del modelo OSI). Cuando el servidor RADIUS – LDAP recibe el pedido de acceso del NAS, busca en la base de datos LDAP dónde están todos los usuarios de la red de la clínica. Dichos eventos son realizados en el nivel de Aplicación, Séptima capa del modelo OSI. Se responderá según sea el caso:

- Accept – request: Este paquete contiene el nombre de usuario, la contraseña encriptada, la dirección IP NAS, y el puerto (1812).
- Reject – request: El nombre de usuario no existe en la base de datos LDAP.

En RADIUS, la autenticación y la autorización están unidas. Si se acierta el nombre de usuario y la contraseña, el servidor RADIUS devuelve una respuesta de Acceso-Aceptar e incluye una lista de pares de atributo-valor que describe los parámetros que deben usarse en esta sesión. Los parámetros comunes incluyen el tipo de servicio (shell o entramado), el tipo de protocolo, la dirección IP para asignar el usuario (estática o dinámica), la lista de acceso a aplicar o una ruta estática para instalar en

la tabla de ruteo de NAS. La información de configuración en el servidor RADIUS define qué se instalará en el NAS.

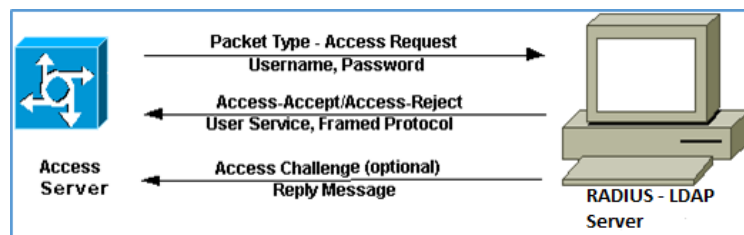


Ilustración 30. Secuencia de autenticación y autorización RADIUS.

h) Firewall o Cortafuegos

El firewall seleccionado como parte de la propuesta es el dispositivo CISCO ASA 5520. Es nuestra primera línea de defensa ante un ataque a la red de la clínica desde internet permitiendo o denegando las transmisiones de una red a la otra. Será situado entre la red interna e internet como dispositivo de seguridad evitando que los intrusos informáticos puedan acceder a la red local.

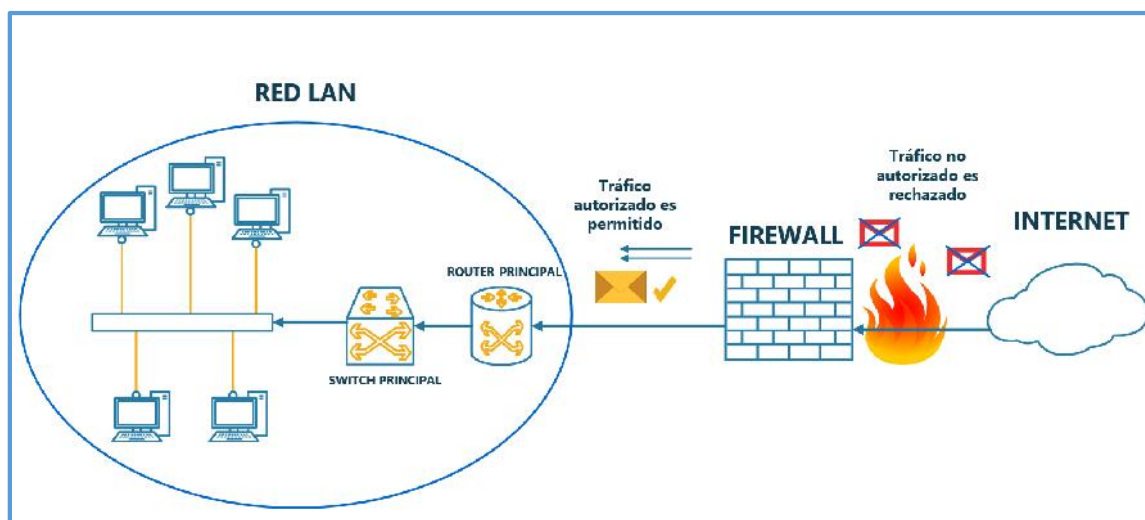


Ilustración 31. Diseño lógico Firewall

Desempeñará los siguientes roles:

- Implementación de Listas de Acceso ACL's
- Permisos y restricciones en puertos específicos, entre otros

i) Diseño de la propuesta de implementación

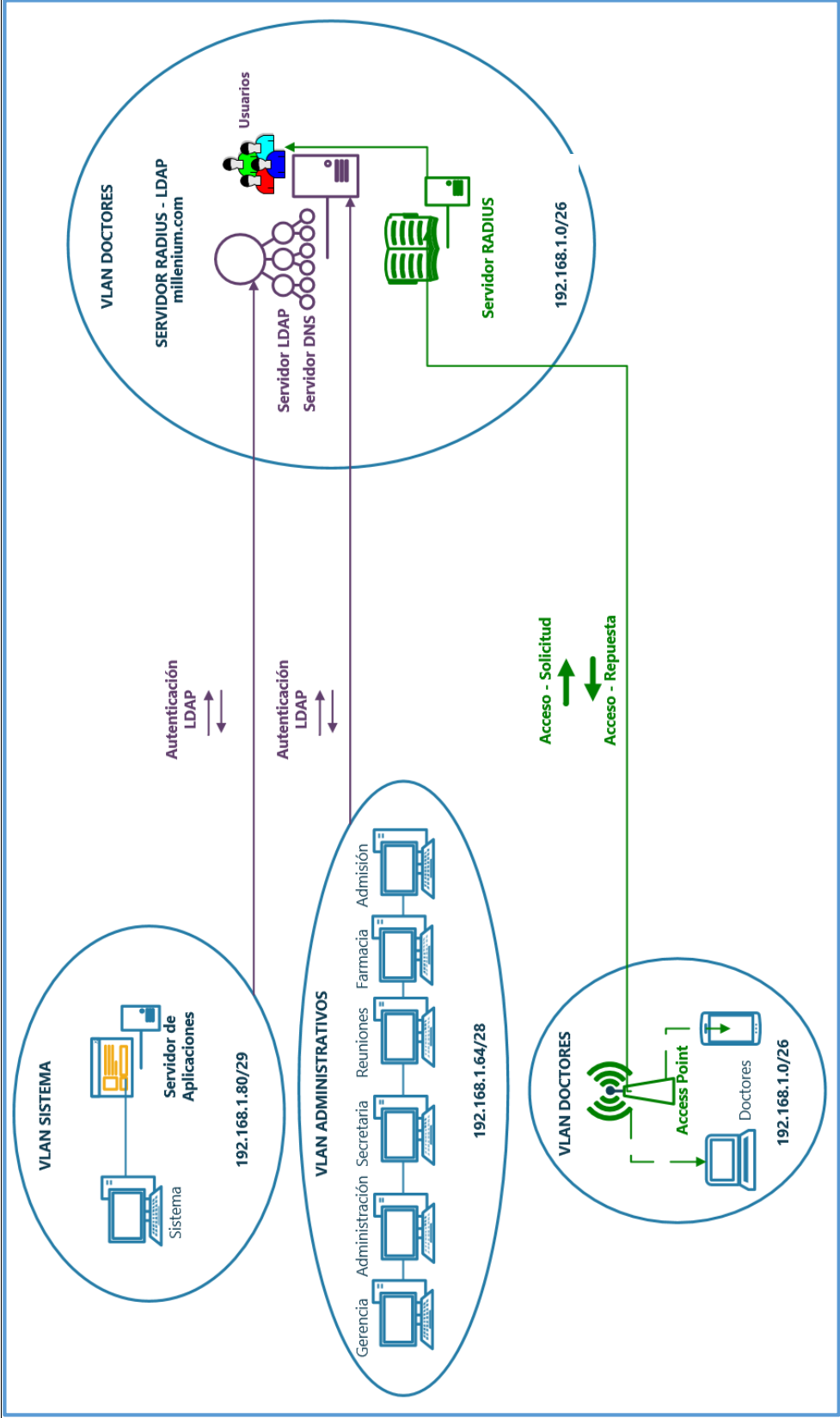


Ilustración 32: Diseño Lógico. Arquitectura de autenticación propuesta.

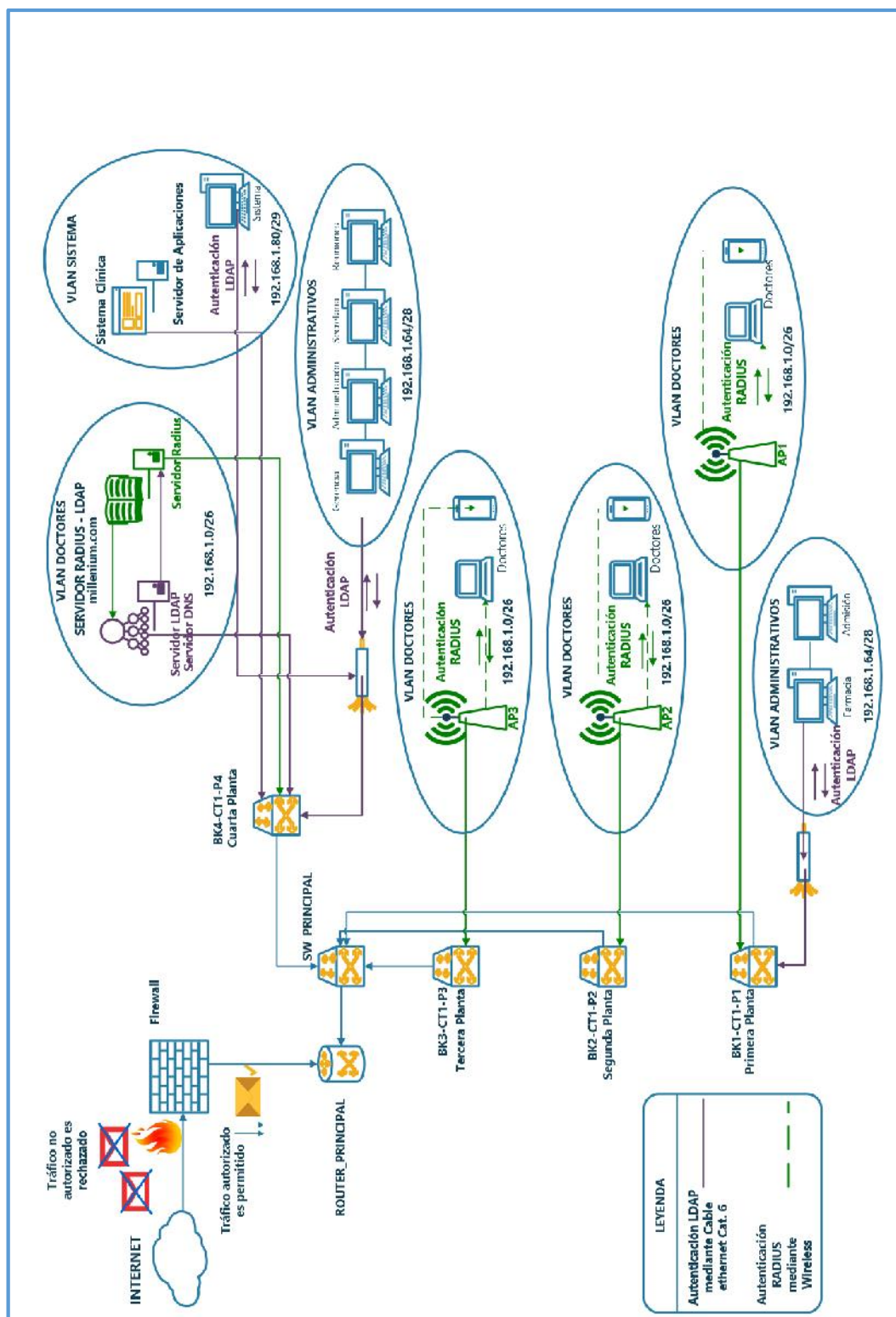


Ilustración 33: Diseño Lógico propuesto.

j) Directivas de seguridad

Se realizaron directivas con el objetivo de ser distribuidas a los equipos y usuarios de la clínica. La configuración y funcionalidad de éstas GPO's (Group Policy Object) definidas para este proyecto más adelante en las ilustraciones desde la ilustración 87 hasta la 106, sin embargo, la función principal de las directivas de grupo es la de facilitar la administración de la red de la clínica con configuraciones centralizadas.

Para la administración de los usuarios:

- Para realizar el mantenimiento de los usuarios (registro, actualización y depuración) y consultas, se deberá en primera instancia de autenticarse con un usuario administrador al servidor LDAP.

Para el uso de los equipos dentro de la red LAN se establece la siguiente directiva:

- Estará conformada sólo por usuarios de escritorio (desktop)
- Las directivas seguridad local por equipo se desactiva (inicio de sesión con usuario local)
- La autenticación es realizada directamente con el servidor LDAP.

El firewall será configurado de la siguiente manera:

- Se dispondrá del NAT para permitir que los hosts salgan a internet.
- Se asignarán zonas desmilitarizadas (DMZ), las cuáles se distribuyen en 3 zonas (Inside, outside, DMZ).
- Se permite el flujo de tráfico desde la zona inside hacia outside
- Se permite el flujo de tráfico desde la zona militarizada hacia outside
- Se permite el flujo de tráfico desde la zona inside hacia la zona DMZ

TIPO DE ZONA	NIVEL DE SEGURIDAD	DIRECTIVA DE SEGURIDAD
Inside	100	Asignada al área de sistemas. Se pretende proteger
Outside	0	Conectada a la parte de la WAN, al ISP.
DMZ	50	Zona desmilitarizada asignada para el servidor de aplicaciones de la clínica

Tabla 20. Directivas de seguridad del Firewall

- Se implementarán Listas de Acceso ACL para restringir el acceso entre VLANs, sólo de ser necesario sea el caso para la autenticación a los servidores integrados RADIUS – LDAP.

Los switches tendrán las siguientes directivas configuradas (los comandos de configuración se encuentran en los anexos):

- Se registrarán todas las VLANs y se activarán los puertos correspondientes con la asignación de la VLAN que pertenece.
- Se activará los enlaces troncales en el switch que están conectado al router.
- Se establecerá la seguridad de puertos de la siguiente manera:

TIPO DE SEGURIDAD DE PUERTOS	DIRECTIVA DE SEGURIDAD
Sticky (Pegajoso)	El puerto recibirá la mac del equipo perteneciente a la clínica de manera automática.
Protected (protegido)	Sólo está permitido la conexión de un equipo registrado en la tabla de direcciones mac, no se permitirá la conexión de cualquier otro equipo que no pertenezca a la clínica.
Shutdown (apagar)	El puerto se apagará automáticamente al intento de conexión de un equipo no registrado en la tabla de direcciones mac.

Tabla 21. Directivas de seguridad de Switches

Estos mecanismos, además de mejorar la autenticación de los usuarios y la integridad de los recursos, optimizan los servicios de seguridad de control de acceso, confidencialidad, disponibilidad, es decir, tanto al usuario o equipo que solicita el servicio como al servidor que lo otorga.

3. Direccionamiento IP

EQUIPO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED
ROUTER	GigabitEthernet 0/0	192.168.1.1	255.255.255.0

Tabla 22: Direccionamiento IP propuesto.

Router:

Este dispositivo cumplirá funciones de enrutamiento de paquete entre redes, asumirá algunas funciones de DHCP para la administración y distribución de las subredes dentro de la red de la clínica. La configuración esta adjunta en los anexos.

3.1. Subneteo VLSM:

Debido a que estas áreas tienen cantidades de distintos usuarios, se aplica el método de Subneteo VLSM (Variable Length Subnet Mask) para dividir en subredes acorde a la necesidad de las áreas.

La red de la clínica se distribuirá en tres áreas, las cuales serán asignadas tres VLANS correspondientes. Se realiza esta acción para una mejor administración, control de tráfico de red y refuerza la seguridad al segmentar la red según las funciones a realizar en la clínica. Teniendo en consideración las funciones respectivas dentro de la Clínica, se realiza la creación de las VLANS:

VLAN	HOST PEDIDOS	HOST ÚTILES	DIRECCIÓN DE RED	MÁSCARA DE RED	RANGO DE IP'S		BROADCAST
DOCTORES	52	62	192.168.1.0	/26	192.168.1.1	192.168.1.62	192.168.1.63
ADMINISTRATIVOS	11	16	192.168.1.64	/28	192.168.1.65	192.168.1.78	192.168.1.79
SISTEMA	3	6	192.168.1.80	/29	192.168.1.81	192.168.1.86	192.168.1.87

Tabla 23: Creación de VLANS.

En la siguiente tabla se muestra la distribución de todas las áreas de la clínica que estarán interconectadas en la red.

VLAN SISTEMA: Esta VLAN comprende sólo el área de sistemas donde está localizada el área de telecomunicaciones y los servidores.

VLAN ADMINISTRATIVOS: Compuesta por todas las áreas que realizan funciones administrativas.

VLAN DOCTORES: Está VLAN la conforman todos los consultorios de la clínica, están interconectadas mediante una WLAN.

Las áreas de la estarán están completamente separadas del tráfico de datos que las mismas realizan, disminuyendo la posibilidad que ocurran violaciones de información confidencial, mejorando el rendimiento y facilitando manejo de la red debido a que los usuarios con requerimientos similares de red compartirán la misma VLAN. También es fácil para el personal de TI identificar las funciones asignadas a las VLANs al proporcionarle un nombre y determinar el alcance de los efectos de la actualización de los servicios de red de la clínica.

VLAN	ÁREA
SISTEMA	Sistemas
ADMINISTRATIVOS	Admisión
	Administración
	Farmacia
	Gerencia
	Secretaria
	Reuniones
DOCTORES	Traumatología1
	Otorrinolaringología
	Pediatría
	Endocrinología
	Geriatría
	Gastroenterología1
	Traumatología2
	Terceros
	Ginecología
	Alquiler
	Interno
	Dentista
	Pediatría
	Cardiología
	Endocrinología
	Gastroenterología2
	Neumología
	Tópico
	Laboratorio
	Gerente
	Sistemas
	Administración
	Secretaría

Tabla 24: Asignación de VLANS.

3. Gestión de acceso de Usuario

- El estándar ISO 27002 señala que se deberían controlar el acceso a la información, los recursos y aplicaciones en base a las necesidades de seguridad de la Organización.
- La información proporcionada al usuario será acorde a sus funciones dentro de la Clínica (SISTEMA, ADMINISTRATIVO, DOCTORES), bajo ninguna circunstancia los usuarios de un área obtendrán información utilizada en otra que no sea la suya.
- La cuenta de usuario será personal e intransferible y será responsabilidad del usuario el buen uso que haga de ella.
- La creación de un nuevo usuario en el sistema de autenticación AAA estará a cargo del administrador de la red.
- Toda solicitud de creación, modificación o baja de cuenta de usuario deberá estar aprobada por el Jefe del área.
- El jefe de un área, poseedor de las cuentas de usuario correspondientes a ésta debe reportar la baja de sus usuarios cuando estos dejan de laborar bajo su cargo.
- Los usuarios que se conectan a la red por un medio cableado (Pc o Laptop), para conectarse a la base de usuarios LDAP y realizar la autenticación correspondiente, los ordenadores deberán ser configurados previamente.
- Los usuarios que se conectan a la red por un medio inalámbrico, deberán autenticarse al Access point de la planta a la que pertenece su área. Se deberá configurar previamente el dispositivo móvil (Smartphone, Laptop) pues deben autenticarse primero al servidor RADIUS, el cual enviará la solicitud al servidor LDAP con el cual está integrado.

4. Configuración de los servidores

a. SERVIDOR LDAP

LDAP es un servidor de directorio para Linux, permite un completo sistema de identidades y una plataforma integral para varios servicios. Instalaremos *SLDAP* que es un servidor de directorio LDAP mediante comandos:

```
root@millenium:~# aptitude install slapd ldap-utils
```

Al finalizar la instalación de manera automática nos solicitará que asignemos una contraseña para el ingreso al servidor:

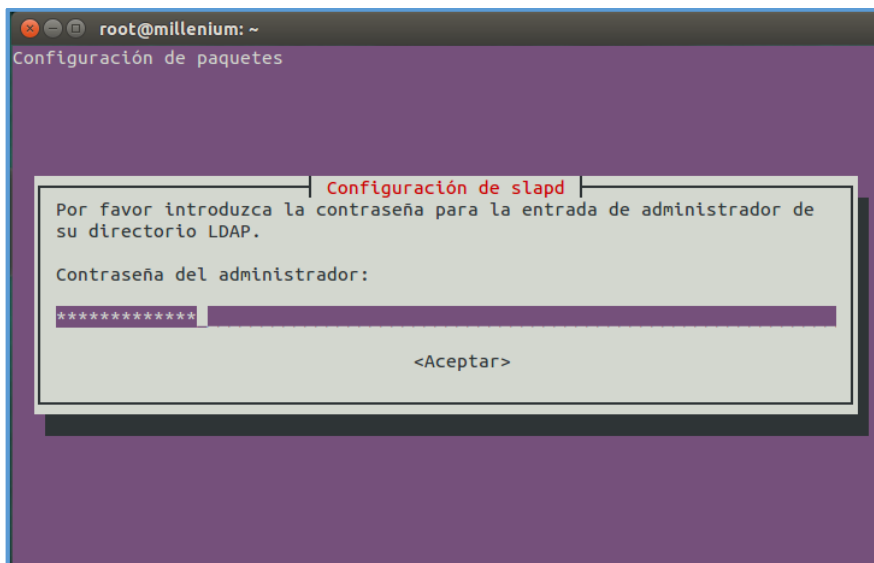


Ilustración 34: Servidor SLDAP Asignar contraseña administrador.

La asignación de esta contraseña es para el usuario que tiene completa administración sobre el directorio.

Para realizar la configuración inicial del servidor ejecutamos el siguiente comando:

```
root@millenium:~# dpkg-reconfigure slapd
```

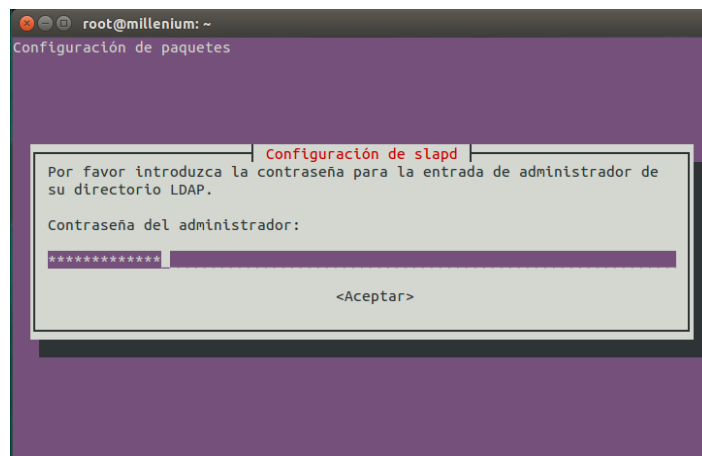


Ilustración 35: Servidor SLDAP configuración inicial.

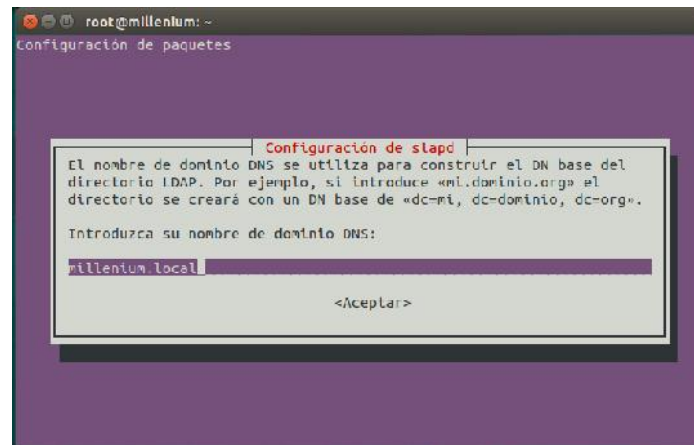


Ilustración 36: Servidor SLDAP configuración inicial.

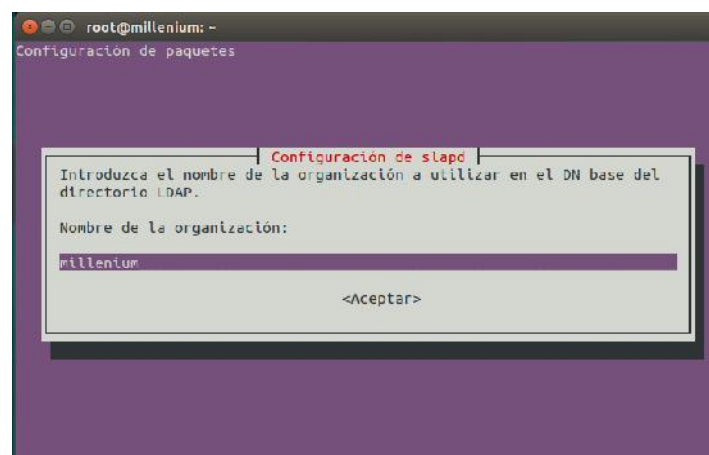


Ilustración 37: Servidor SLDAP configuración inicial.

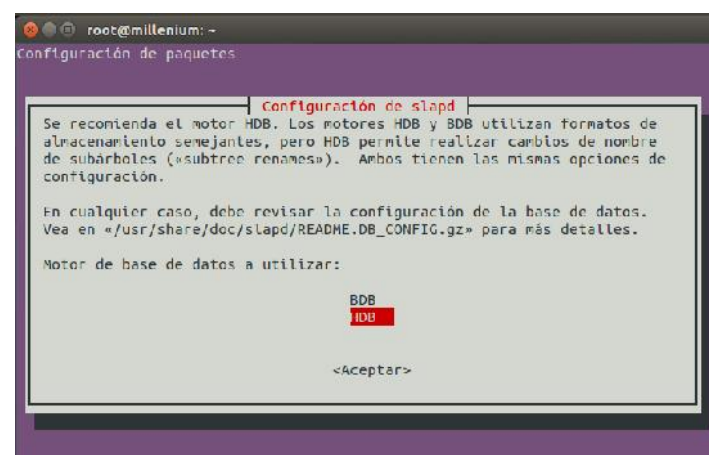


Ilustración 38: Servidor SLDAP configuración inicial.

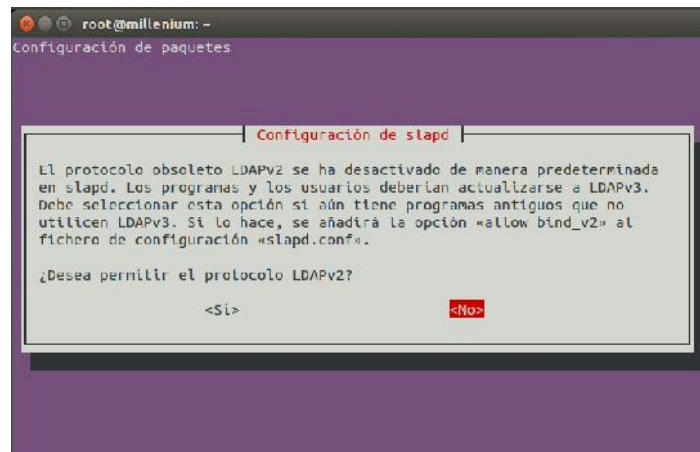


Ilustración 39: Servidor SLDAP configuración inicial.

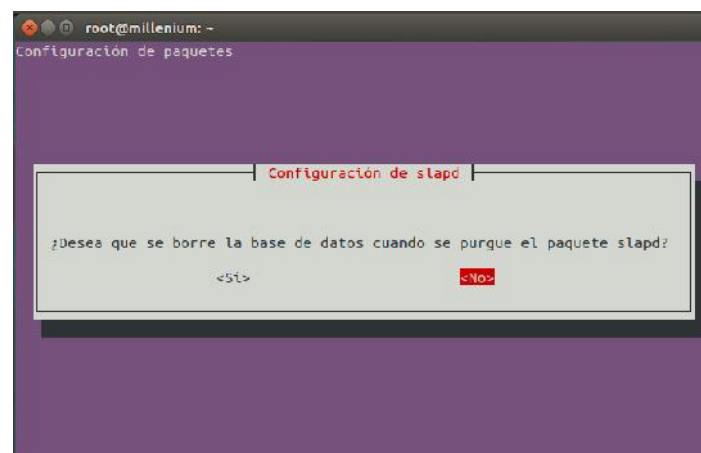


Ilustración 40: Servidor SLDAP configuración inicial.

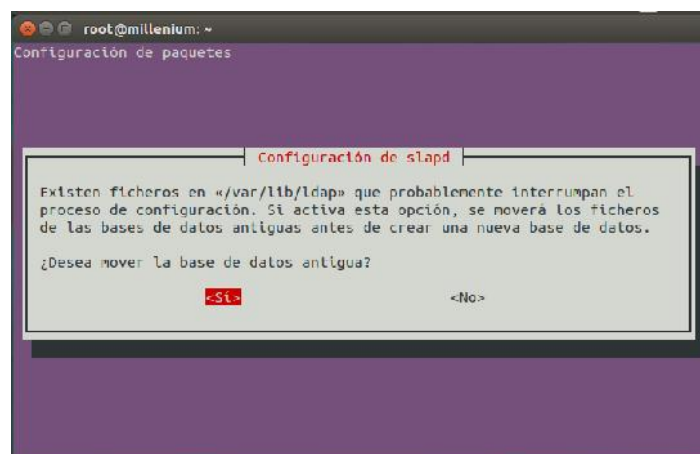
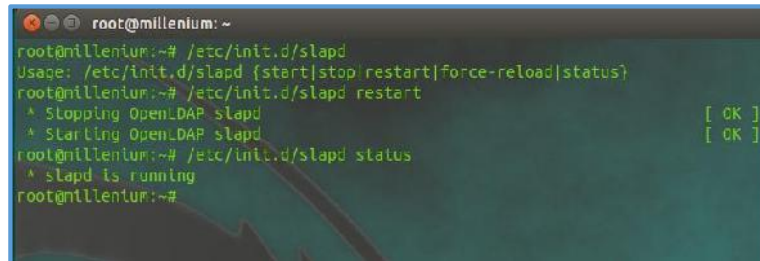


Ilustración 41: Servidor SLDAP configuración inicial.

La configuración del servidor de almacena en la ruta `/etc/ldap`, no es recomendable manipular los archivos de configuración de manera constante.

El servidor LDAP, como en cualquier servidor en Linux posee script de arranque, detención, entre otros en la carpeta `/etc/init.d`. Para una correcta configuración y actualización de los cambios realizados, utilizamos los servicios de arranque y detención del servidor:

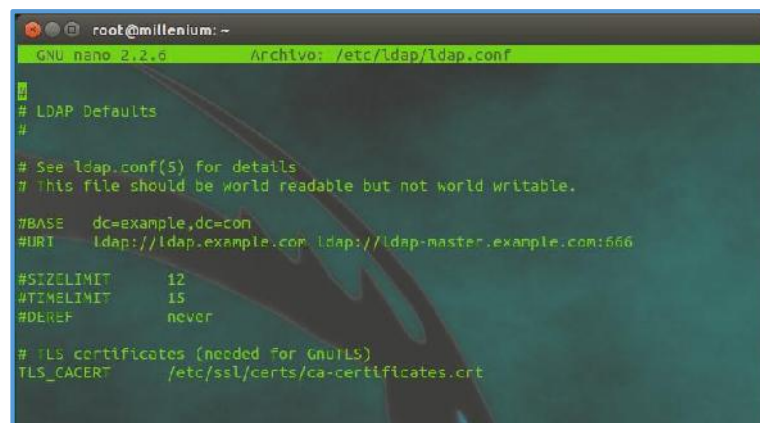


```
root@millenium:~# /etc/init.d/slapd
Usage: /etc/init.d/slapd {start|stop|restart|force-reload|status}
root@millenium:~# /etc/init.d/slapd restart
^ Stopping OpenLDAP slapd [ OK ]
^ Starting OpenLDAP slapd [ OK ]
root@millenium:~# /etc/init.d/slapd status
^ slapd is running
root@millenium:~#
```

Ilustración 42: Servidor LDAP servicios básicos.

Los archivos de configuración de SLAPD son instalados en el directorio `/etc/ldap/`. Para usar la herramienta de control del servidor, primero configuramos algunas directrices de LDAP que se encuentra en el archivo `ldap.conf`. Este es el archivo de configuración para todas las aplicaciones cliente que utiliza las bibliotecas de LDAP como por ejemplo `ldapadd`, `ldapsearch`.

```
root@millenium:~# nano /etc/ldap/ldap.conf
```

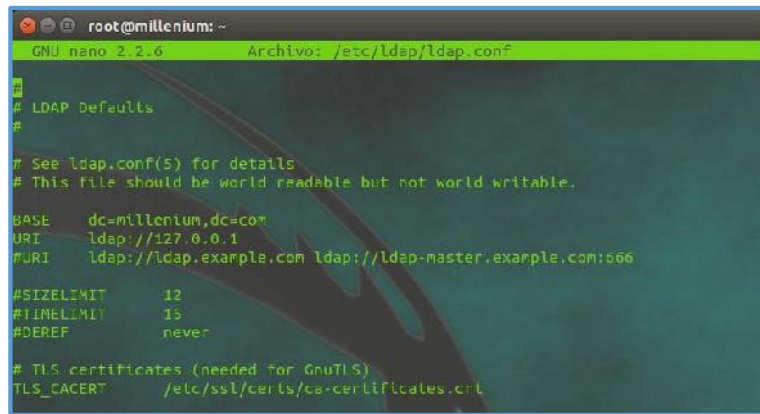


```
GNU nano 2.2.6 Archivo: /etc/ldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
#BASE dc=example,dc=com
#URI ldap://ldap.example.com ldap://ldap-master.example.com:666
#SIZELIMIT 12
#TIMELIMIT 15
#DEREF never
# TLS certificates (needed for GnuTLS)
TLS_CACERT /etc/ssl/certs/ca-certificates.crt
```

Ilustración 43: Servidor LDAP configuración archivo `ldap.conf` por defecto.

Dentro del archivo modificamos las siguientes líneas:

```
BASE      dc=millenium,dc=com
URI       ldap://127.0.0.1
```



```
root@millenium: ~  
GNU nano 2.2.6 Archivo: /etc/ldap/ldap.conf  
#  
# LDAP Defaults  
#  
# See ldap.conf(5) for details  
# This file should be world readable but not world writable.  
BASE dc=millenium,dc=com  
URI ldap://127.0.0.1  
#URI ldap://ldap.example.com ldap://ldap-master.example.com:666  
#SIZELIMIT 12  
#TIMELIMIT 15  
#DEREF never  
# TLS certificates (needed for GnuTLS)  
TLS_CACERT /etc/ssl/certs/ca-certificates.crt
```

Ilustración 44: Servidor LDAP configuración archivo ldap.conf.

Cargar las plantillas: Las plantillas que cargamos vienen instaladas ya por defecto en el servidor LAPD, estas nos sirven para crear el esquema básico el almacenamiento de usuarios unix para LDAP, esto nos permite crear y guardar cuentas de usuario en nuestro directorio.

Se ejecutan los siguientes comandos:

```
root@millenium:~# ldapadd -Y EXTERNAL -H ldapi:/// -f  
/etc/ldap/schema/cosine.ldif
```

```
root@millenium:~# ldapadd -Y EXTERNAL -H ldapi:/// -f  
/etc/ldap/schema/nis.ldif
```

```
root@millenium:~# ldapadd -Y EXTERNAL -H ldapi:/// -f  
/etc/ldap/schema/inetorgperson.ldif
```

Debemos crear el archivo del esquema básico, este será creado en formato *ldif*, en el cual debemos configurar:

- **Base del directorio:** Se configura en el parámetro *olcSuffix* del archivo de configuración del esquema básico. En nuestro caso usaremos: `dc=millenium,dc=com`
- **Nombre de usuario administrador:** Se configura en el parámetro *olcRootDN* del archivo de configuración del esquema básico. En nuestro caso usaremos: `cn=admin,dc=millenium,dc=com`
- **Contraseña:** Se configura en el parámetro *olcRootPW* del archivo de configuración del esquema básico. Usaremos: `admin123admin`

- **Permiso de acceso a contraseñas:** Se configura en el parámetro *olcAccess: to attrs=userPassword*. Daremos al usuario administrador permiso de escritura y a cada usuario para cambiar su propia contraseña
- **Permiso de acceso global al directorio:** Se configura en el parámetro *olcAccess: to **. Daremos al usuario administrador permiso de escritura y a todos los usuarios, permisos de lectura

Este archivo lo guardamos en la carpeta temporal porque una vez ejecutado debería borrarse pues contiene la contraseña del administrador en texto plano. El archivo creado como *ldap-esquema-basico.ldif*

```
# ----- Archivo ldap-esquema-basico.ldif -----

# Cargamos el modulo dynamic backend

dn: cn=module, cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb
# Base de datos configuración
dn: olcDatabase=hdb, cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=millenium,dc=com
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=millenium,dc=com
olcRootPW: admin123admin
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_ik_max_objects 1500
olcDbConfig: set_ik_max_locks 1500
olcDbConfig: set_ik_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=millenium,dc=com"
write by anonymous auth by self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=millenium,dc=com" write by * read

# -----
```

Una vez creado el archivo, lo cargamos en el servidor LDAP mediante el comando

```
Root@millenium:~# ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/ldap-esquema-
basico.ldif
```

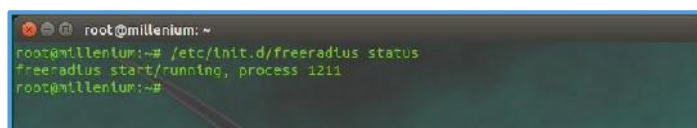
b. SERVIDOR RADIUS

Para la simulación se instaló el software FreeRADIUS que es un producto de código abierto con licencia GPL de GNU. Se puede obtener desde el sitio web <http://freeradius.org/>. Se realizó la instalación por comandos:

```
root@millenium:~#Aptitude install freeradius freeradius-ldap freeradius-utils
```

Comprobamos mediante comandos básicos la correcta instalación del servidor Freeradius:

```
Root@millenium:~# /etc/init.d/freeradius status
```



```
root@millenium:~# /etc/init.d/freeradius status
freeradius start/running, process 1211
root@millenium:~#
```

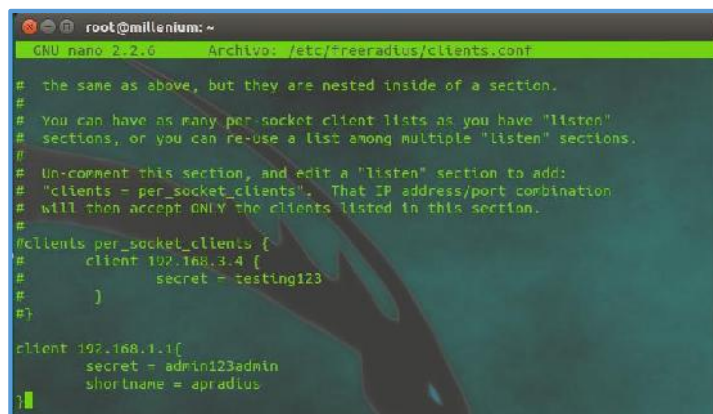
Ilustración 45: Servidor Freeradius estado del servidor.

Hecho esto, procedemos a configurar el archivo `clients.conf` en el cual se almacenan las configuraciones de los clientes, en este caso el dispositivo intermediario:

```
Root@millenium:~# nano /etc/freeradius/clients.conf
```

En la parte final del archivo agregamos las siguientes líneas de código:

```
Client 192.168.1.1{
    secretname= admin123admin
    shortname= apradius
}
```



```
root@millenium:~# nano /etc/freeradius/clients.conf
GNU nano 2.2.6 Archivo: /etc/freeradius/clients.conf

# the same as above, but they are nested inside of a section.
# You can have as many per socket client lists as you have "listen"
# sections, or you can re-use a list among multiple "listen" sections.
#
# Un-comment this section, and edit a "listen" section to add:
# "clients = per_socket_clients". That IP address/port combination
# will then accept ONLY the clients listed in this section.
#
#clients per_socket_clients {
#  client 192.168.3.4 {
#    secret = testing123
#  }
#}

client 192.168.1.1{
    secret = admin123admin
    shortname = apradius
}
```

Ilustración 46: Servidor Freeradius archivo clients.conf.

c. HABILITAR LA AUTENTICACIÓN MEDIANTE LDAP

FreeRADIUS entre la variedad de sus funciones permite distintas formas de autenticación, la que se utilizó fue la autenticación a SLDAP (servidor LDAP). Para habilitar la autenticación realizamos lo siguiente:

Abrimos el archivo *eap.conf* localizado en */etc/freeradius/eap.conf*:

```
root@millenium:~# nano /etc/freeradius/eap.conf
```

y agregamos las siguientes líneas de código en la parte inicial del archivo:

```
Default_eap_type = peap
md5 {
    private_key_password = admin123admin
}
peap {
    default_eap_type = chap
}
```

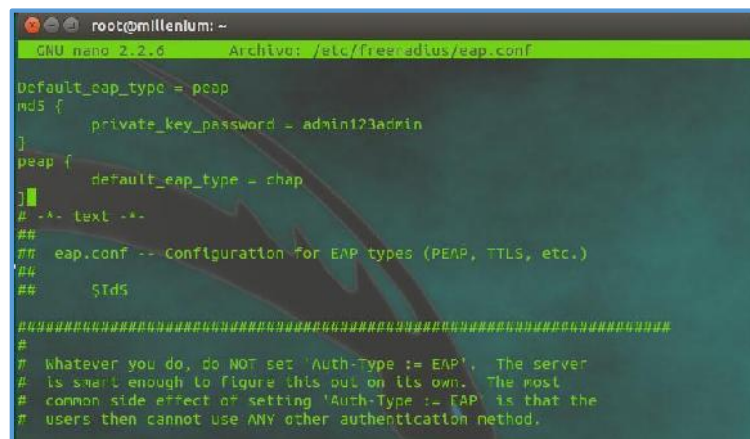


Ilustración 47: Servidor Freeradius archivo eap.conf.

Restauramos el servidor:

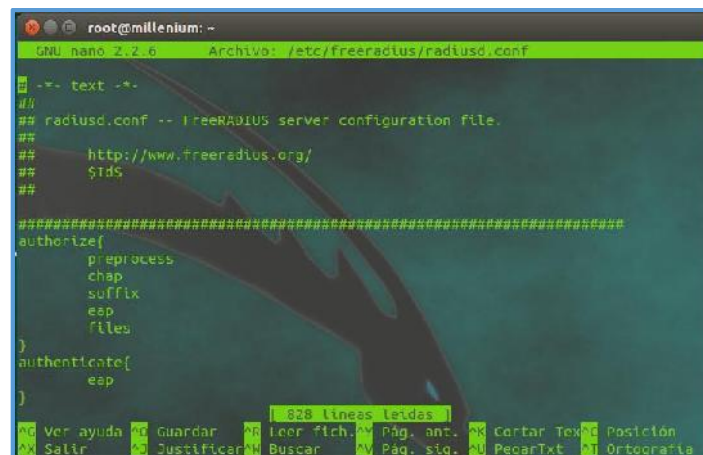
```
Root@millenium:~# /etc/init.d/freeradius restart
```

También debemos autorizar los protocolos en el archivo *radiusd.conf* localizado en la dirección */etc/freeradius/radiusd.conf*. Abrimos el archivo:

```
Root@millenium:~# nano /etc/etc/freeradius/radiusd.conf
```

Y escribimos las siguientes líneas de código en la parte inicial del archivo:

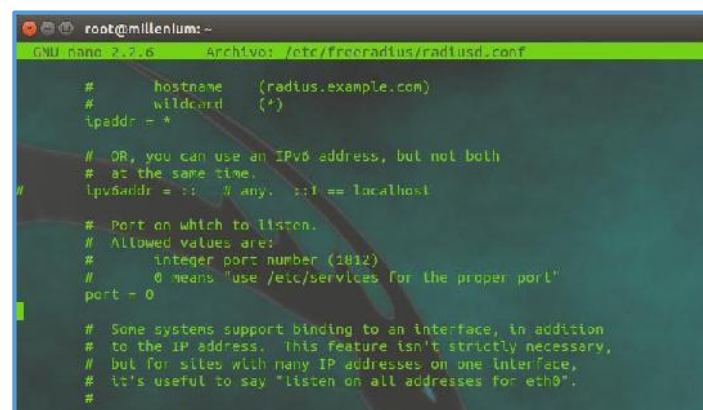
```
Authorize {  
    preprocess  
    chap  
    suffix  
    eap  
    files  
}  
  
Authenticate {  
    eap  
}
```



```
root@millenium: ~  
GNU nano 2.2.6 Archivo: /etc/freeradius/radiusd.conf  
#-- text --  
##  
## radiusd.conf -- FreeRADIUS server configuration file.  
##  
##      http://www.freeradius.org/  
##      $Id$  
##  
#####  
authorize{  
    preprocess  
    chap  
    suffix  
    eap  
    files  
}  
authenticate{  
    eap  
}
```

Ilustración 48: Servidor Freeradius archivo radiusd.conf - A.

En el mismo archivo debemos activar la línea de código *puerto*, de tal manera como se muestra en la ilustración:

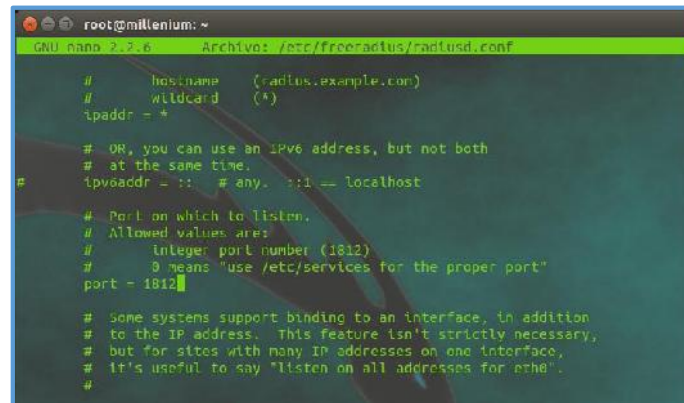


```
root@millenium: ~  
GNU nano 2.2.6 Archivo: /etc/freeradius/radiusd.conf  
#      hostname      (radius.example.com)  
#      wildcard      (*)  
ipaddr = *  
  
# OR, you can use an IPv6 address, but not both  
# at the same time.  
#  
# ip6addr = :: # any. ::1 == localhost  
#  
# Port on which to listen.  
# Allowed values are:  
#     integer port number (1024)  
#     0 means "use /etc/services for the proper port"  
port = 0  
  
# Some systems support binding to an interface, in addition  
# to the IP address. This feature isn't strictly necessary,  
# but for sites with many IP addresses on one interface,  
# it's useful to say "listen on all addresses for eth0".  
#
```

Ilustración 49: Servidor Freeradius archivo radiusd.conf por defecto.

Modificamos:

Port= 1812



```
root@millenium: ~
GNU nano 2.2.6 Archivo: /etc/freeradius/radiusd.conf

# hostname (radius.example.com)
# wildcard (*)
ipaddr = +

# OR, you can use an IPv6 address, but not both
# at the same time.
# ipv6addr = :: # any. ::1 == localhost

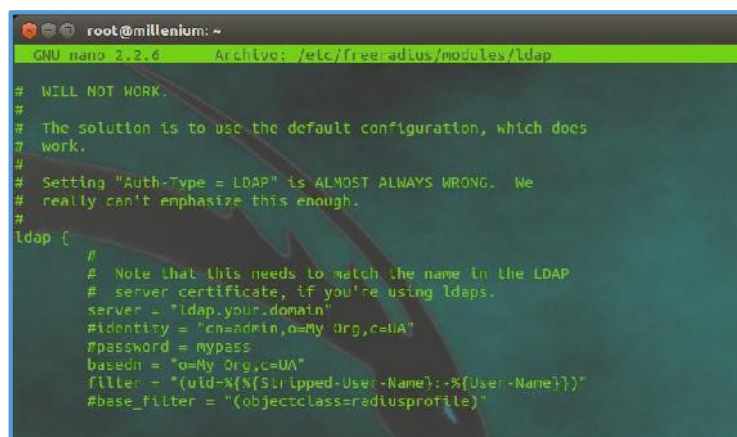
# Port on which to listen.
# Allowed values are:
# integer port number (1812)
# 0 means "use /etc/services for the proper port"
port = 1812

# Some systems support binding to an interface, in addition
# to the IP address. This feature isn't strictly necessary,
# but for sites with many IP addresses on one interface,
# it's useful to say "listen on all addresses for other".
#
```

Ilustración 50: Servidor Freeradius archivo radiusd.conf B.

Para usar el servidor LDAP a nivel administrativo, debemos actualizar el usuario con privilegios globales. Modificaremos el archivo de texto plano *ldap* localizado en */etc/freeradius/modules/ldap*. Ejecutamos el siguiente comando para editar el archivo:

```
root@millenium:~# nano /etc/freeradius/modules/ldap
```



```
root@millenium: ~
GNU nano 2.2.6 Archivo: /etc/freeradius/modules/ldap

# WILL NOT WORK.
# The solution is to use the default configuration, which does
# work.
# Setting "Auth-Type = LDAP" is ALMOST ALWAYS WRONG. We
# really can't emphasize this enough.
#
ldap {
#
# Note that this needs to match the name in the LDAP
# server certificate, if you're using ldaps.
server = "ldap.your.domain"
#identity = "cn=admin,dc=My Org,c=UA"
#password = mypass
basedn = "dc=My Org,c=UA"
filter = "(uid=%N{Stripped-User-Name}:-%{User-Name})"
#base_filter = "(objectclass=radiusprofile)"
}
```

Ilustración 51: Servidor Freeradius archivo ldap por defecto.

Modificamos el archivo *ldap* que se encuentra en:

```
/etc/freeradius/modules/ldap
```

Dentro de este fichero, modificamos las siguientes líneas de comandos:

```
Server = "192.168.1.200"
```

Se quita el comentario de la línea de identidad para autorizar al usuario administrador para poder utilizarlo:

```
identity = "cn=admin,dc=millenium,dc=com"
```

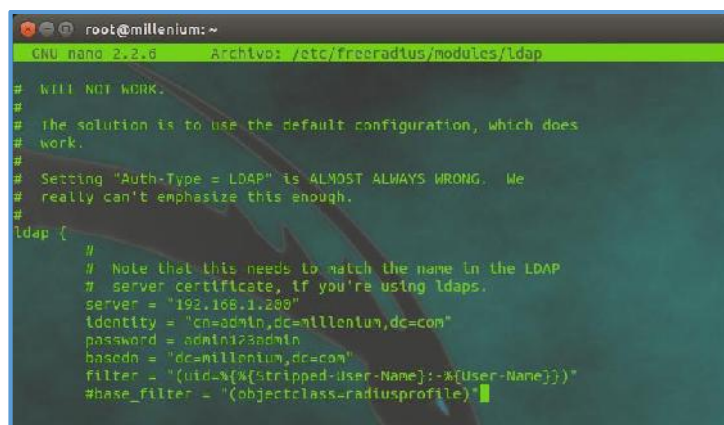
De la misma forma quitamos el comentario y actualizamos la contraseña correspondiente al usuario administrador ingresado:

```
password = admin123admin
```

La basedn cambia a la ruta actual donde hemos registrado el usuario administrador

```
Basedn= "dc=millenium,dc=com"
```

De tal manera debe quedar como se muestra en la ilustración:

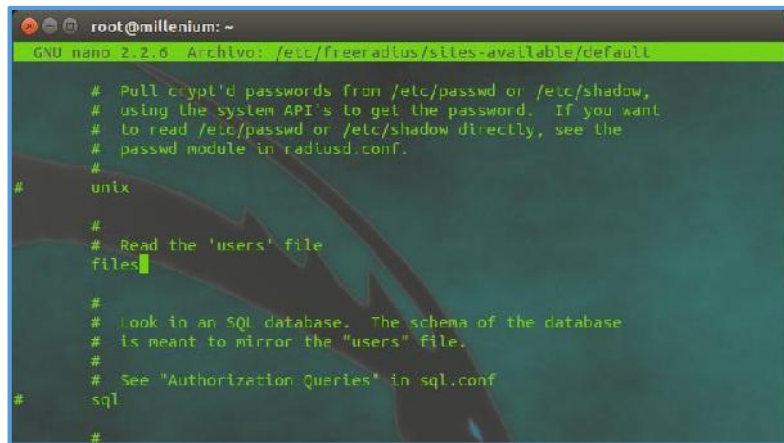


```
root@millenium: ~  
GNU nano 2.2.6 Archivo: /etc/freeradius/modules/ldap  
  
# Will NOT WORK.  
# The solution is to use the default configuration, which does  
# work.  
# Setting "Auth-Type = LDAP" is ALMOST ALWAYS WRONG. We  
# really can't emphasize this enough.  
#  
ldap {  
    #  
    # Note that this needs to match the name in the LDAP  
    # server certificate, if you're using ldaps.  
    server = "192.168.1.200"  
    identity = "cn=admin,dc=millenium,dc=com"  
    password = admin123admin  
    basedn = "dc=millenium,dc=com"  
    filter = "(uid=%[stripped-user-name]-%[user-name])"  
    #base_filter = "(objectclass=radiusprofile)"
```

Ilustración 52: Servidor Freeradius archivo ldap.

No se modifican los campos restantes.

Ahora modificamos el fichero *default* para habilitar la autenticación localizada en la dirección */etc/freeradius/sites-available/default*



```
root@millenium: ~
GNU nano 2.2.6 Archivo: /etc/freeradius/sites-available/default

# Pull crypt'd passwords from /etc/passwd or /etc/shadow,
# using the system API's to get the password.  If you want
# to read /etc/passwd or /etc/shadow directly, see the
# passwd module in radiusd.conf.
#
# unix
#
# Read the 'users' file
# file:
#
# Look in an SQL database.  The schema of the database
# is meant to mirror the "users" file.
#
# See "Authorization Queries" in sql.conf
# sql
#
```

Ilustración 53: Servidor Freeradius archivo default A por defecto.

Las líneas a modificar son varias:

Comentamos la línea *file*:

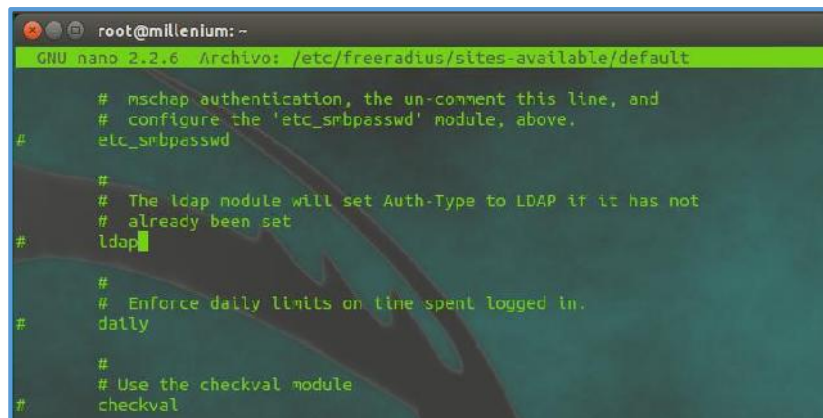


```
root@millenium: /etc/freeradius/sites-available
GNU nano 2.2.6 Archivo: default

# Pull crypt'd passwords from /etc/passwd or /etc/shadow,
# using the system API's to get the password.  If you want
# to read /etc/passwd or /etc/shadow directly, see the
# passwd module in radiusd.conf.
#
# unix
#
# Read the 'users' file
# file:
#
# Look in an SQL database.  The schema of the database
# is meant to mirror the "users" file.
#
```

Ilustración 54: Servidor Freeradius archivo default A.

Siguiente parte:



```
root@millenium: ~
GNU nano 2.2.6 Archivo: /etc/freeradius/sites-available/default

# mschap authentication, the un-comment this line, and
# configure the 'etc_smbpasswd' module, above.
# etc_smbpasswd
#
# The ldap module will set Auth-Type to LDAP if it has not
# already been set
# ldap
#
# Enforce daily limits on time spent logged in.
# daily
#
# Use the checkval module
# checkval
#
```

Ilustración 55. Servidor Freeradius archivo default B por defecto.

Y quitamos comentario a la línea *ldap*:

```
root@millenium: /etc/freeradius/sites-available
GNU nano 2.2.6 Archivo: default
# mschap authentication, the un-comment this line, and
# configure the 'etc smbpasswd' module, above.
etc_smbpasswd
#
# The ldap module will set Auth-Type to LDAP if it has not
# already been set
ldap
#
# Enforce daily limits on time spent logged in.
daily
#
# Use the checkval module
checkval
```

Ilustración 56: Servidor Freeradius archivo default B.

Finalmente modificamos el archivo *inner-tunnel* localizado en la dirección */etc/freeradius/sites-available/inner-tunnel*.

```
root@millenium:~# nano /ect/freeradius/sites-available/inner-tunnel
```

```
root@millenium: ~
GNU nano 2.2.6 Archivo: ...reeradius/sites-available/inner-tunnel
#
# The example below uses module failover to avoid querying all
# of the following modules if the EAP module returns "ok".
# Therefore, your LDAP and/or SQL servers will not be queried
# for the many packets that go back and forth to set up TLS
# or PEAP. The load on those servers will therefore be reduced.
#
eap {
    ok = return
}
#
# Read the 'users' file
files
#
# Look in an SQL database. The schema of the database
# is meant to mirror the "users" file.
#
```

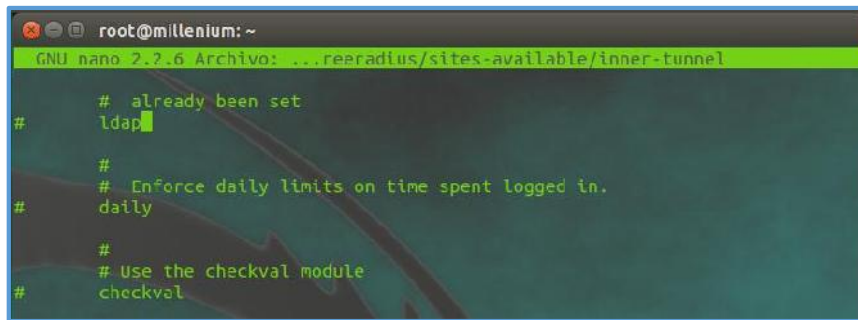
Ilustración 57: Servidor Freeradius archivo inner-tunnel A por defecto.

Debemos comentar a la línea de comando *file*:

```
root@millenium: /etc/freeradius/sites-available
GNU nano 2.2.6 Archivo: inner-tunnel
#
# Read the 'users' file
# files
#
# Look in an SQL database. The schema of the database
# is meant to mirror the "users" file.
#
# See "Authorization Queries" in sql.conf
# sql
```

Ilustración 58: Servidor Freeradius archivo inner-tunnel A.

Luego buscamos la siguiente línea de código:



```
root@millenium: ~
GNU nano 2.2.6 Archivo: ...freeradius/sites-available/inner-tunnel

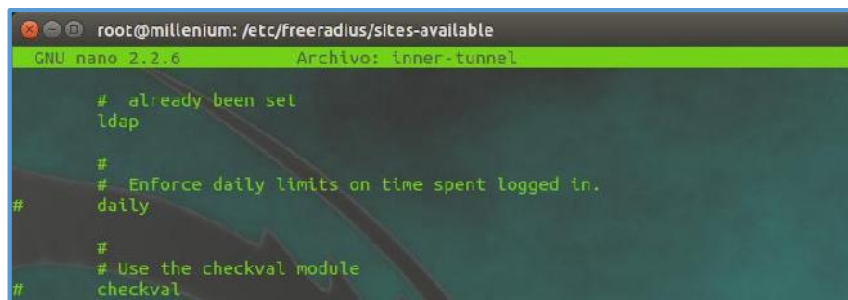
# already been set
# ldap

#
# Enforce daily limits on time spent logged in.
# daily

#
# Use the checkval module
# checkval
```

Ilustración 59: Servidor Freeradius archivo inner-tunnel B por defecto.

Quitar el comentario a la línea *ldap*:



```
root@millenium: /etc/freeradius/sites-available
GNU nano 2.2.6 Archivo: inner-tunnel

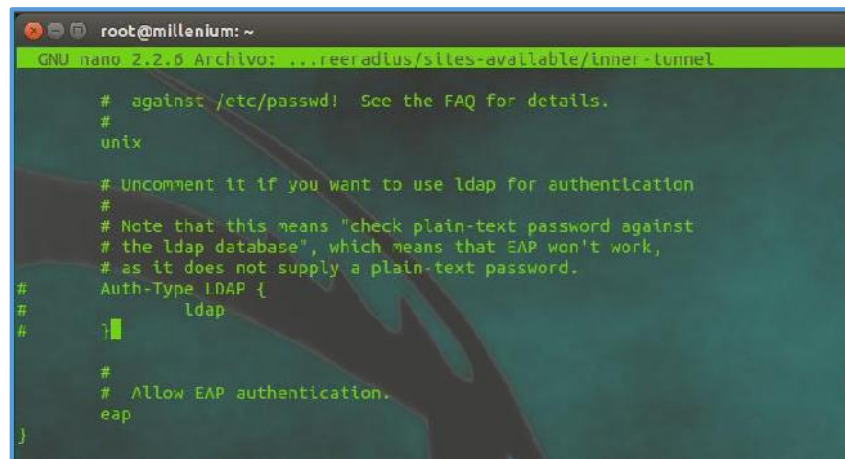
# already been set
ldap

#
# Enforce daily limits on time spent logged in.
# daily

#
# Use the checkval module
# checkval
```

Ilustración 60: Servidor Freeradius archivo inner-tunnel B.

Buscamos las siguientes líneas de código:



```
root@millenium: ~
GNU nano 2.2.6 Archivo: ...freeradius/sites-available/inner-tunnel

# against /etc/passwd! See the FAQ for details.
# unix

# Uncomment it if you want to use ldap for authentication
#
# Note that this means "check plain-text password against
# the ldap database", which means that EAP won't work,
# as it does not supply a plain-text password.
#
Auth-Type LDAP {
# ldap
#
# Allow EAP authentication.
eap
}
```

Ilustración 61: Servidor Freeradius archivo inner-tunnel C por defecto.

Y quitar los comentarios de las siguientes líneas:

```
Auth-Type LDAP {

    ldap

}
```

```

root@millenium: /etc/freeradius/sites-available
GNU nano 2.2.6 Archivo: inner-tunnel

# against /etc/passwd! See the FAQ for details.
#
unix
# Uncomment it if you want to use ldap for authentication
#
# Note that this means "check plain-text password against
# the ldap database", which means that EAP won't work,
# as it does not supply a plain-text password.
Auth-Type LDAP {
    ldap
}

#
# Allow EAP authentication.
eap
}

```

Ilustración 62: Servidor FreeRadius archivo inner-tunnel C.

Finalmente reiniciamos FreeRADIUS y comprobamos mediante el siguiente comando:

`root@millenium:~# freeradius -X`

```

root@millenium: ~
} # server
radiusd: ##### Opening IP addresses and Ports #####
listen {
    type = "auth"
    ipaddr = *
    port = 1812
}
listen {
    type = "acct"
    ipaddr = *
    port = 0
}
listen {
    type = "auth"
    ipaddr = 127.0.0.1
    port = 18120
}
... adding new socket proxy address * port 44118
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on authentication address 127.0.0.1 port 18120 as server inner-tunnel
Listening on proxy address * port 1814
Ready to process requests.

```

Ilustración 63: Comprobación de conectividad FreeRADIUS con autenticación LDAP.

5. Crear grupos y usuarios en el servidor LDAP para la autenticación

5.1. Registro de usuarios en el servidor LDAP:

Para registrar usuarios en el servidor LDAP, utilizaremos una plantilla con formato *LDIF*:

```

# ----- Archivo usuarios.ldif -----

dn: ou=Sistema,dc=millenium,dc=com
objectClass: organizationalUnit

```

objectClass: top
ou: Sistema

dn: ou=Administrativo,dc=millenium,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Administracion

dn: ou=Doctores,dc=millenium,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Doctores

#*****

dn: cn=sadmin ,ou=Sistema,dc=millenium,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
cn: sadmin
gidNumber: 1001
homeDirectory: /home/sadmin
loginShell: /bin/bash
sn: Osmar Albuja
uid: Sadmin
userPassword: o123o20A
uidNumber: 1011

dn: cn=screyes,ou=Sistema,dc=millenium,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
cn: screyes
gidNumber: 1001
homeDirectory: /home/screyes
loginShell: /bin/bash
sn: Reyes
uid: screyes
userPassword: c351c4F1
uidNumber: 1012

dn: cn=avloayza,ou=Administrativo,dc=millenium,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
cn: Avloayza
gidNumber: 1002
homeDirectory: /home/avloayza
loginShell: /bin/bash
sn: loayza


```
uid: avloayza
userPassword: v003v75J
uidNumber: 1013
```

```
dn: cn=avhidalgo,ou=Administrativo,dc=millenium,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
cn: avhidalgo
gidNumber: 1002
homeDirectory: /home/avhidalgo
loginShell: /bin/bash
sn: Hidalgo
uid: avhidalgo
userPassword: h923h01P
uidNumber: 1014
```

```
dn: cn=dssuarez,ou=Doctores,dc=millenium,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
cn: dssuarez
gidNumber: 1003
homeDirectory: /home/Dssuarez
loginShell: /bin/bash
sn: Suarez
uid: dssuarez
userPassword: d461d88R
uidNumber: 1015
```

```
dn: cn=dplopez,ou=Doctores,dc=millenium,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
cn: dplopez
gidNumber: 1003
homeDirectory: /home/dplopez
loginShell: /bin/bash
sn: Lopez
uid: dplopez
userPassword: p571p96L
uidNumber: 1016
```

```
#*****
```

Registrados los usuarios, utilizamos la herramienta JXplorer ldap, la cual nos permitirá tener una administración ágil en la lectura, búsqueda de usuarios y grupos.

En el menú principal del explorador LDAP, hacemos clic en el botón *connect* para conectar con el servidor LDAP implementado:

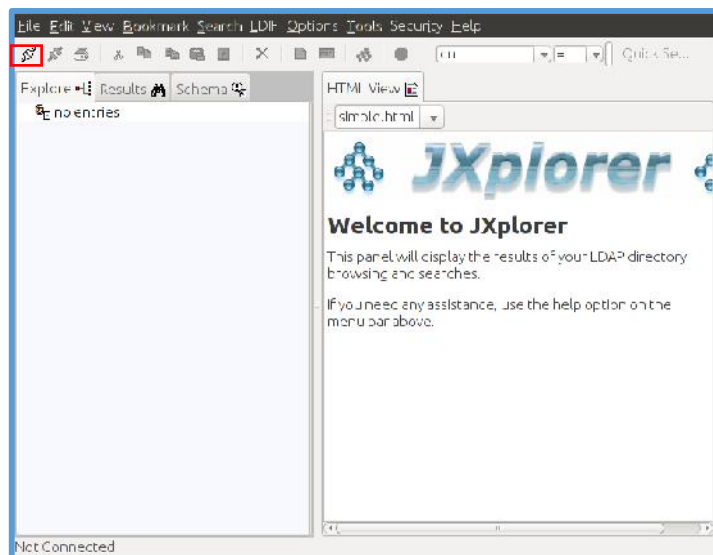


Ilustración 64: Menú Principal JXplorer.

El botón *connect* abre una ventana que nos solicita los datos para la conexión:

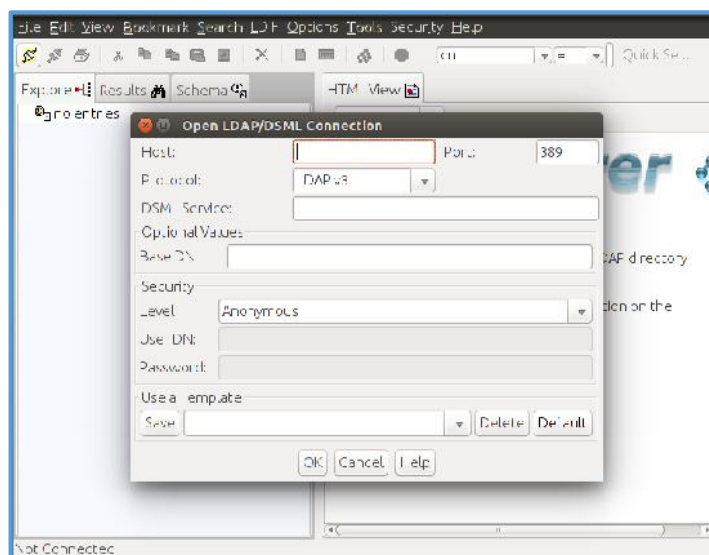


Ilustración 65: Ventana de conexión a un servidor LDAP.

Se ingresan los datos del usuario administrador y el DN donde se encuentra localizado e ingresamos al servidor LDAP

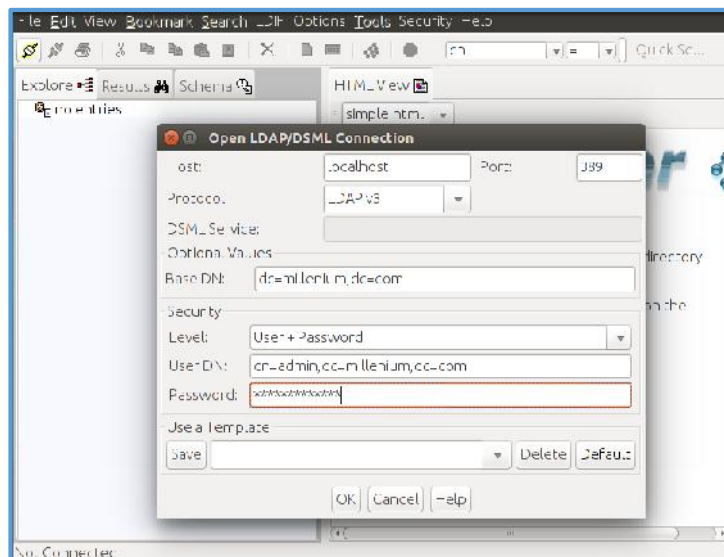


Ilustración 66: Datos para la conexión al servidor LDAP mediante JXplorer.

La conexión al servidor LDAP muestra la plantilla de grupos registrada:

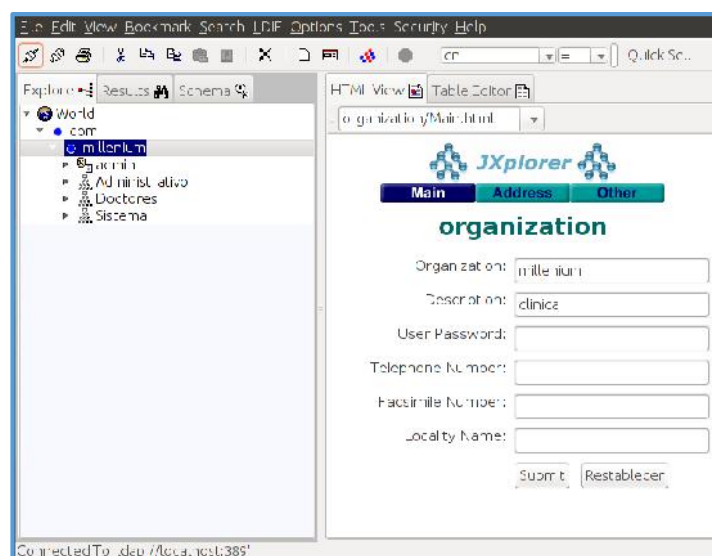


Ilustración 67: Menú del servidor LDAP JXplorer – grupos registrados.

Verificamos que los usuarios se hayan registrado en los grupos respectivamente, desplegamos los grupos:

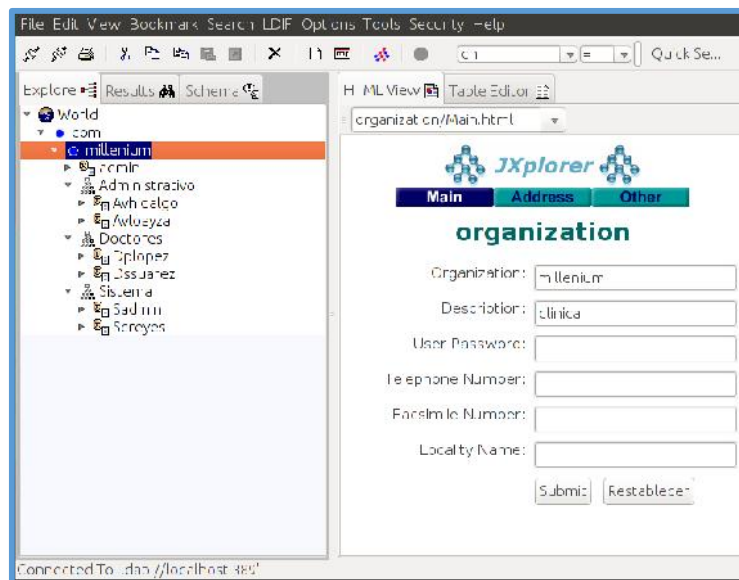


Ilustración 68: Menú del servidor LDAP JXplorer – usuarios registrados.

6. Autenticación RADIUS - LDAP para usuarios:

a. RED WLAN

Laptops:

Para conectarse a la red inalámbrica de la clínica necesitamos el programa SecureW2. Se realizará las configuraciones correspondientes del equipo previamente a la ejecución del programa:

Iremos a **Inicio/Panel de Control** y hacemos click **Redes e Internet**.

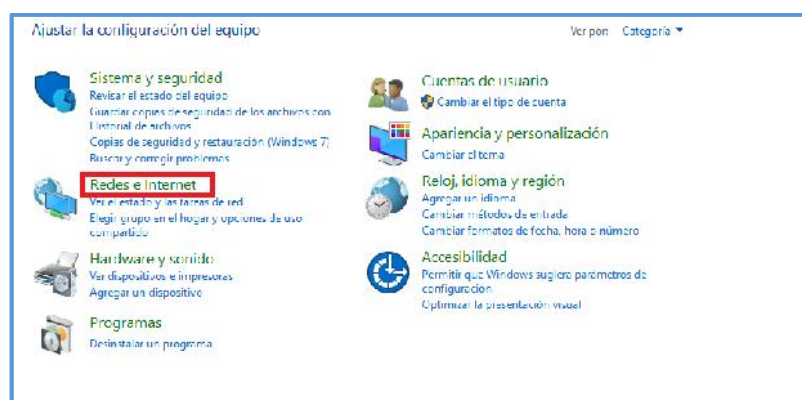


Ilustración 69: Configuraciones previas para usar securityW2 1.

Ahora vamos a **Centro de Recursos Compartidos**

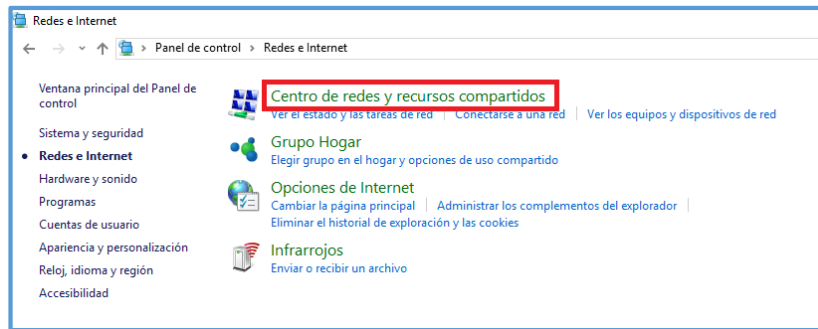


Ilustración 70: Configuraciones previas para usar securityW2 2.

Debemos agregar la nueva red inalámbrica. Para tal acción iniciaremos la función **Configurar una nueva conexión o red**.

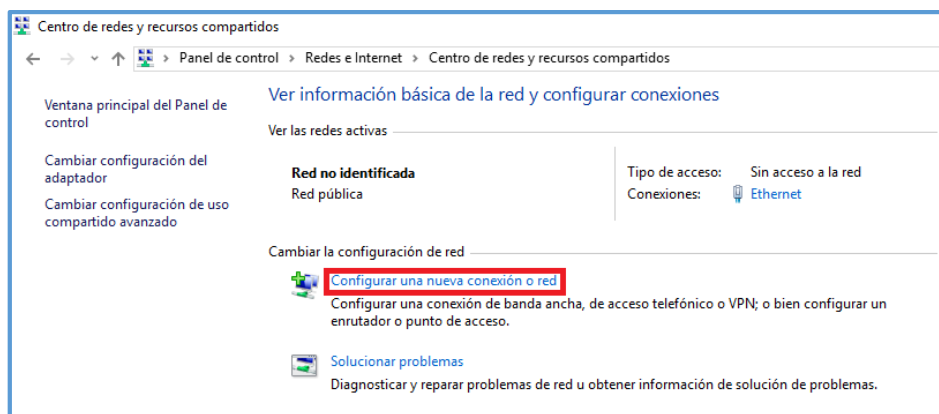


Ilustración 71: Configuraciones previas para usar securityW2 3.

La nueva red se creará manualmente.

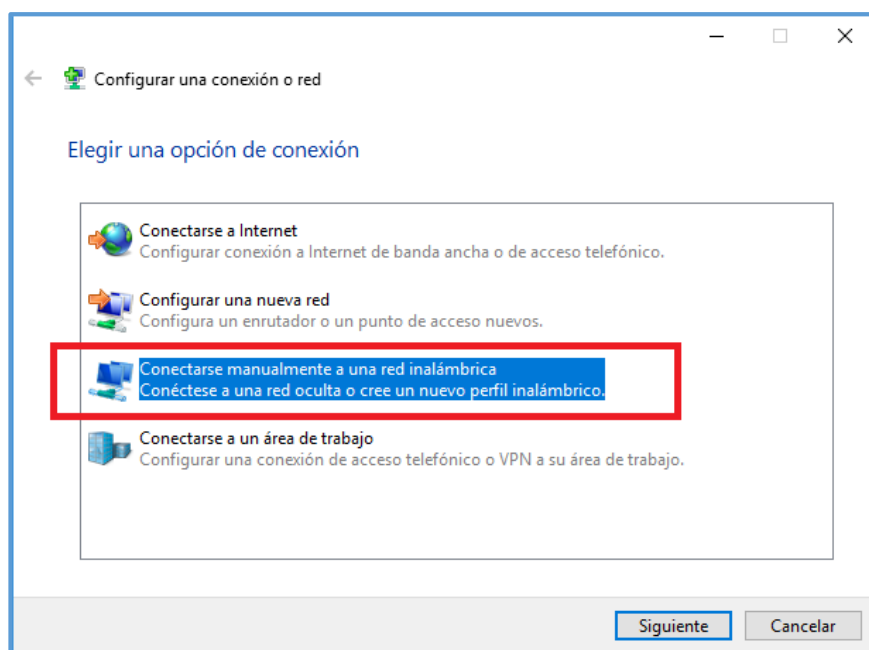


Ilustración 72: Configuraciones previas para usar securityW2 4.

Se registra los datos de la red.

Conectarse manualmente a una red inalámbrica

Escriba la información de la red inalámbrica que desea agregar.

Nombre de la red: apradius

Tipo de seguridad: WPA2-Enterprise

Tipo de cifrado: AES

Clave de seguridad: ☐ Ocultar caracteres

☒ Iniciar esta conexión automáticamente

☐ Conectarse aunque la red no difunda su nombre

Advertencia: esta opción podría poner en riesgo la privacidad del equipo.

Siguiente Cancelar

Ilustración 73: Configuraciones previas para usar securityW2 5.

Después de verificar que se agregó correctamente la red, se debe **cambiar la configuración de conexión**.

Conectarse manualmente a una red inalámbrica

apradius se agregó correctamente.

→ Cambiar la configuración de conexión
Abra las propiedades de la conexión para cambiar la configuración.

Cerrar

Ilustración 74: Configuraciones previas para usar securityW2 6.

Elegimos el método de **autenticación de red (SecureW2)** y hacemos click en **Configurar**.

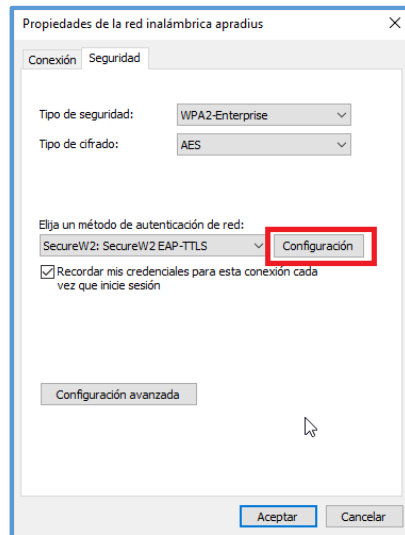


Ilustración 75: Configuraciones previas para usar securityW2 7.

El nombre de perfil queda tal cual, y nos dirigimos a **configurar**.



Ilustración 76: Configuraciones para usar securityW2 1.

Y se configura de la siguiente manera:



Ilustración 77: Configuraciones para usar securityW2 2.



Ilustración 78: Configuraciones para usar securityW2 3.



Ilustración 79: Configuraciones para usar securityW2 4.



Ilustración 80: Configuraciones para usar securityW2 5.

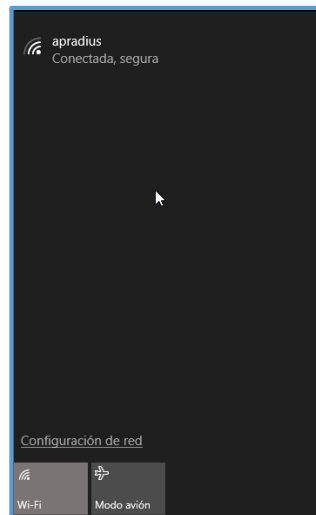


Ilustración 81: Verificación de conexión a la red inalámbrica.

Dispositivos Android:

Los dispositivos con SO Android, cuentan con un almacén interno de CA (Autoridad de Certificación) y admite la autenticación EAP-TTLS/PAP de forma nativa. Para conectarnos a la red inalámbrica debemos seleccionar el SSID (apradius) y marcar las siguientes opciones:

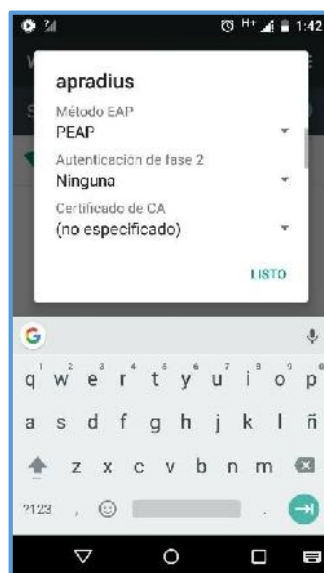


Ilustración 82: Configuración para la conexión a la red inalámbrica en SO Android 1.

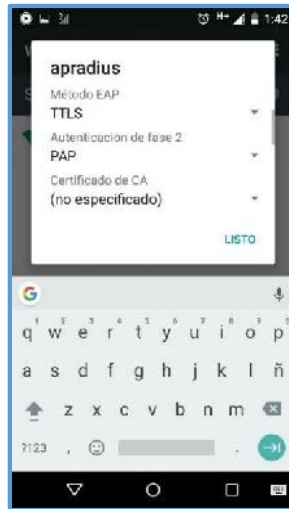


Ilustración 83: Configuración para la conexión a la red inalámbrica en SO Android 2.

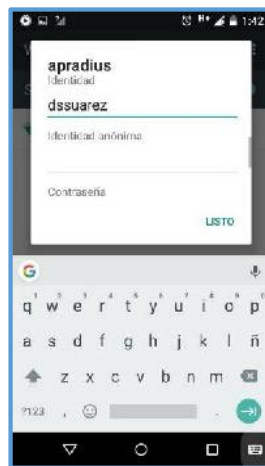


Ilustración 84: Configuración para la conexión a la red inalámbrica en SO Android 3.

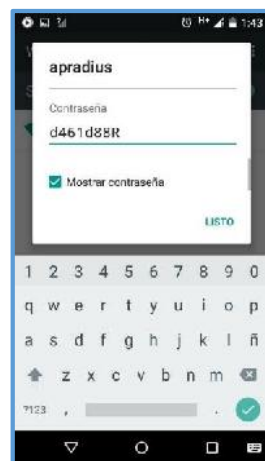


Ilustración 85: Configuración para la conexión a la red inalámbrica en SO Android 4.

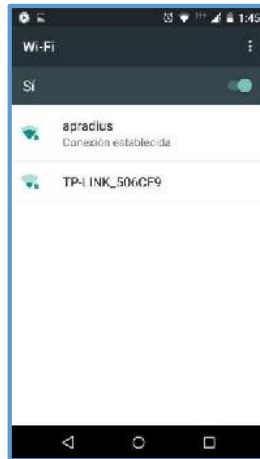


Ilustración 86: Verificación de la conexión a la red inalámbrica en SO Android.

b. RED LAN

Para reforzar los usuarios de escritorio que se conectan a la red mediante cable Ethernet utilizamos un *plug-in* llamado *PGINA*.

Plug-in PGINA

Empezamos la instalación aplicación el archivo ejecutable.

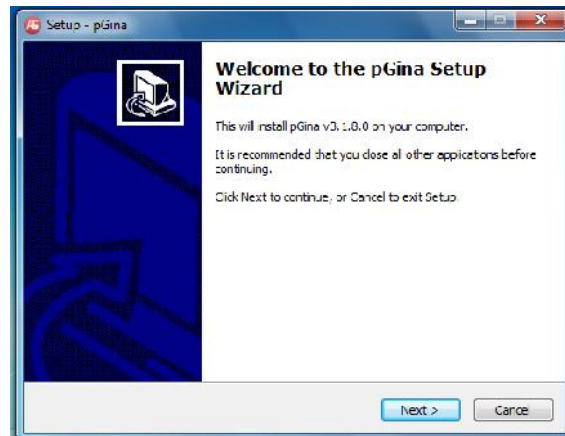


Ilustración 87: Instalación del plug-in PGINA - A.

A continuación, leeremos el acuerdo de licencia y aceptamos:

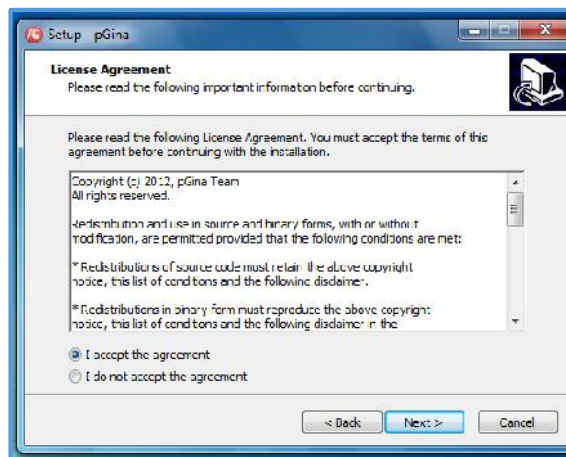


Ilustración 88: Acuerdo de Licencia Plug-in PGINA.

Especificamos la ruta o dirección del directorio dónde instalaremos el plug-in. En este caso utilizamos la configuración por defecto:

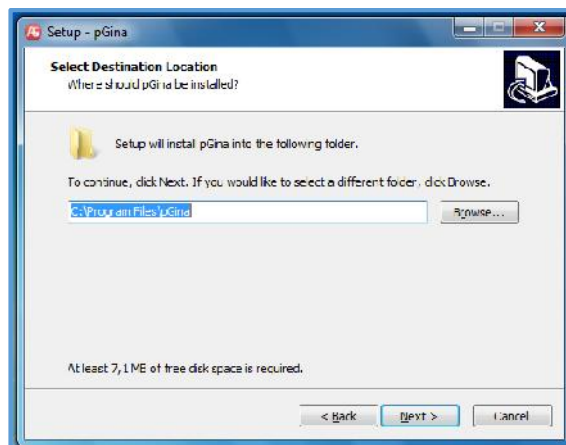


Ilustración 89: Selección destino de instalación del Plug-in PGINA.

Creamos el atajo para la ejecución del Plug-in:

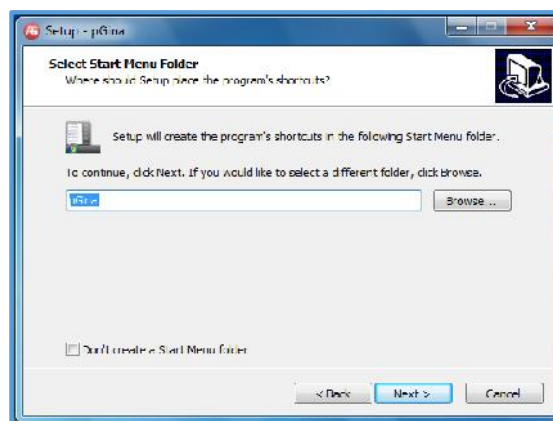


Ilustración 90: Creación del atajo para el Plug-in PGINA.

Colocaremos un icono en el escritorio para iniciar la configuración:

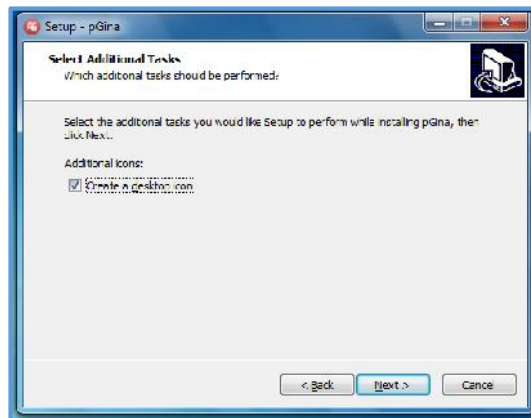


Ilustración 91: Icono de escritorio del Plug-in PGINA.

Instalamos el plug-in:

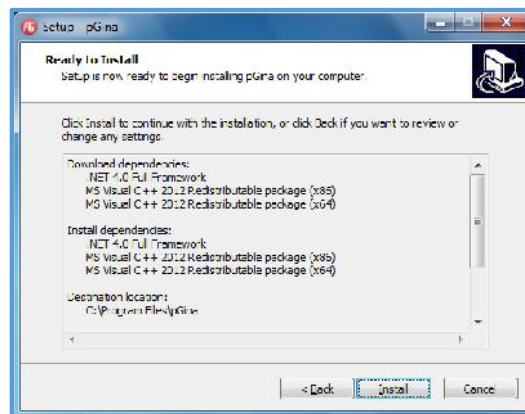


Ilustración 92: Instalación del Plug-in PGINA.

Terminamos la instalación y ejecutamos el plug-in:

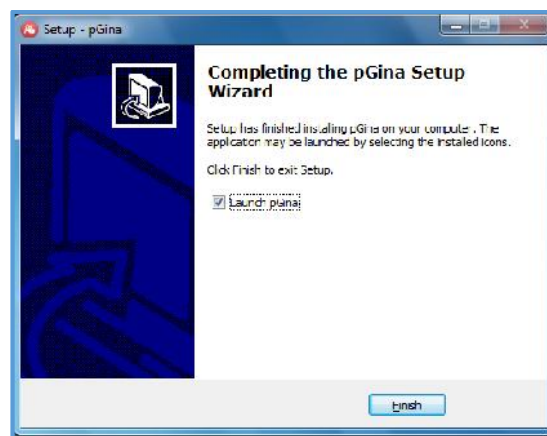


Ilustración 93: Fin de la instalación y ejecución del Plug-in PGINA.

Al iniciar el plug-in PGINA, mostrará una interfaz en la que tendremos visualiza la primera pestaña la cual muestra las configuraciones a manera general, cambiaremos de ventana arrastrando el mouse sobre la pestaña

Plugin selection:

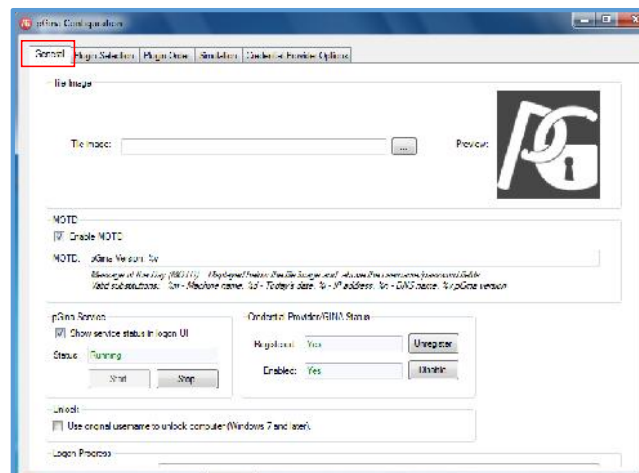


Ilustración 94: Plug-in PGINA menú principal.

La ventana de *Plugin Selection* contiene una lista de plugins que disponemos, la configuración por defecto es la siguiente:

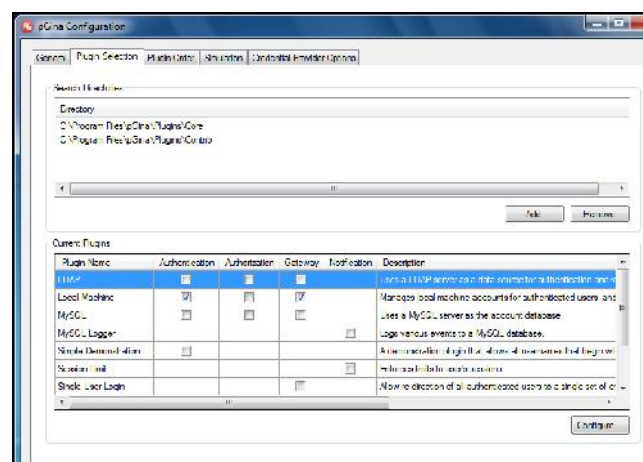


Ilustración 95: Plug-in PGINA pestaña Plugin selection por defecto.

Activamos los plugins para la autenticación AAA, después ejecutamos el botón *configure*:

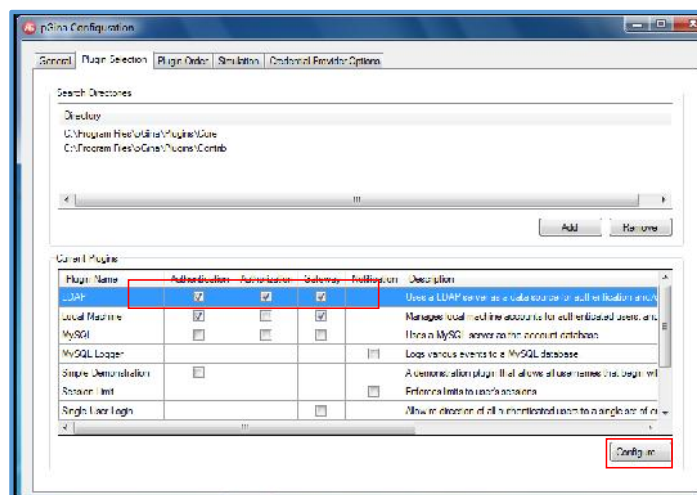


Ilustración 96: Plug-in PGINA pestaña Plugin selection correcta.

En la ventana *LDAP Plugin Settings* se agregarán los ajustes correspondientes para tener acceso al servidor LDAP mediante el usuario administrador, de esta manera podemos realizar la verificación del usuario de escritorio para el equipo correspondiente.

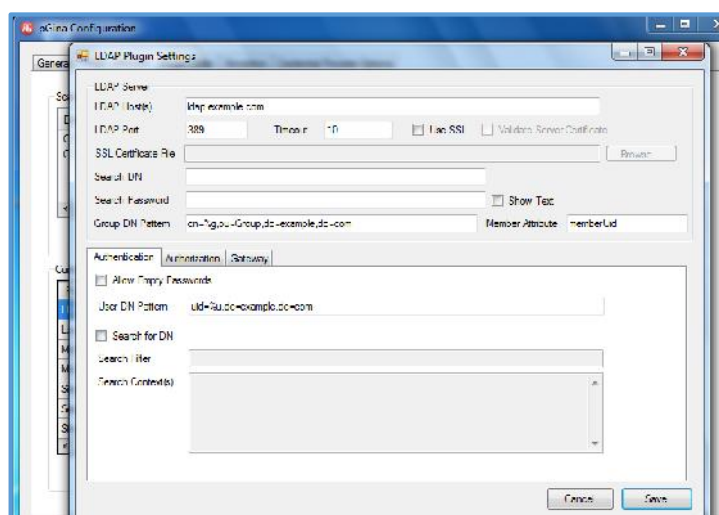


Ilustración 97: Plug-in PGINA pestaña Plugin Settings por defecto.

Registramos la información correspondiente sobre el servidor LDAP y el usuario administrador:

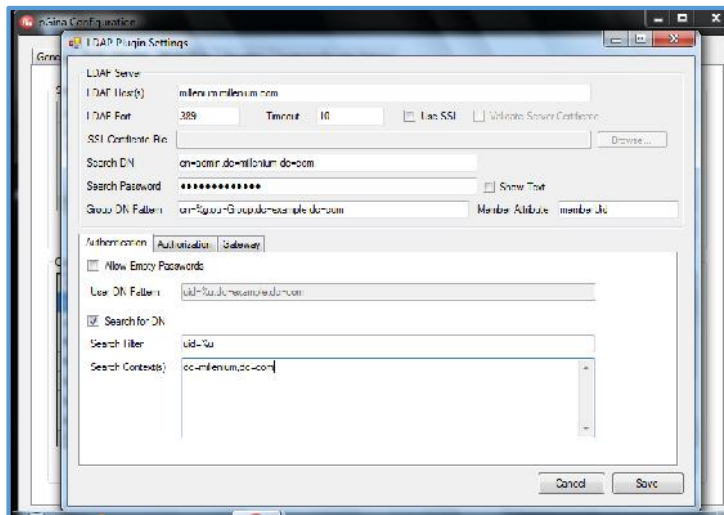


Ilustración 98: Plug-in PGINA pestaña Plugin Settings.

En la ventana de *Plugin order* se establece la jerarquía en lo referente a la consulta sobre a donde recurrir para el proceso de autenticación, autorización.

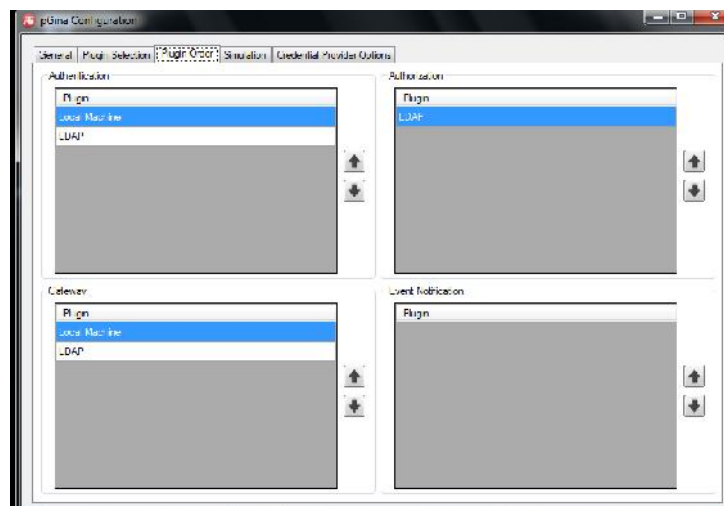


Ilustración 99: Plug-in PGINA pestaña Plugin Order por defecto.

Ahora establecemos prioridad en el orden para que la autenticación de usuario se dirija al servidor LDAP, verificamos que *LDAP* esté en prioridad:

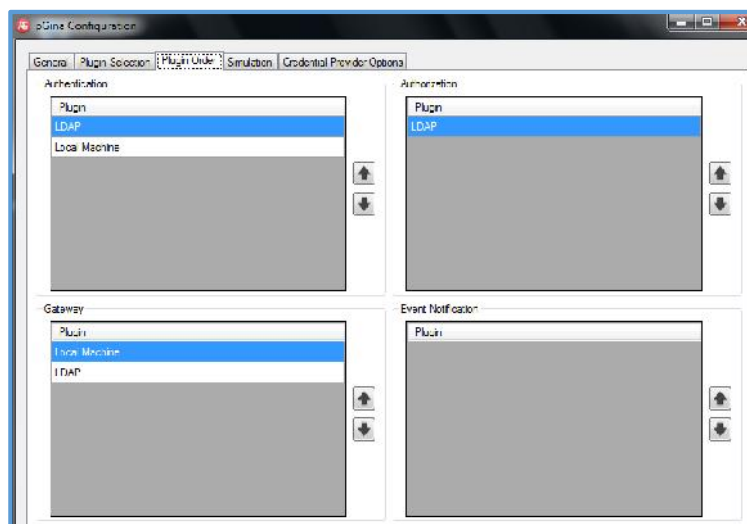


Ilustración 100: Plug-in PGINA pestaña Plugin Order correcta.

Para comprobar si la configuración hecha funcionará correctamente, en la pestaña *Simulation* realizaremos una prueba de autenticación de usuario a manera de simulación:

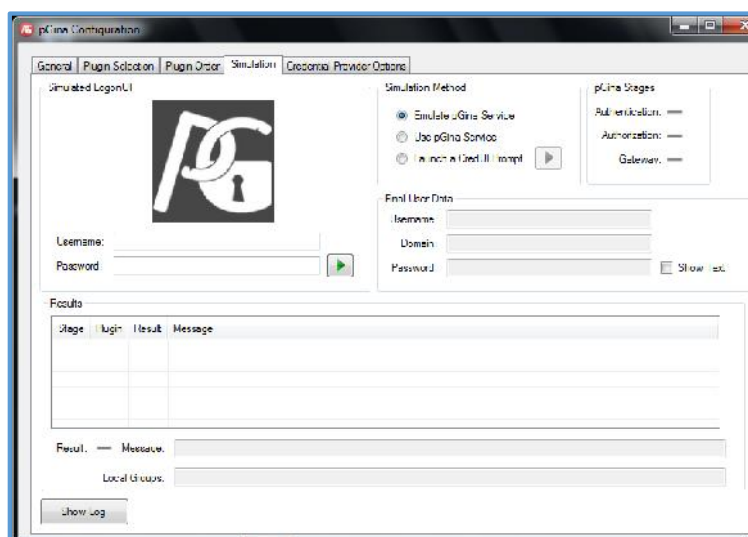


Ilustración 101: Plug-in PGINA pestaña Simulation por defecto.

Ingresamos los datos del Usuario *Dssuarez* y su contraseña correspondiente y ejecutaremos el botón de simulación:

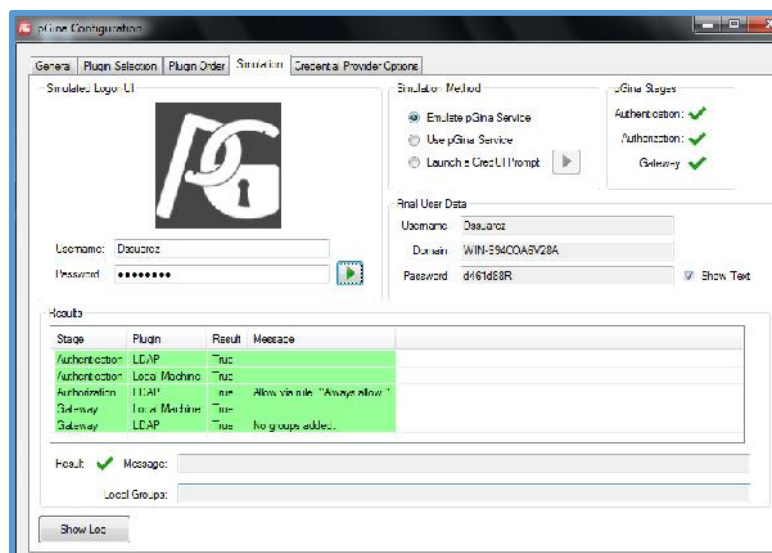


Ilustración 102: Plug-in PGINA pestaña Simulation. Prueba de un usuario LDAP.

Como se aprecia en la ilustración, la conexión al servidor, la autenticación del usuario y verificación de su contraseña es exitosa.

Lo siguiente es configurar que el ordenador al iniciar el sistema, nos solicite autenticarnos, se configuran los siguientes parámetros:

Debemos habilitar una de las directivas de seguridad local, aquella se ubica en el panel de control:

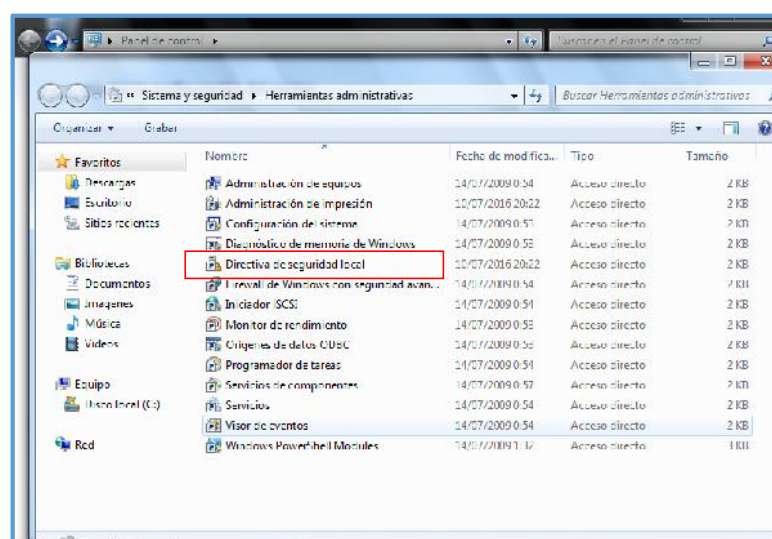


Ilustración 103: Panel de control Usuario de escritorio.

Entramos en la carpeta de directivas locales, dentro de ésta damos doble clic en la carpeta de opciones de seguridad:

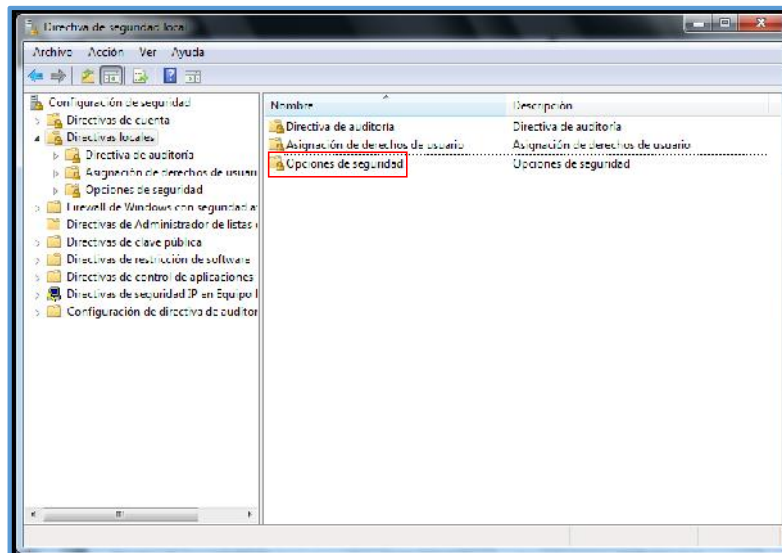


Ilustración 104: Carpeta de Opciones de Seguridad Local - Usuario de escritorio.

Y buscaremos la directiva de Inicio de sesión interactivo mostrar el último nombre de usuario:

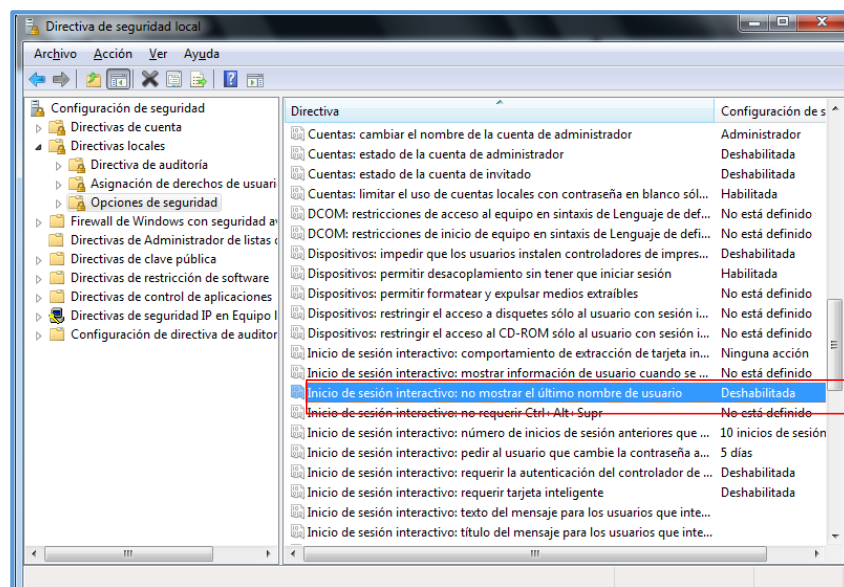


Ilustración 105: Directivas de Seguridad Local - Usuario de escritorio.

Habilitamos la directiva:

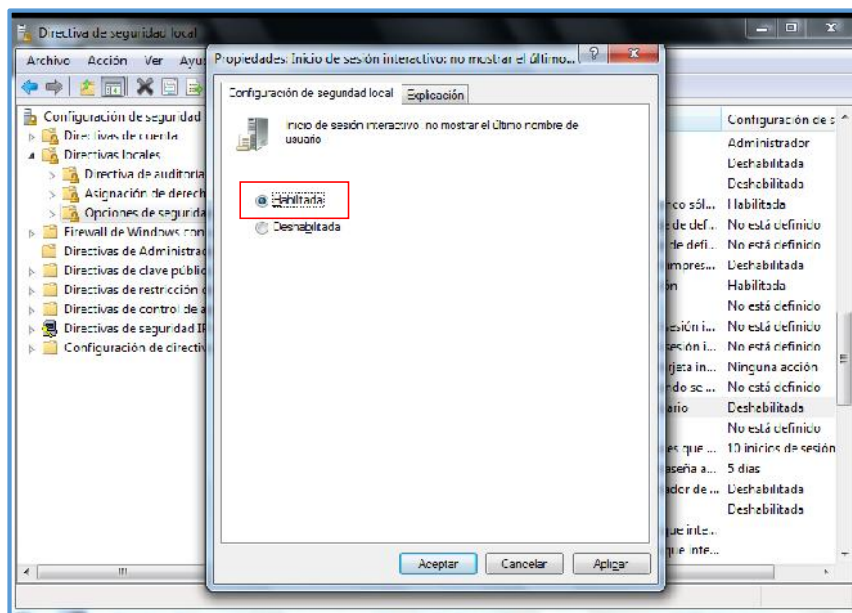


Ilustración 106: Habilitar Directivas de Seguridad Local - Usuario de escritorio.

Finalmente aceptamos y al reiniciar el equipo, éste solicitará un usuario y una contraseña del servidor LDAP para el ingreso.

5.2.4. Fase IV: Simulación de la estructura de red y Equipos Propuestos

5.2.4.1. Simulación en Packet Tracer

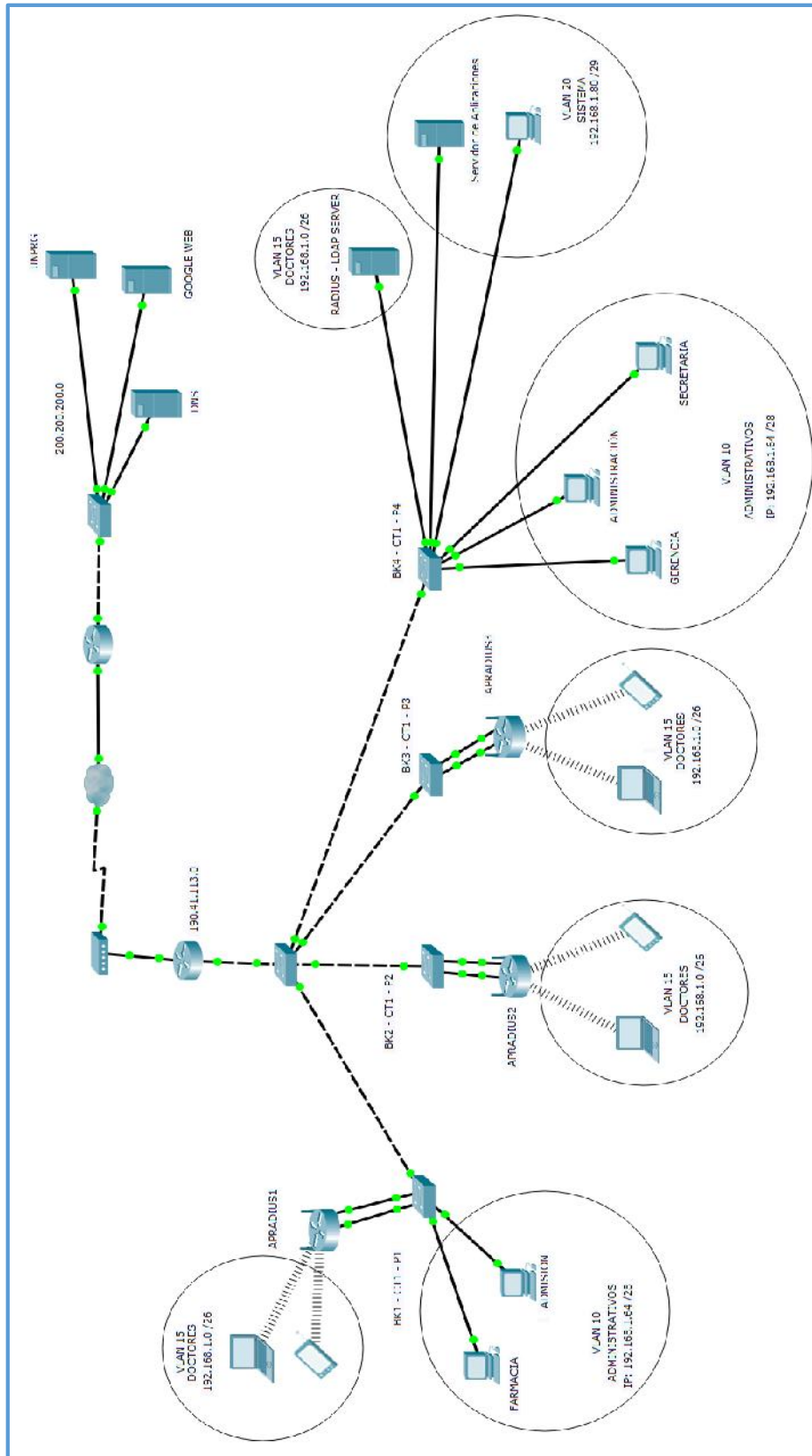


Ilustración 107: Simulación de la red propuesta.

5.2.4.2. Equipos Propuestos

Para el diseño de la red de la clínica, la configuración e integración de los servidores se propone utilizar equipos de marca **CISCO**. Estos equipos son de gama regular – alta diseñados para mejorar el rendimiento, calidad y administración de la infraestructura de red.

Los precios de los equipos son acordes a la excelente calidad, por ende, es una inversión que genera ventajas en la administración de la red y evita riesgos en pérdida, robo, de datos.




Presentamos algunas empresas fabricantes de equipos de telecomunicaciones:

EMPRESAS			
CISCO	3COM	ALCATEL	TRENDNET
Empresa productora de equipos de telecomunicaciones. Ofertan productos y servicios asociados: Router, Switches y redes de almacenamiento como principales equipos de venta. Reconocido por el enorme volumen de ventas sus productos y la calidad de estos.	Empresa fabricantes de tarjetas de red, switches, routers, Access Points, controladores, entre otros. En el año 2009 fue comprada por la empresa HP.	Empresa multinacional francesa dedicada a la venta de hardware, software y servicios a proveedores de servicios de telecomunicaciones, vende equipos de telefonía fija y móvil, redes de datos y distribución de video y televisión	Empresa dedicada a la venta de dispositivos de red. Amplia cartera de productos, abarca las categorías de dispositivos inalámbricos, por cable, de vigilancia, de conectividad y periféricos.

Tabla 25: Comparativa Empresas fabricantes de equipos de red.

Los equipos de red propuestos:

a) ROUTER:

Cisco 800 Series Routers	881	880VA	888
			
Implementación típica	Small branch, retail, or managed CPE	Small branch, retail, or managed CPE	Small branch, retail, or managed CPE
Cantidad de usuarios	1 - 20	1 - 20	1 - 20
Rendimiento	Up to 15 Mbps	Up to 15 Mbps	Up to 15 Mbps
Ethernet	Fast Ethernet 10/100	-	-
VDSL2/ADSL2+	-	Multimode VDSL2, ADSL2+, ADSL2 & ADSL1	-
SHDSL	-	-	Multimode EFM/ATM SHDSL
Fibra	-	-	-
3G/4G LTE	3.5G/3.7G HSPA+ or 3G EVDO	3.7G HSPA + or 3G EVDO	3.7 HSPA+
Serial	-	-	-
Puertos	4	4	4
802.11 wireless	2.4 GHz 802.11n Antena integrada; dual-band concurrent 2.4/5.0 GHz 802.11n Wi-Fi with DFS/CleanAir (Q4CY2012)	2.4 GHz 802.11n Antena integrada; dual-band concurrent 2.4/5.0 GHz 802.11n Wi-Fi with DFS/CleanAir (Q4CY2012)	2.4 GHz 802.11n Antena integrada
Voz	4 FXS , 1 FXO, 1 BRI	4 FXS, 2 BRI	-
PoE	2 puertos integrados PoE	2-port puertos integrados PoE	2-puertos integrados PoE
Protocolos de enrutamiento	RIPv1, v2, BGP, OSPF, EIGRP	RIPv1, v2, BGP, OSPF, EIGRP	RIPv1, v2, BGP, OSPF, EIGRP
IPv6	Sí	Sí	Sí
Servicios Avanzados IP	Actualizable	Actualizable	Actualizable
Video/medianet	Listo	Listo	Listo
Soporte VPN	GETVPN, DMVPN with licenciado	GETVPN, DMVPN with licenciado	GETVPN, DMVPN with licenciado

ScanSafe	Listo	Listo	Listo
IPsec tunnels	20	20	20
SSL VPN	Licenciado	Licenciado	licenciado
Filtrado de contenido	Licenciado	Licenciado	licenciado
Integrated WAN optimization - Cisco WAAS Express	1.5 Mbps optimizado; 30-75 conexiones TCP; licenciado	1.5 Mbps optimizado; 30-75 conexiones TCP; licenciado	1.5 Mbps optimizado; 30-75 conexiones TCP; licenciado
Visibilidad y Control de aplicaciones (AVC)	No	No	No
IOS Características de alta disponibilidad	Sí	Sí	Sí
Dimensiones máximas	1.9 x 12.8 x 10.4 in	1.9 x 12.8 x 10.4 in	1.9 x 12.8 x 10.4 in
Peso máximo	5.5 lb (2.5 kg)	5.5 lb (2.5 kg)	5.5 lb (2.5 kg)

Tabla 26: Comparación de Routers CISCO

ROUTER CISCO 880 series (C881-K9)

Se propone utilizar un **Router CISCO 880** conectado al IPS y encargada del enrutamiento de los datos que recibe del Switch.



Ilustración 108: Router CISCO 800 series.

Fuente: http://ecx.images-amazon.com/images/I/717e7NKZyZL._SL1500_.jpg

Descripción del producto:

El router cuenta con 4 puertos, posee servicios integrados que combinan el acceso a Internet, la seguridad y los servicios inalámbricos en un único dispositivo seguro. Ofrece velocidades de banda ancha y gestión simplificada.

Se pueden establecer las siguientes funciones:

- Firewall.
- Filtrado de contenido.
- Configuración de VLANs
- VPN y WLAN, a velocidades de banda ancha para pequeñas oficinas.
- Fácil instalación.
- Funciones de gestión centralizada

Datos técnicos:

GENERAL	
Anchura	<ul style="list-style-type: none"> • 32.5 cm
Profundidad	<ul style="list-style-type: none"> • 24 cm
Altura	<ul style="list-style-type: none"> • 4.3 cm
Peso	<ul style="list-style-type: none"> • 5 kg
Procesador / Memoria / Almacenamiento	
Memoria flash instalada (máx.)	<ul style="list-style-type: none"> • 128 MB Flash
Interfaz proporcionada	
Tipo de conector	<ul style="list-style-type: none"> • RJ-45
Interfaz	<ul style="list-style-type: none"> • Ethernet 10Base-T/100Base-TX
Cantidad	<ul style="list-style-type: none"> • 4
Tipo (FF)	<ul style="list-style-type: none"> • LAN
Interfaz	<ul style="list-style-type: none"> • Consola
Cantidad	<ul style="list-style-type: none"> • 1
Tipo (FF)	<ul style="list-style-type: none"> • Administración
Tipo (FF)	<ul style="list-style-type: none"> • WAN
Tipo de conector	<ul style="list-style-type: none"> • 4 PIN USB tipo A
Tipo (FF)	<ul style="list-style-type: none"> • USB
Diverso	
Método de autenticación	<ul style="list-style-type: none"> • RADIUS, TACACS +
Cumplimiento de normas	<ul style="list-style-type: none"> • AS / NZ 3548 Class B, CISPR 22, CISPR 24, EN 60555-2, EN 61000-3-2, EN 61000-3-3, EN

	61000-6-1, EN300-386, EN50082-1, EN55022, EN55022 Clase B, EN55024, FCC CFR47 Part 15, FCC CFR47 Part 15 B, ICES-003, ICES-003 Clase B, VCCI V-3
Algoritmo de cifrado	<ul style="list-style-type: none"> AES de 128 bits, 192 bits AES, 256-bit AES, DES, LEAP, PEAP, PKI, SSL, TKIP, Triple DES
Cumplimiento de normas	<ul style="list-style-type: none"> IEEE 802.1D, IEEE 802.1Q, IEEE 802.1x
Tecnología de conectividad	<ul style="list-style-type: none"> Cableada
Protocolo de interconexión de datos	<ul style="list-style-type: none"> Ethernet, Fast Ethernet
Transferencia de datos	<ul style="list-style-type: none"> 100 Mbps
Características	<ul style="list-style-type: none"> List (ACL) de control de acceso, señal ascendente automática (MDI / MDI-X), Detección de Reenvío Bidireccional (BFD), Class-Based Weighted Fair Queue Server (CBWFQ), filtrado de contenido, servidor DHCP, soporte DiffServ, proxy DNS, Dynamic Multipoint VPN (DMVPN), alta disponibilidad, snooping IGMP, Sistema de prevención de intrusiones (IPS), soporte IPv6, Link Fragmentación y entrelazado (LFI), equilibrio de carga, filtrado de dirección MAC, soporte de NAT, Calidad de Servicio (QoS), Spanning Tree Protocol (STP) de apoyo, Stateful Failover, Stateful Packet Inspection (SPI), limitación de tráfico, filtrado de URL, Forwarding-Lite (VRF-Lite), soporte VLAN, soporte virtual Ruta VPN failover WAN, Weighted Fair Queuing (WFQ)
Factor de forma	<ul style="list-style-type: none"> Externo
Factor de forma (FE)	<ul style="list-style-type: none"> Escritorio
Interruptor integrado	<ul style="list-style-type: none"> Conmutador de 4 puertos
Red de Protocolo de transporte	<ul style="list-style-type: none"> DDNS, DHCP, DNS, FTP, IPSec, L2TP, L2TPv3
Protocolo de gestión remota	<ul style="list-style-type: none"> HTTP, HTTPS, SNMP 3, SSH, Telnet
Protocolo de enrutamiento	<ul style="list-style-type: none"> BGP, EIGRP, GRE, HSRP, PNDH, OSPF, PIM-SM, RIP-1, RIP-2, VRRP
Indicadores de estado	<ul style="list-style-type: none"> Estado puerto, alimentación
Tipo	<ul style="list-style-type: none"> Router
Puertos WAN Cantidad	<ul style="list-style-type: none"> 1
Dispositivo de alimentación	

Factor de forma	<ul style="list-style-type: none"> • Externo
Frecuencia requerida	<ul style="list-style-type: none"> • 50/60 Hz
Voltaje nominal	<ul style="list-style-type: none"> • CA 120/230 V
Potencia suministrada	<ul style="list-style-type: none"> • 60 vatios
Tipo	<ul style="list-style-type: none"> • Adaptador de corriente
Garantía del fabricante	
Servicio y mantenimiento	<ul style="list-style-type: none"> • 1 año de garantía
Detalles de Servicio y Mantenimiento	<ul style="list-style-type: none"> • Garantía limitada - 1 año
Parámetros de entorno	
Temperatura mínima de funcionamiento	<ul style="list-style-type: none"> • 0 °C
Temperatura máxima de funcionamiento	<ul style="list-style-type: none"> • 40 °C
Ámbito de humedad de funcionamiento	<ul style="list-style-type: none"> • 10 - 85% (sin condensación)

Tabla 27: Datos técnicos Router CISCO 800 series.

Fuente: http://ds3comunicaciones.com/cisco/AIRONET_CISCO881_K9.html

Justificación

Fundamentado en la comparativa de los diferentes modelos de routers, se opta por utilizar el CISCO 880 series pues es uno de lo que provee características acordes a la necesidad de la Clínica (método de autenticación, capacidad suficiente para la cantidad de usuarios que conforman la entidad).

b) SWITCH:

Switch CISCO 2960-L (48 puertos)



Ilustración 109: Switch CISCO 2960-L 48 puertos.

Fuente: <http://www.impresoras.cl/impresoras/1374/WS-C2960-48PST-S.jpg>

Para la conexión entre usuarios se propone conectarlos con un switch CISCO 2960-L con 48 puertos, permite mayor productividad y dinamismo

empresarial, con funciones de seguridad que permiten que dichas transiciones en la red se realicen de manera segura y eficiente.

Características

- 48 Puertos Gigabit Ethernet con line-rate forwarding
- 2 or 4 Gigabit Small Form-Factor Pluggable (SFP) enlace ascendente
- Power over Ethernet Plus (PoE+) soporte con 370W de poder de alimentación
- Funcionamiento sin ventilador y temperatura hasta 55°C desplegar fuera del armario de cableado.
- Tiempo medio de vida entre fallos. (MTBF)
- Menos de 11,5 pulgadas de profundidad en uso con espacio ilimitado.
- Reducción del consumo de energía y las características avanzadas de gestión de energía
- Consola RJ45 y acceso USB para operaciones simplificadas.
- Interfaz de usuario web intuitiva para una fácil implementación y gestión

Datos técnicos:

PRODUCTO ID	10/100/1000 ETHERNET PORTS	UPLINK INTERFACES	DISPONIBLE ALIMENTACIÓN POE	FANLESS	DIMENSIONES (H X D X W)	PESO
WS-C2960L-48TS-LL	48	4 SFP	–	Y	1.73 x 9.45 x 17.5 in. (4.4 x 24 x 44.5 cm)	7.21 lb (3.27 kg)

Tabla 28: Datos técnicos Switch CISCO 2960-L

Justificación:

Se propone utilizar un Switch CISCO 2960L debido a que está diseñado para proveer rauda velocidad en la red, alto nivel de disponibilidad.

Se utiliza un switch de 48 puertos pues cumple con la capacidad actual de usuarios en la red de la clínica, de tener un incremento en la cantidad de usuario se cuenta con puertos aún disponibles.

c) ACCESS POINT:

TP-LINK TL-WR843N Wireless-N 300Mbps Router/Access Point



Ilustración 110: TP-Link TL-WR843N

Fuente: <https://www.computeralliance.com.au/InventoryImages/10787.jpg>

El TP-LINK Punto de Acceso Inalámbrico TL-WR843N está diseñado para establecer o ampliar una red inalámbrica de la clínica, alta velocidad escalable para conectar múltiples dispositivos.

Datos técnicos:

Interfaz	4 10/100Mbps LAN Ports 1 10/100Mbps WAN Port		
Antena	2*5dBi Omni Directional Antenna (RP-SMA)		
Fuente de alimentación externa	9VDC / 0.85A		
Normas inalámbricas	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b		
Dimensiones (W x D x H)	7.6 x 5.3 x 1.3 in.(192 x 134 x 33 mm)		
CARACTERÍSTICAS INALÁMBRICAS			
Frecuencia	2.4-2.4835GHz		
Velocidad de señal	11n: Up to 300Mbps(dynamic) 11g: Up to 54Mbps(dynamic) 11b: Up to 11Mbps(dynamic)		
Sensibilidad de recepción	270M:	-68dBm@10%	PER
	130M:	-68dBm@10%	PER
	108M:	-68dBm@10%	PER
	54M:	-68dBm@10%	PER
	11M:	-85dBm@8%	PER
	6M:	-88dBm@10%	PER
	1M:	-90dBm@8%	PER
Potencia de transmisión	CE: <20dBm FCC: <30dBm		
Seguridad inalámbrica	64/128/152-bit WEP, WPA / WPA2, WPA-PSK / WPA2-PSK		
CARACTERÍSTICAS DEL SOFTWARE			
Calidad de servicio	WMM, Bandwidth Control		

Tipo WAN	Dynamic IP/Static IP/PPPoE/PPTP(Dual Access)/L2TP(Dual Access)/BigPond
Administración	Access Control Local Management Remote Management
DHCP	Server, Client, DHCP Client List, Address Reservation
Reenvío de puertos	Virtual Server,Port Triggering, UPnP, DMZ
DNS Dinámico	DynDns, Comexe, NO-IP
VPN Pass-Through	PPTP, L2TP, IPSec (ESP Head)
Access Control	Parental Control, Local Management Control, Host List, Access Schedule, Rule Management
Seguridad de firewall	DoS, SPI Firewall IP Address Filter/MAC Address Filter/Domain Filter IP and MAC Address Binding
Protocolos	Support IPv4 and IPv6
Red de invitados	2.4GHz Guest Network x1

Tabla 29: Datos técnicos TP-LINK TL-WR843N

Justificación:

Se propone utilizar un TP-LINK Punto de Acceso Inalámbrico TL-WR843N pues se puede realizar las configuraciones correspondientes en éste, será utilizado como NIS para el servidor RADIUS. Proveerá la conectividad a los dispositivos inalámbricos.

d) FIREWALL:

Firewall Cisco ASA serie 5520



Ilustración 111. CISCO Firewall ASA 5520

Fuente:http://www.cisco.com/c/dam/en/us/support/docs/SWTG/ProductImages/Security-ASA-5520_frnt_back_rt_1000.jpg

El dispositivo de seguridad adaptable de la serie Cisco® ASA 5500 orientado a reforzar la seguridad en el acceso a la red de la clínica funcionando como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra.

Datos Técnicos:

Memoria (MB)	512
Memoria Flash del Sistema (MB)	64
Puertos integrados	4-10/100/1000 1-10/100
Cantidad máxima de interfaces virtuales (VLAN)	150
Ranura de expansión SSC/SSM	Sí (SSM)
CARACTERÍSTICAS	
Seguridad en la capa de aplicaciones	Sí
Funciones de firewall transparente de capa 2	Sí
Contextos de Seguridad (incluidos/máximos) 2	2/20
Inspección GTP/GRPS2	Sí
Compatibilidad con alta disponibilidad ³	A/A y A/S
Agrupación de VPN y equilibrio de carga	Sí

Tabla 30. Datos técnicos Firewall CISCO ASA 5520

Justificación:

La selección de un firewall CISCO ASA 5520 evitará la propagación de códigos maliciosos a través de la red. Accesos no autorizados o posibles intrusiones de terceros a la red corporativa.

CAPITULO VI: Costos y Beneficios

CAPITULO VI: Costos y Beneficios

6.1. Análisis de Costos y Beneficios

a) Hardware y materiales

MATERIAL	CANTIDAD	PRECIO	SUBTOTAL
Router CISCO 880 series	1	S/. 1725.00	S/. 1725.00
Firewall CISCO ASA 5520 series	1	S/. 20714.00	S/. 20714.00
Switch CISCO 2960 L-48TS-LL	1	S/. 7586.55	S/. 7586.55
Switch CISCO 2960 L-24TS-LL	4	S/. 5068.05	S/. 20272.20
TP-LINK TL-WR843N Wireless-N 300Mbps Router/Access Point	3	S/. 159.25	S/. 477.75
Cable UTP Cat. 6A marca PANDUIT 305 m.	2	S/. 776,38	S/. 1472.76
Conector RJ-45 macho	29	S/. 0.60	S/. 17.40
Conector RJ-45 hembra	29	S/. 10.16	S/. 294.81
Roseta	29	S/. 2.72	S/. 78.88
Canaletas SATRA 60 x 22	200	S/. 8.50	S/. 1700.00
TOTAL			S/. 54339.35

Tabla 31: Hardware y materiales

b) Software

SOFTWARE	PRECIO
VMWare Workstation versión 10	S/. 0.00
Ubuntu Server versión 14.04 TLS	S/. 0.00
FreeRADIUS	S/. 0.00
SLADP	S/. 0.00
Packet Tracer versión 7	S/. 0.00
JXplorer	S/. 0.00
SecureW2	S/. 0.00
Plug-in PGINA	S/. 0.00

Tabla 32. Costos de los Softwares utilizados

c) Recursos Humanos

ACTIVIDAD	SUBTOTAL
Instalación de cableado y activación	S/. 3000.00
Instalación, configuración de los dispositivos de red	S/. 400.00
Instalación, configuración e integración de los servidores	S/. 2500.00
TOTAL	S/. 5900.00

Tabla 33: Recursos Humanos

d) Resumen de Costos

MATERIALES	INVERSION
Hardware y materiales	S/. 54339.35
Software	S/. 0.00
Recursos Humanos	S/. 5900.00
TOTAL	S/. 60239.35

Tabla 34: Resumen de Costos

d) Factibilidad Económica

RUBRO	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
INGRESOS		S/. 5400000	S/. 5400000	S/. 5400000	S/. 5400000	S/. 5400000
Ventas	S/. 0	S/. 5400000	S/. 5400000	S/. 5400000	S/. 5400000	S/. 5400000
EGRESOS	S/. 1860319.18	S/. 1800000	S/. 1800000	S/. 1800000	S/. 1800000	S/. 1800000
Inversión Fija	S/. 60319.18					
Hardware y Materiales	S/. 54419.18					
Software	S/. 0					
Recursos Humanos	S/. 5900					
Capital de Trabajo	S/. 1800000	S/. 1800000	S/. 1800000	S/. 1800000	S/. 1800000	S/. 1800000
SALDO DE CAJA	S/. -1860319.18	S/. 3600000	S/. 3600000	S/. 3600000	S/. 3600000	S/. 3600000

Tabla 35. Flujo de Caja

TASA DE REFERENCIA	0.1
---------------------------	-----

Tabla 36. Tasa de referencia

	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5	TOTAL
VANI (10%)=		4909090.909	4462809.92	4057099.92	3688272.66	3352975.145	20470248.55
VANE (10%)=	1860319.18	1636363.636	1487603.31	1352366.64	1229424.22	1117658.382	6823416.185

Tabla 37. Valor Actual Neto

El análisis Beneficio/Costo es:

$$B/C E = \frac{VAN(\text{Ingresos})}{VAN(\text{Egresos})} = \frac{20470248.55}{6823416.185} = 3.00$$

Resumen de la evaluación económica

EVALUACIÓN ECONÓMICA	VAN	B/C
	S/. 13646832.365	3.00

Tabla 38. Evaluación Económica

En cuanto a la evaluación económica, por cada S/. 3.00 que recuperamos gastamos S/.1.00, teniendo en cuenta que el periodo de recuperación de la inversión económica es de 5 años.

Por consiguiente, se observa que, el B/C es > a 1 (3.00), esto quiere decir que la inversión para adquirir el hardware, software y recursos humanos es aceptable, lo que representa un beneficio de S/. 13646832.365

6.2. Beneficios

Beneficios Tangibles

La implementación del presente proyecto de investigación conectar las áreas de la clínica, y a su vez fortaleciendo la transferencia de información entre ellas.

A su vez proporciona una estructura más robusta de la física, resolviendo las caídas de la red LAN y WLAN.

Beneficios Intangibles

La integración de los servidores RADIUS-LDAP fortalecen la seguridad de la información dentro de la red de la clínica pues aumenta el nivel de acceso a la misma.

CAPITULO VII: Conclusiones

CAPITULO VII: Conclusiones

Hoy en día, la autenticación es una forma esencial para proteger el acceso a los recursos de información. Adicionalmente existen muchas herramientas que realizan tal labor enfocada a usuarios de una red, con sus ventajas y desventajas respectivamente.

Es relevante concluir anunciando que nada puede ser totalmente seguro, si existen desventajas en las herramientas, en su mayoría es debido a la naturaleza del protocolo que se utiliza y en algunos casos el punto débil del mecanismo de autenticación es el mismo usuario.

La integración de los servidores RADIUS – LDAP en la plataforma Linux permite:

- Al identificar las vulnerabilidades en la red de la clínica, obtuvimos información necesaria para utilizar las herramientas adecuadas y así fortalecer la seguridad disminuyendo considerablemente las vulnerabilidades mediante los mecanismos presentados en el informe.
- El diseño de esquema de red propuesto mediante la metodología Top Down Network Design, optimizó la red de la clínica la cual se encontraba sin un orden o administración eficaz para los servicios de telecomunicaciones.
- La simulación de la integración de los servidores RADIUS – LDAP demuestran notoriamente que la autenticación al acceso a la red de la clínica debe ser administrado para optimizar desde la calidad de servicios de la red interna y el ancho de banda.
- La creación de usuarios y políticas de acceso a la red, generan el deber de autenticarse si desean consultar o utilizar recursos de la red interna o externa. Mejora el control y distribución de recursos a los usuarios dentro de la red.
- El informe de seguridad detalla que los servidores AAA deben adaptarse a complejas exigencias que demanda la actualidad. De igual forma es necesario ofrecer a los usuarios un sistema convincente y confiable que incremente la productividad y que soporte de nuevos avances referidos a seguridad.

- También, se fortaleció la integración mediante configuración de VLANs, seguridad de puertos o interfaces, otorgando seguridad a los recursos de información.

El presente diseño de Sistema de seguridad de red, cumple con el objetivo principal del trabajo pues refuerza el control de acceso a usuarios de la Clínica Millenium – Chiclayo, a partir de herramientas de software libre para la autenticación en redes inalámbricas y a su vez se reutilizó para autenticar equipos con conexión cableada.

Este proyecto permitió obtener más conocimientos sobre el área de redes y seguridad informática, software libre enfocados a la autenticación, conocer protocolos modernos y robustos, éstos han sido establecidos para fortalecer el nivel de inseguridad informática que actualmente existe. Finalmente, el presente proyecto fue una oportunidad plausible para poner en práctica los conocimientos que adquirí durante mi ciclo de vida en la Universidad Nacional Pedro Ruiz Gallo.

CAPITULO VIII: Recomendaciones

- Es indispensable designar un ambiente correcto para la centralización de datos y seguridad física del servidor y dispositivos.
- Se debe realizar copias de seguridad o respaldo de la configuración de los dispositivos intermediarios, y de los servidores.
- Realizar periódicamente monitoreo y auditoría de red interna para tener conocimiento de la situación de ésta.
- Se recomienda contratar personal para el área de TI y capacitarlos para la administración de los servidores y dispositivos de red mencionados.

CAPITULO IX: Referencias Bibliográficas

CAPITULO IX: Referencias Bibliográficas

Bibliografía

Cepeda, i. (2012). *Implementacion de un cliente radius en linux*. Quito, ecuador.

Cmm. (13 de noviembre de 2015). *Ldap*. Obtenido de <http://es.ccm.net/contents/269-protocolo-ldap>

Definición de linux. (04 de abril de 2016). *Concepto definición*. Obtenido de <http://conceptodefinicion.de/linux/>

Delgado ortiz, h. (2010). *Seguridad en redes inalámbricas*. Lima - Perú: macro e.i.r.l.

Delgado ortiz, h. (2010). *Seguridad en redes inalámbricas*. Lima - Perú: macro e.i.r.l.

Dueñas, j. B. (octubre de 2012). Servidores dns. En j. B. Dueñas, *implementación de servidores con gnu/linux* (págs. 431 - 434). Creativecommons.

Facundo arena, h. (2011). *La biblia del linux*. Buenos aires - argentina: mp ediciones.

Gamainternet. (04 de abril de 2016). *Gama internet*. Obtenido de <http://wireless.gamainternet.com/glosario.html>

Informaticamoderna. (04 de abril de 2016). *Informatica moderna*. Obtenido de http://www.informaticamoderna.com/acces_point.htm

Lazo garcía, n. A. (2012). *Diseño e implementación de una red lan y wlan con*. Lima, Perú.

Ldap_linux. (13 de noviembre de 2015). *Servidor ldap*. Obtenido de <http://es.tldp.org/como-insflug/comos/ldap-linux-como/ldap-linux-como-1.html>

Masadelante. (04 de abril de 2016). *Mas adelante*. Obtenido de <https://www.masadelante.com/faqs/ancho-de-banda>

Metodologia redes. (04 de abril de 2016). *Metodologias para implementar proyectos de redes*. Obtenido de <http://metodologiaspararedes.blogspot.pe/>

Microsoft. (04 de abril de 2016). *Wikipedia*. Obtenido de [https://msdn.microsoft.com/es-es/library/hh831679\(v=ws.11\).aspx](https://msdn.microsoft.com/es-es/library/hh831679(v=ws.11).aspx)

Millenium, c. (2016). *Clinica milenium*.

- Miranda, c., villatoro, k., & hernández, r. (2012). *Implementación de un prototipo de red inalámbrica que permita elevar los*. San salvador, el salvador.
- Olvera morales, c. (2009). *Ipv6 para todos*. Buenos aires - argentina: asociación civil argentinos en internet.
- Propia, e. (2016). *Elaboración propia*.
- Pucp, r. T. (13 de noviembre de 2015). *Protocolos de confidencialidad e integración de datos*. Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1445/lazo_garcia_nuttsy_servidores_aaa.pdf?sequence=1
- Radius_1812. (13 de noviembre de 2015). *Radius*. Obtenido de <http://dtoapantano-shura.blogspot.pe/>
- Ramírez, o. (2013). *Modelo de seguridad, para un centro de operaciones de seguridad (soc)*. Mexico df, mexico.
- Real academia de ingeniería. (04 de abril de 2016). *Raing*. Obtenido de <http://diccionario.raing.es/es/lema/intranet>
- Sánchez, c. (2012). *Seguridad en redes inalámbricas usando herramientas de software libre*. Veracruz, méxico.
- Secur-it @c.r.s. (04 de abril de 2016). *Secur-it*. Obtenido de <https://securitcrs.wordpress.com/knowledge-base/glosario/>
- Servidor_Idap. (13 de noviembre de 2015). *Ventajas en el uso de Idap*. Obtenido de <https://comunicacionestux.wordpress.com/2009/11/10/servidor-ldap/>
- Tanenbaum, a. (2012). *Modelos de referencia: modelo de referencia tcp/ip*. Washington - estados unidos: person educacion de méxico.
- Ubuntu_mexico. (13 de noviembre de 2015). *¿qué es ubuntu?* Obtenido de <http://www.ubuntumx.org/queesubuntu.php>
- Unlp. (13 de noviembre de 2015). *Introducción a ipv6*. Obtenido de <http://www.cu.ipv6tf.org/pdf/ipv6-unlp.pdf>
- Villalón huerta, a. (2012). *Seguridad en unix y redes*. Gnu free documentation license.
- Web, g. D. (2016). *Glosario de informatica y de web*. Obtenido de <http://www.internetglosario.com/17/anchodebanda.html>

ANEXOS

A1. Instalación de VMware Workstation 10

VMware Workstation es un software de virtualización disponible para Mac, Linux y Windows. Permite instalar un sistema operativo en una máquina virtual, ejecutándose sobre el sistema operativo principal. Se crearon 2 máquinas virtuales, una asignada para la instalación Linux (Ubuntu server 14.04 LTS) y funcionó como servidor y la otra máquina se instaló sistema operativo Windows 7 pro que cumplió el papel de un cliente.

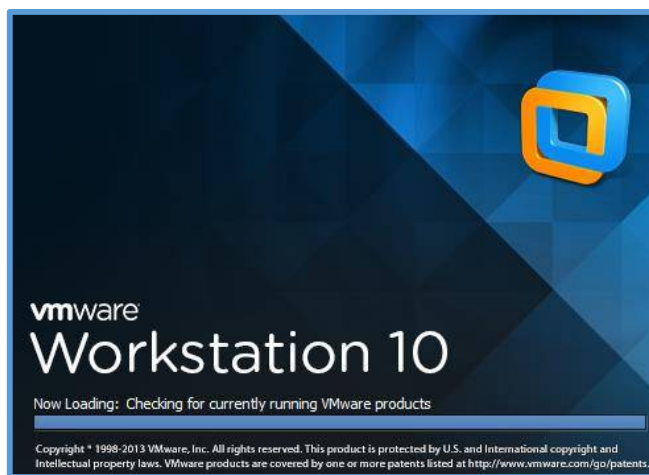


Figura A-1 VMware Workstation 6

La instalación se ejecuta con un asistente, aceptamos la licencia y clic en la opción *Siguiente* y continuamos la instalación, seleccionamos la ruta dónde almacenaremos el software e iconos que se crearan. Al finalizar se recomienda reiniciar el equipo.

A2. Configuración básica de máquina virtual Ubuntu Server 14.04 LTS

Ubuntu es una distribución Linux que ofrece un sistema operativo enfocado a soporte para servidores. Se escogió la versión 14.04 LTS (Long Term Support) pues reciben soporte durante cinco años y es la versión más estable actualmente.

Al iniciar el sistema operativo, éste por defecto aparece en modo consola, no tiene interfaz gráfica.

```
Ubuntu 14.04.4 LTS millenium tty1
millenium login: root
Password:
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 4.2.0-27-generic i686)

* Documentation:  https://help.ubuntu.com/

System information as of Sat Sep 17 18:35:05 PET 2016

System load: 1.98      Memory usage: 5%    Processes:   169
Usage of /:  4.5% of 18.32GB    Swap usage:  0%    Users logged in: 0

Graph this data and manage this system at:
https://landscape.canonical.com/

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@millenium:~#
```

Figura A -2 Ubuntu Server 14.04 LTS Modo Consola

Para realizar una correcta instalación de cualquier aplicación o configuración, actualizaremos los repositorios mediante, comandos. Es importante mencionar que el ingreso al sistema se realizó con el usuario *root*, ya no es necesario ingresar los comandos *sudo* o *su* para ingreso al superusuario:

```
root@millenium:~# aptitude update
```

```
root@millenium:~# aptitude upgrade
```

Una vez actualizado procedemos a instalar el modo gráfico:

Instalar GNOME con los programas básicos.

```
root@millenium:~# Aptitude install x-window-system-core gnome-core
```

```
root@millenium:~# startx
```

El sistema se reinicia y la interfaz gráfica se activa:



Figura A -3 Ubuntu Server 14.04 LTS Interfaz gráfica

Para una mejor administración e identificación del servidor se configuró el nombre del equipo, el cual sólo será visible dentro de nuestra red local y se le asignó una IP estática, se realizó mediante el editor nano:

Para salvar cambios en el editor *nano* debe realizarse con la combinación de teclas *Ctrl + o*, y finalmente salimos del editor con la combinación de teclas *Ctrl + x*.

```
root@millenium:~# nano /etc/hostname
```

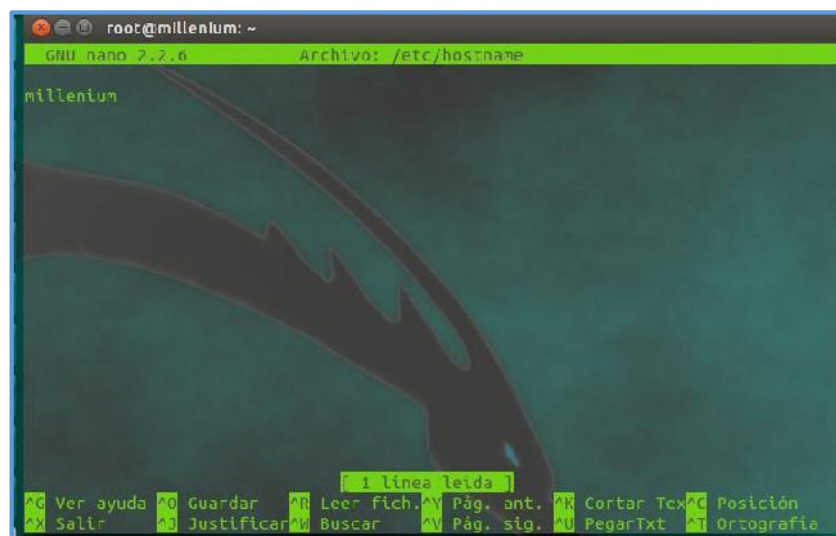


Figura A - 4 Ubuntu Server 14.04 LTS nombre del equipo

```
Root@millenium:~# nano /etc/hosts
```

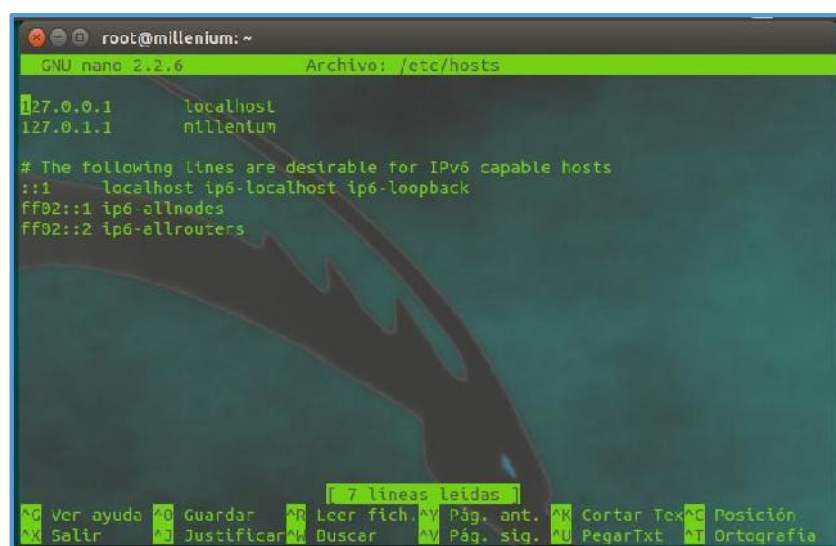
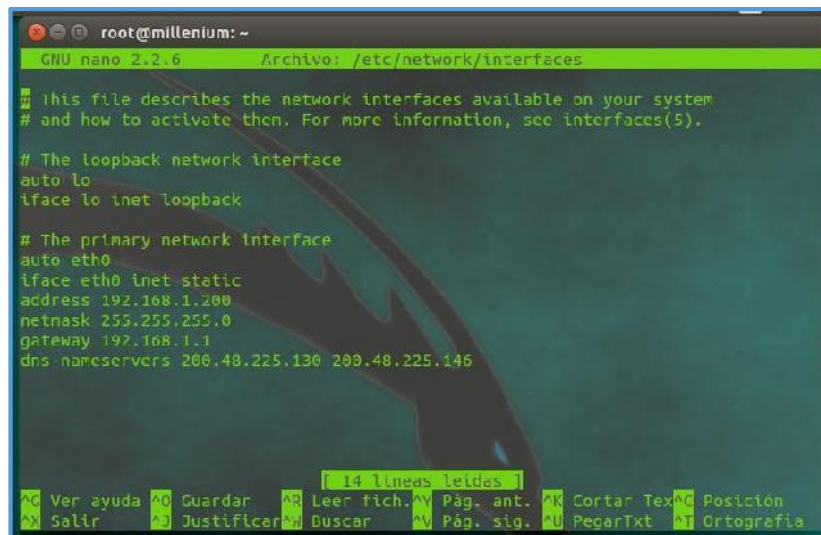


Figura A - 5 Ubuntu Server 14.04 LTS nombre del equipo

root@millenium:~# nano /etc/network/interfaces



```
root@millenium: ~
GNU nano 2.2.6 Archivo: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.200
netmask 255.255.255.0
gateway 192.168.1.1
dns nameservers 200.48.225.130 200.48.225.146

14 líneas leídas
Ver ayuda  Guardar  Leer fich.  Pág. ant.  Cortar Text  Posición
Salir  Justificar  Buscar  Pág. sig.  PegarTxt  Ortografía
```

Ilustración A - 6 Ubuntu Server 14.04 LTS Asignación de IP estática

A3. PREGUNTAS – ENCUESTA N° 01

ENCUESTA 01

Por favor, dedique unos minutos a completar esta pequeña encuesta. La información que nos proporcione será utilizada para optimizar el uso de las redes de telecomunicaciones de la Clínica Millenium:

1.- ¿En qué nivel de conocimiento en tecnologías de la información se considera?

- A) Básico
- B) Intermedio
- C) Avanzado

2.- ¿Cuenta con algún equipo de cómputo dentro de la Clínica?

- A) Sí
- B) No

3.- ¿El computador que está a su cargo, cuenta con conexión a la red LAN o internet?

- A) Sí
- B) No

4.- ¿En general, ¿cómo describiría el rendimiento del computador?

- A) Bueno
- B) Regular
- C) Malo
- D) No sabe / No contesta

5.- ¿En general cómo describiría el servicio de internet?

- A) Bueno
- B) Regular
- C) Malo
- D) No sabe / no opina

6.- ¿Usted usa la conexión inalámbrica (wifi) que la clínica proporciona?

- A) Sí

B) No

7.- ¿Con qué frecuencia utiliza el servicio de internet que la clínica proporciona?

A) Diariamente

B) Varias veces a la semana

C) Varias veces al mes

D) Varias veces al año

E) Nunca

8.- A través de qué equipo/equipos accede a Internet. Marque una o varias respuestas según el caso.

Respuesta Múltiple. Marque con una X

<input type="checkbox"/>	Ordenador portátil / Notebook
<input type="checkbox"/>	Teléfono Móvil (Smartphone)
<input type="checkbox"/>	Tablet
<input type="checkbox"/>	Otros

9.- ¿Tiene conocimiento si la cobertura de la red inalámbrica (wifi) abastece a la Clínica?

A) Sí

B) No

10.- ¿Usted considera necesario la distribución de la red inalámbrica (wifi) en toda la Clínica?

A) Sí

B) No

11.- ¿Cuáles son las consultas o búsquedas más frecuentes que usted realiza en internet?

Respuesta Múltiple. Marque con una X

<input type="checkbox"/>	Gestión Administrativa
<input type="checkbox"/>	Contenido Administrativo

	Contenido Médico
	Ocio

12.- ¿Cuáles son los mayores problemas que encuentra al utilizar el internet?

Respuesta Múltiple

	Velocidad
	Seguridad
	Demasiada Publicidad
	Caída de internet
	Otros problemas (mencionar): _____

13.- ¿Para Usted, qué es más importante en una red de computadoras?

A) Velocidad

B) Seguridad

C) Movilidad

D) Escalabilidad

14.- ¿En qué medida confía en el internet?

A) Ninguna confianza

B) No mucha confianza

C) Relativamente confiable

D) Mucha confianza

15.- ¿Tiene a su disposición algún equipo personal de cómputo?

A) Sí

B) No

16.- ¿Se contacta con sus pacientes a través de internet?

A) Sí

B) No

17.- ¿Usted cuenta con un usuario y contraseña para ingresar a un equipo de cómputo?

A) Sí

B) No

C) No sabe / No opina

18.- ¿En general, cómo describiría el servicio de atención al usuario del área de Sistemas?

A) Bueno

B) Regular

C) Malo

D) No sabe / no contesta

19.- ¿Con qué frecuencia ha experimentado la pérdida del servicio de Internet?

A) Diariamente

B) Varias veces a la semana

C) Varias veces al mes

D) Varias veces al año

E) Nunca

20.- ¿Con qué frecuencia ha experimentado la pérdida de información debida a alguna falla del equipo de cómputo?

A) Diariamente

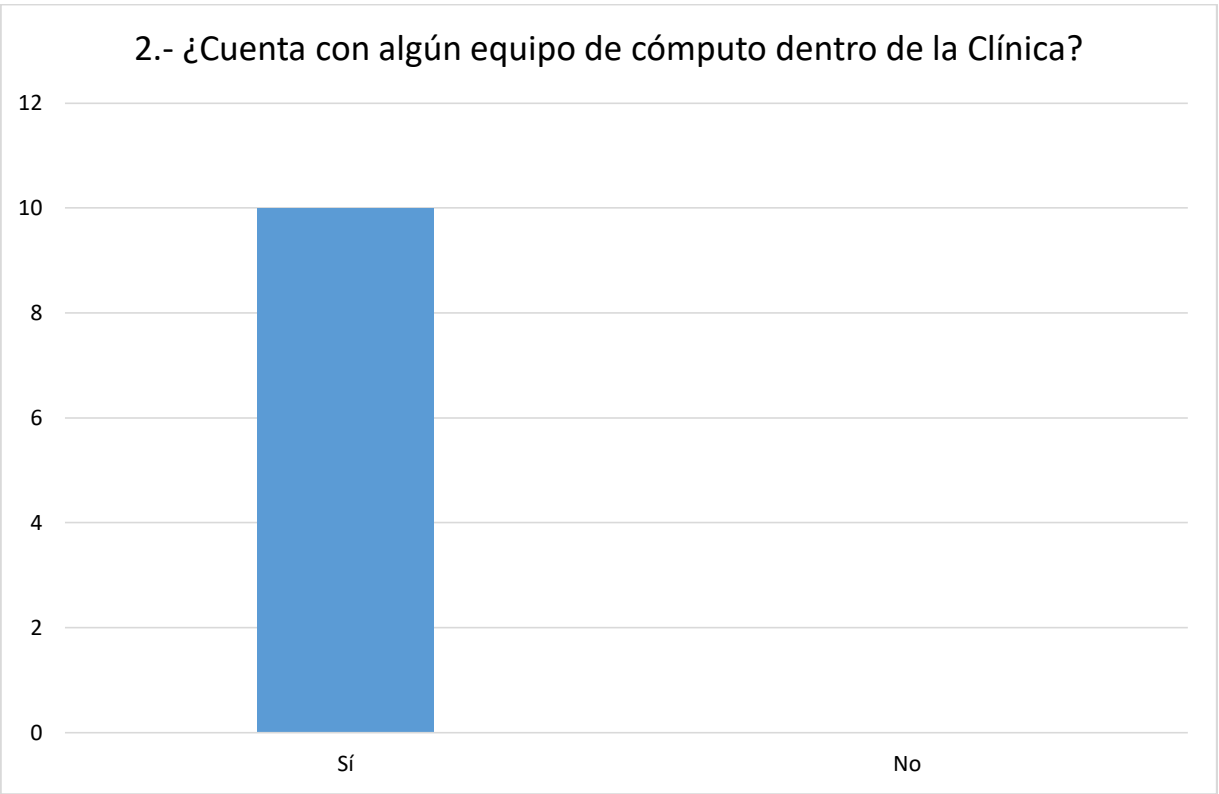
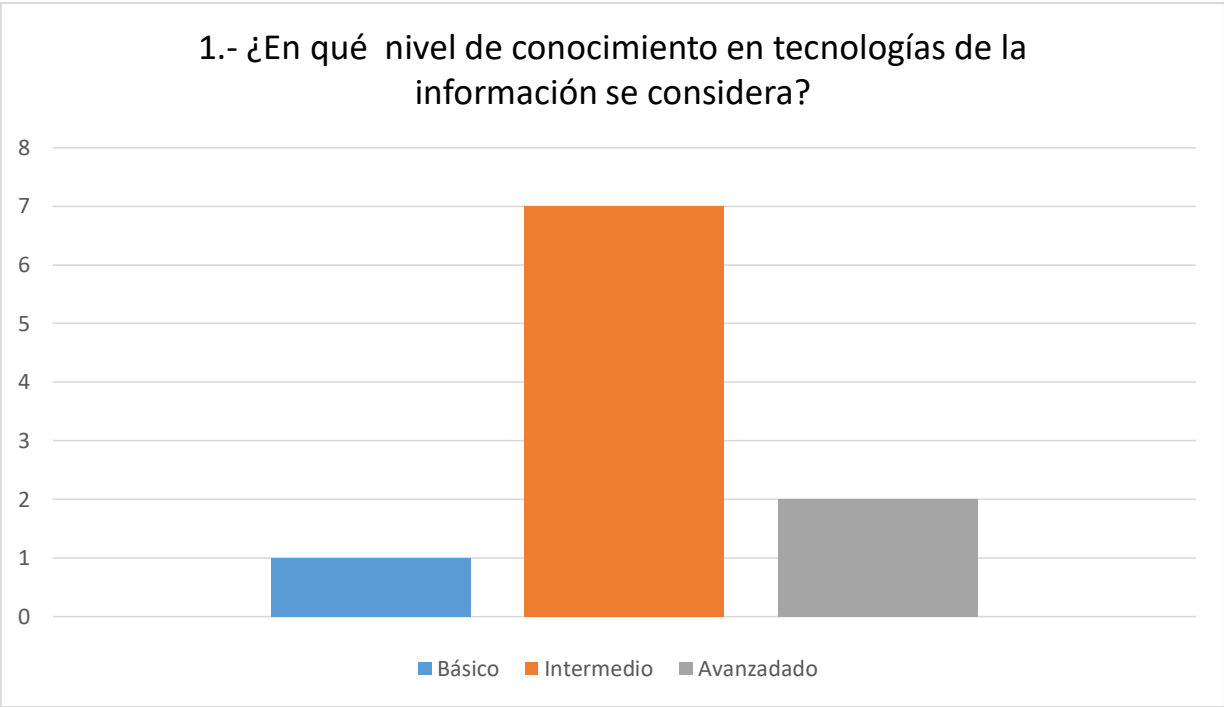
B) Varias veces a la semana

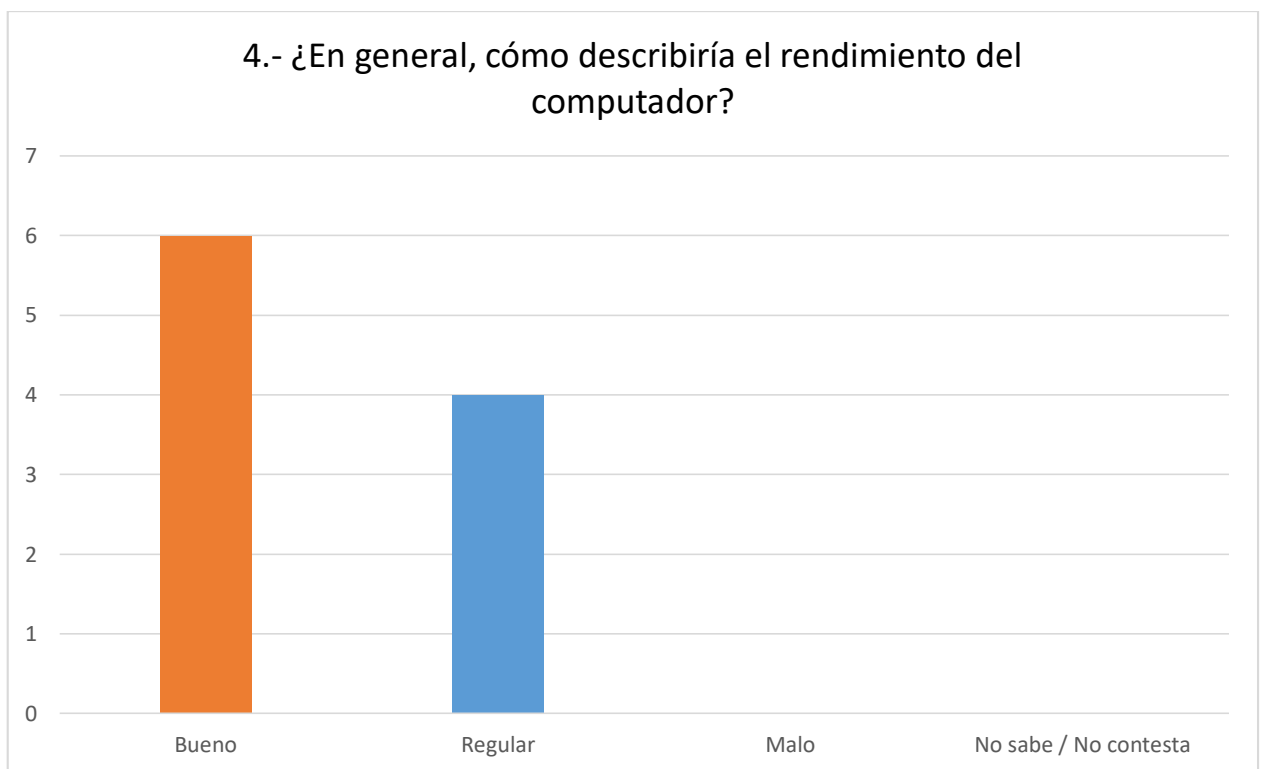
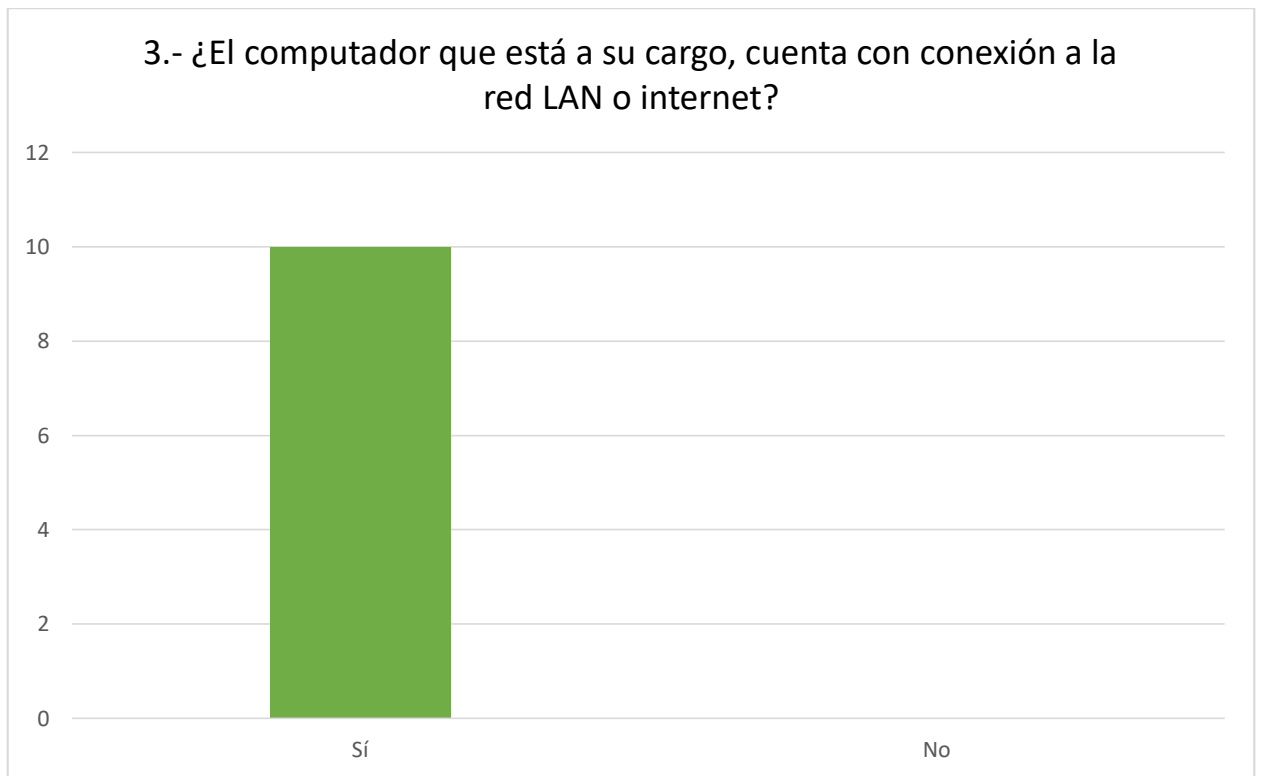
C) Varias veces al mes

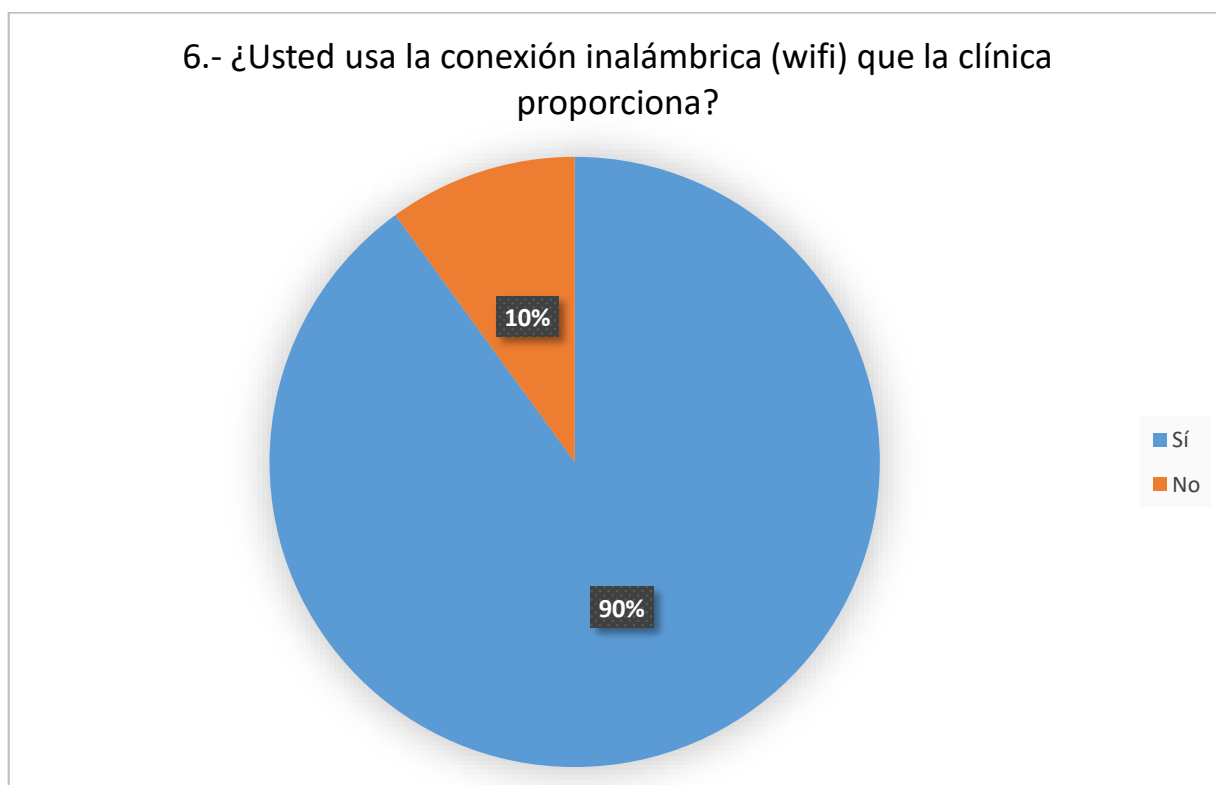
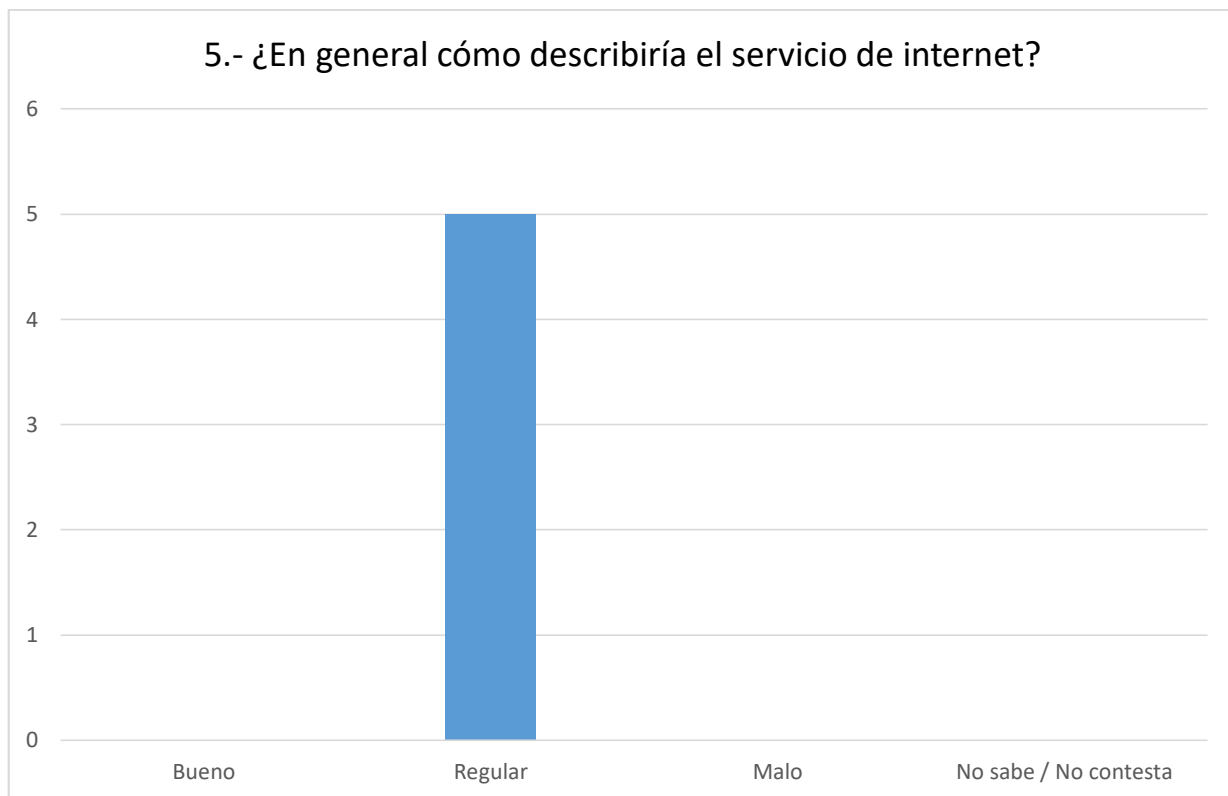
D) Varias veces al año

E) Nunca

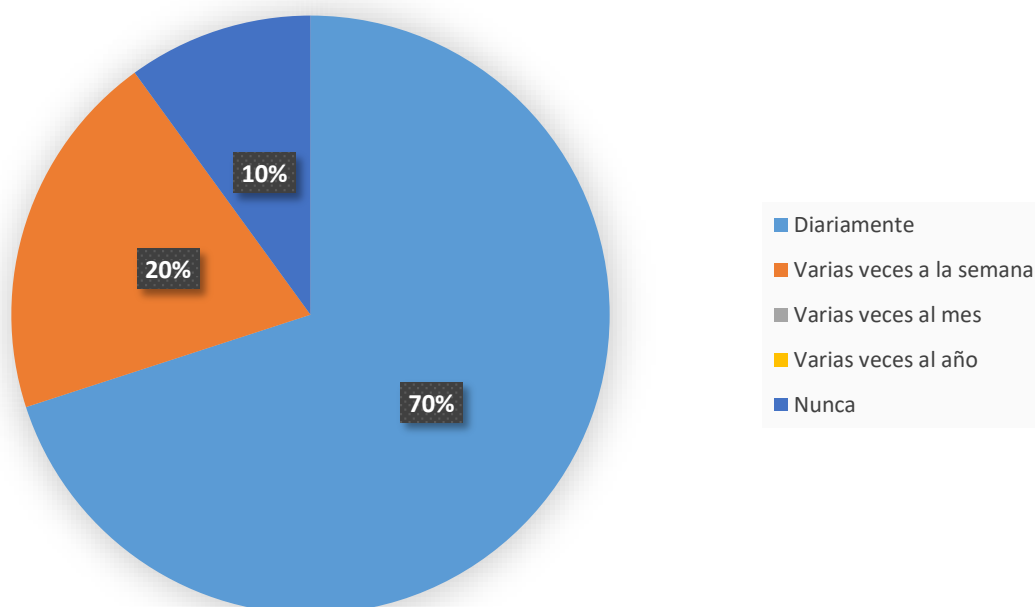
A4. RESULTADOS – ENCUESTA 01



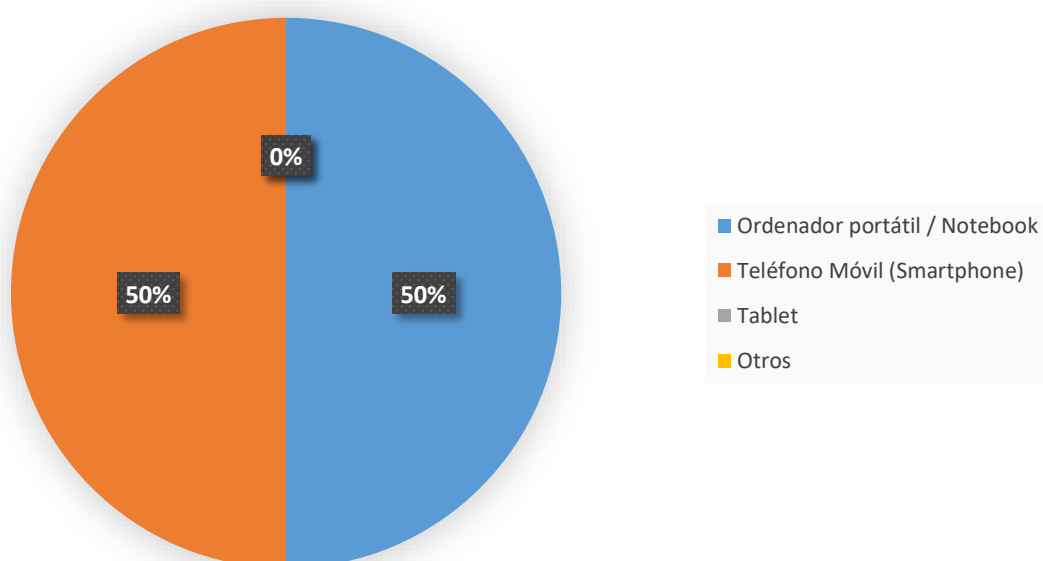


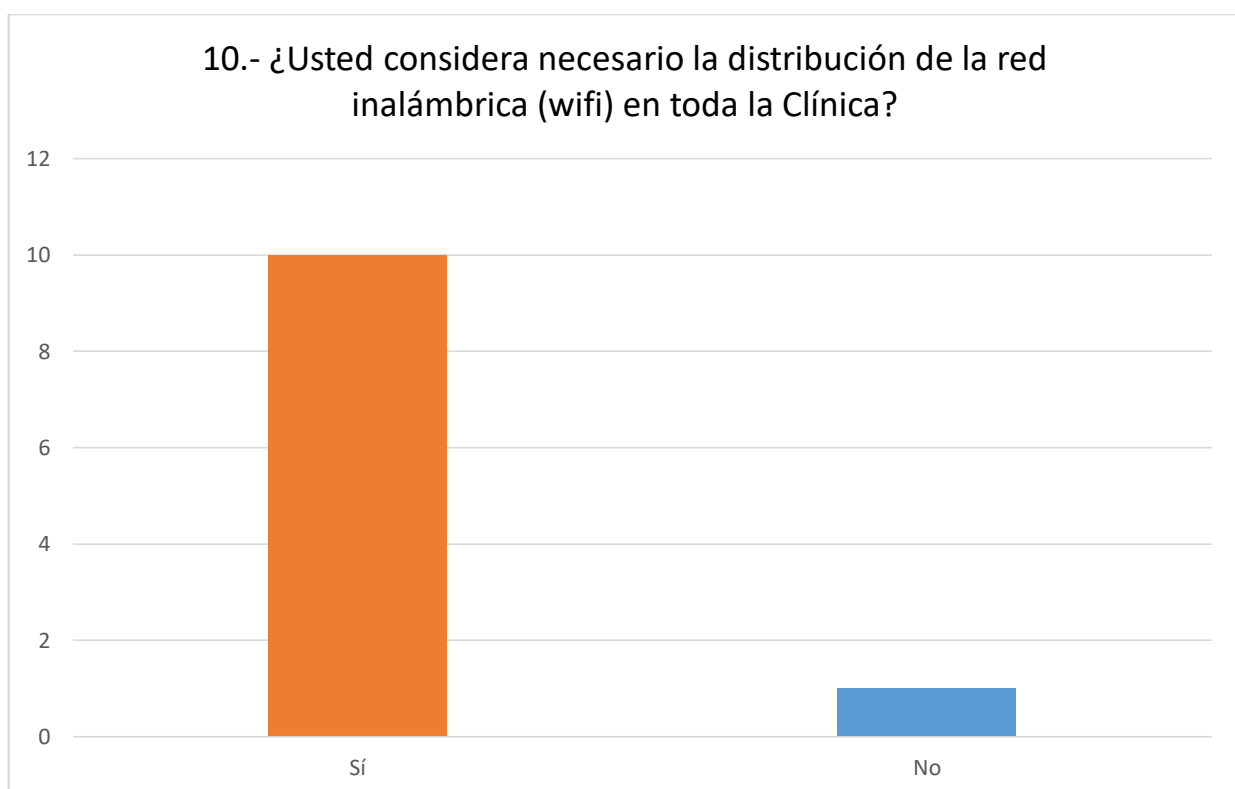
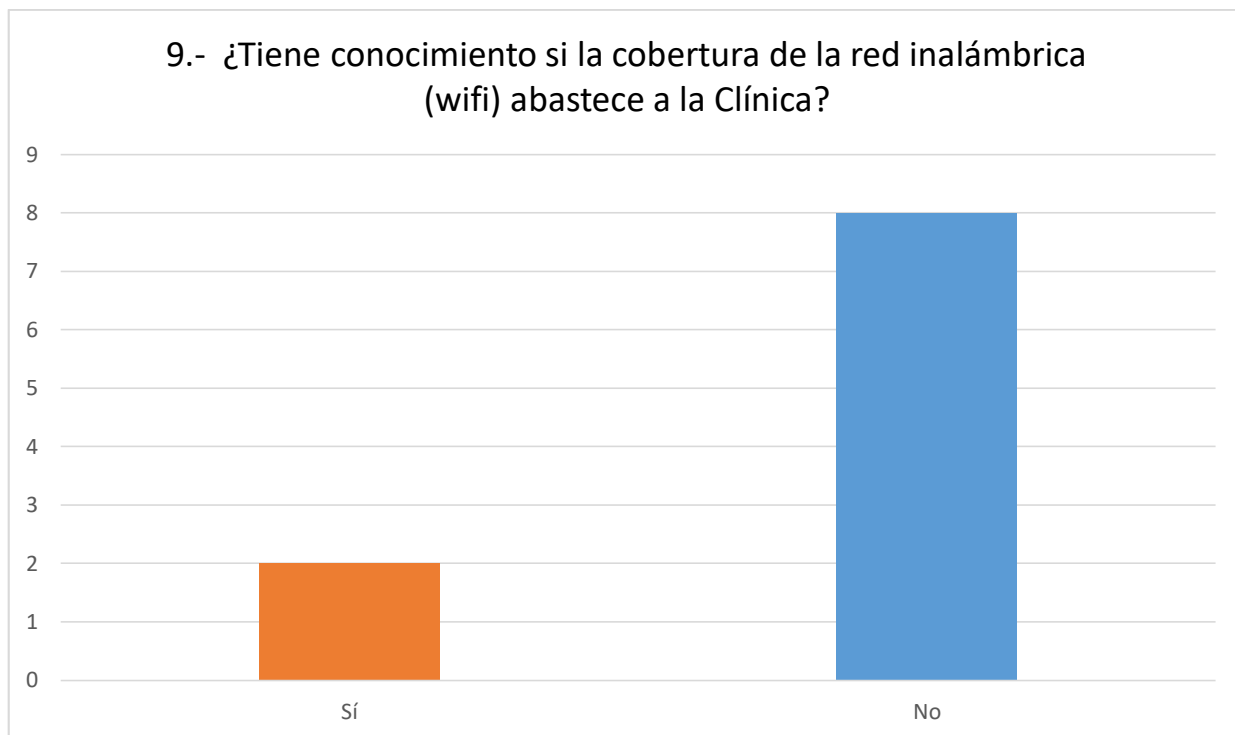


7.- ¿Con qué frecuencia utiliza el servicio de internet que la clínica proporciona?

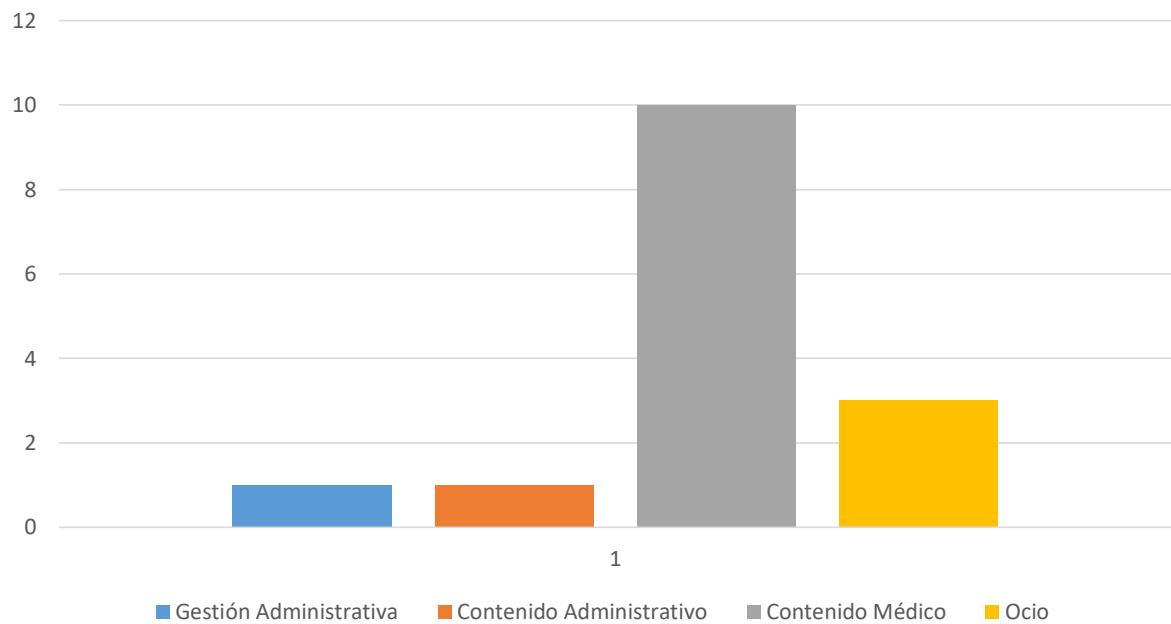


8.- A través de qué equipo/equipos accede a Internet. Marque una o varias respuestas según el caso.

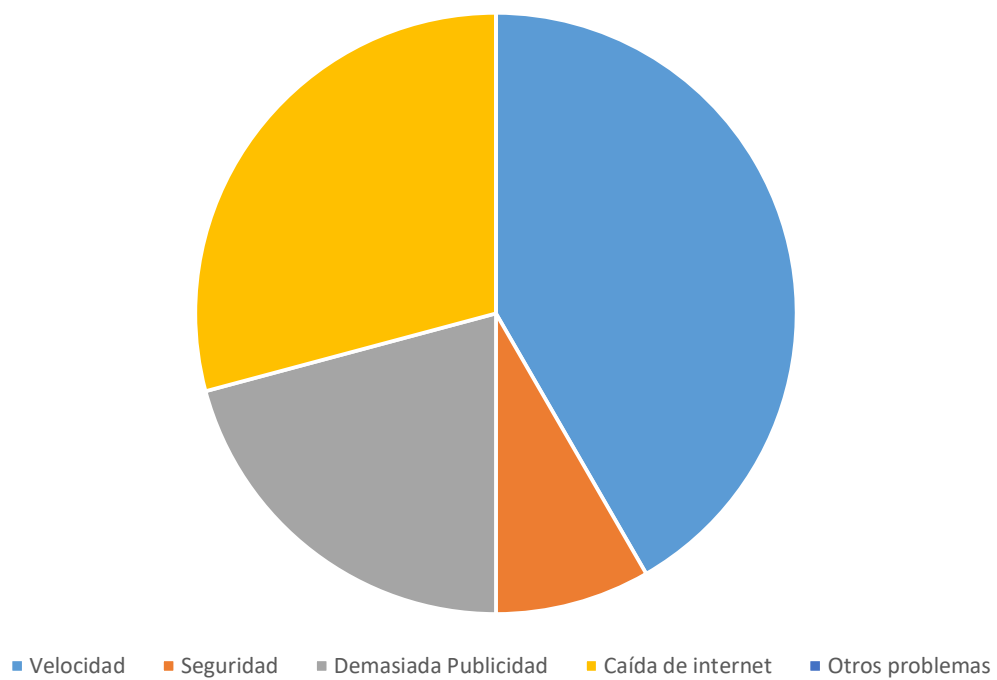


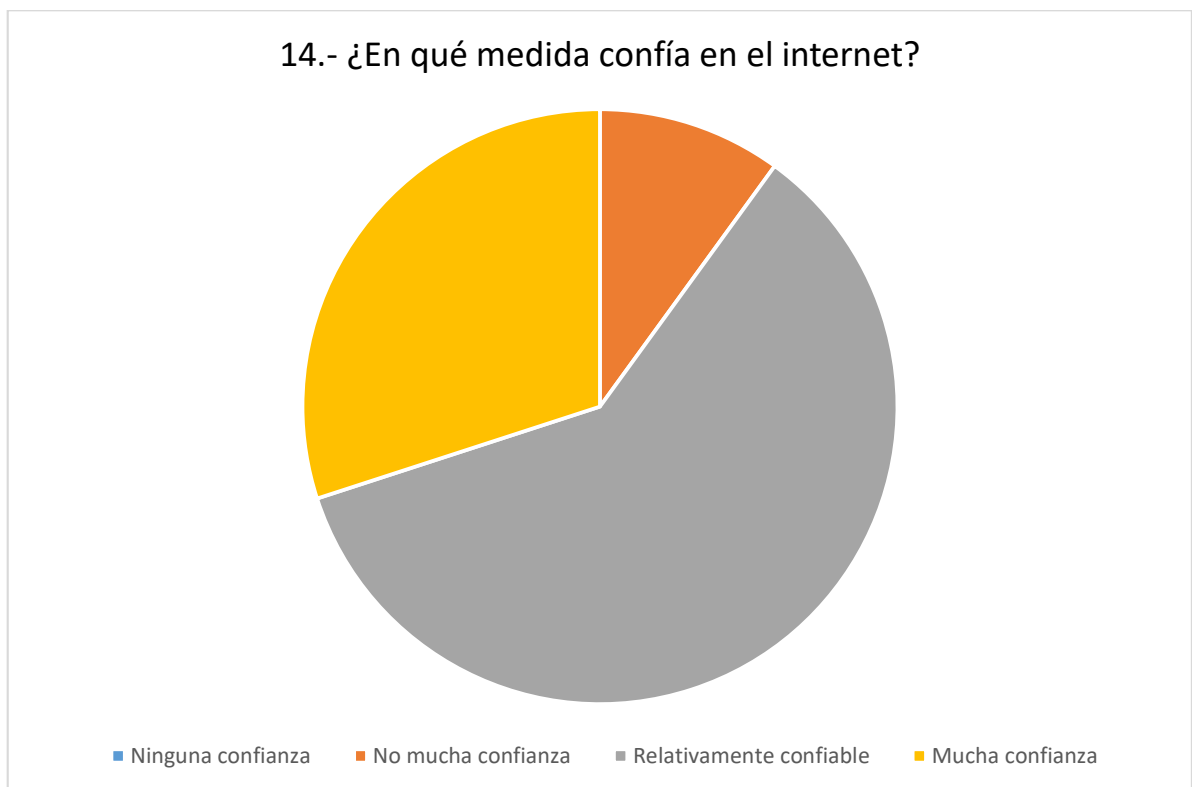
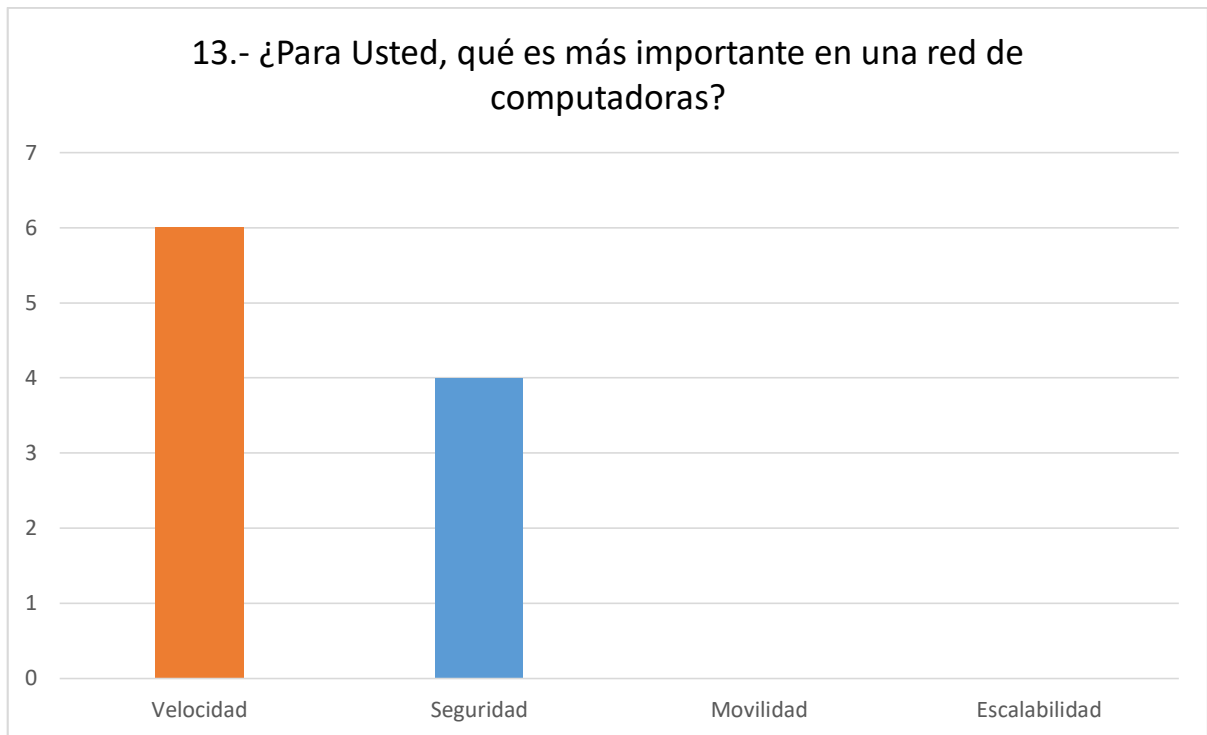


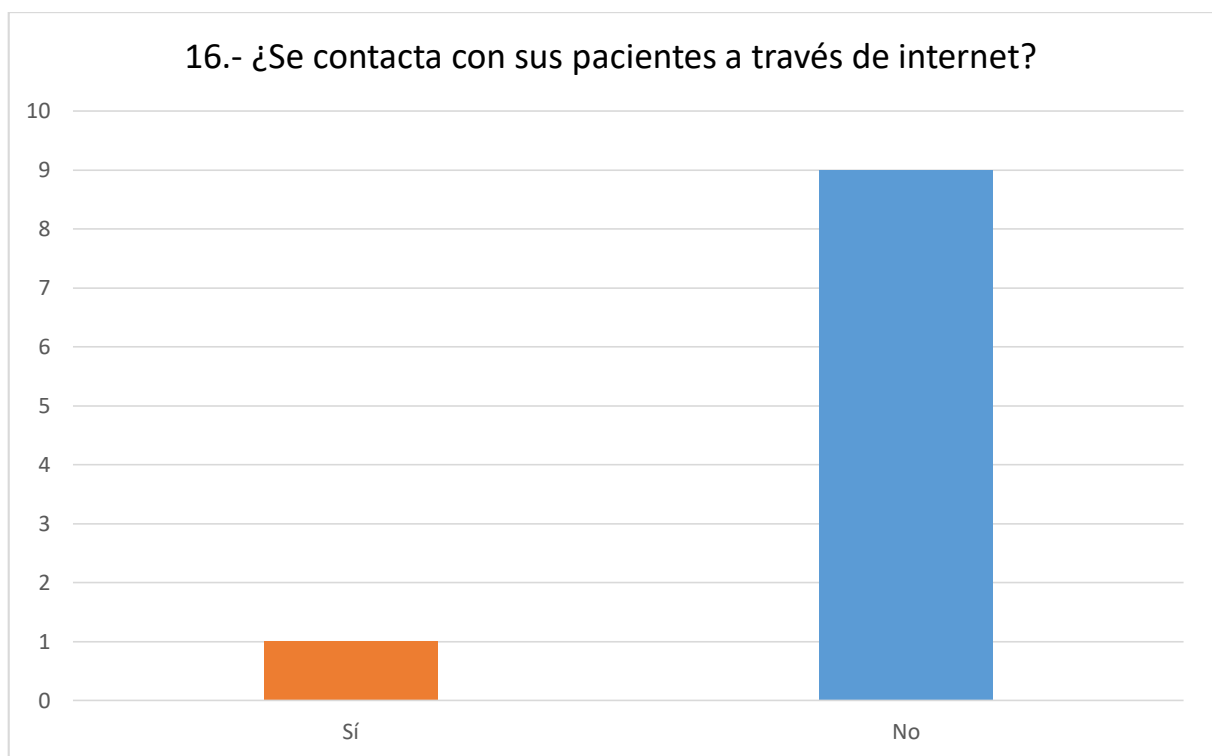
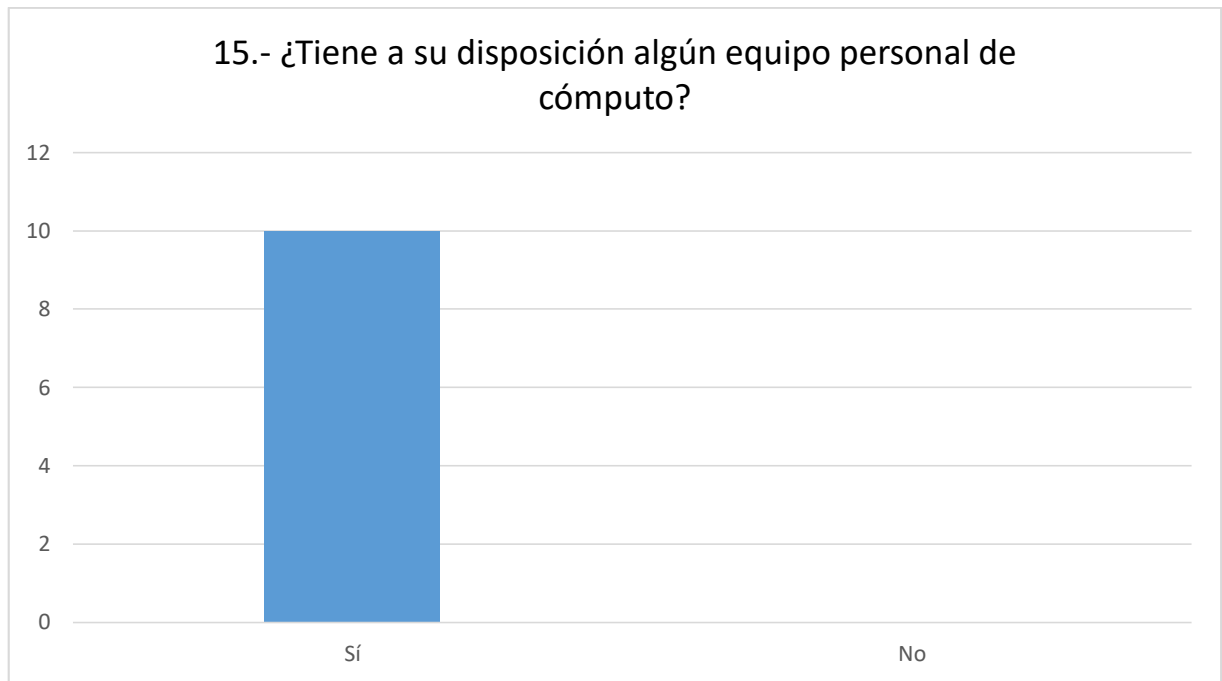
11.- ¿Cuáles son las consultas o búsquedas más frecuentes que usted realiza en internet?



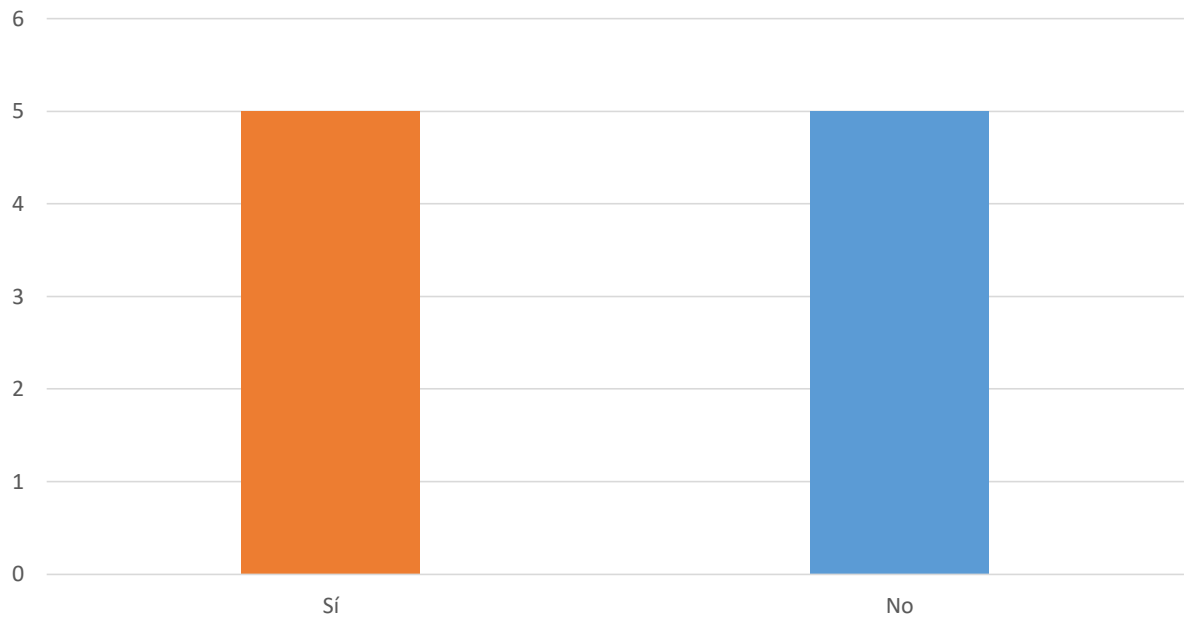
12.- ¿Cuáles son los mayores problemas que encuentra al utilizar el internet?



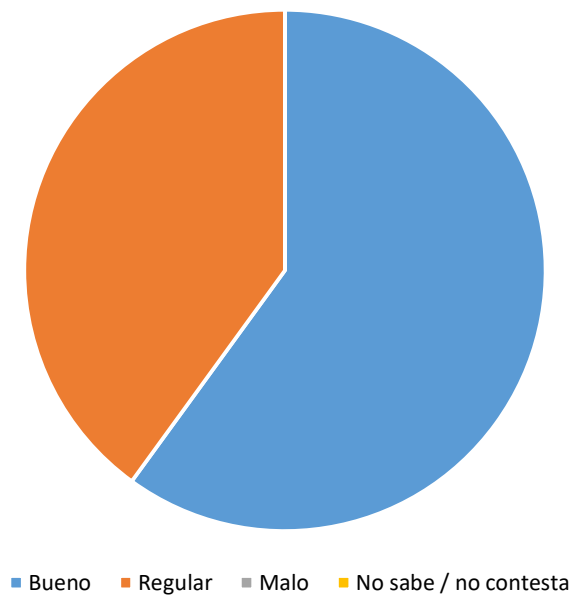


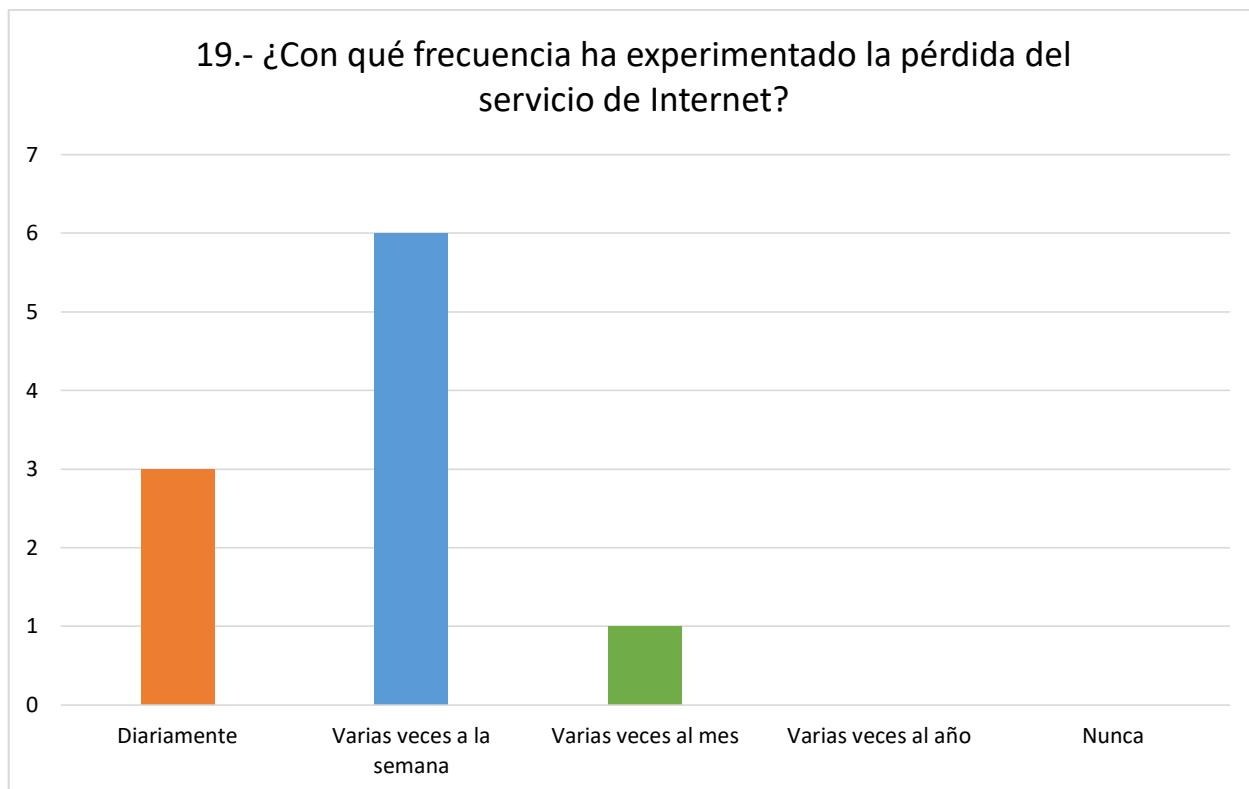


17.- ¿Usted cuenta con un usuario y contraseña para ingresar a un equipo de cómputo?



18.- ¿En general, cómo describiría el servicio de atención al usuario del área de Sistemas?





A.5. ENCUESTA 02

ENCUESTA Nº 02

Por favor, dedique unos minutos a completar esta pequeña encuesta, la información que nos proporcione será utilizada para optimizar el uso de las redes de telecomunicaciones de la Clínica Millenium.

1.- ¿Cuántas computadoras tiene la Clínica?

2.- ¿Cuántas computadoras están interconectadas en Red en la Clínica?

3.- ¿De qué manera la Clínica realiza sus procesos de registro clientes, citas, consultas médicas y entrega de resultados clínicos?

4.- ¿Conoce usted de servidores?

5.- ¿Creé usted que una consistente red de datos ayudará en la gestión de información de los pacientes?

6.- ¿La Clínica tiene pensado expandirse a futuro?

7.- ¿La Clínica tiene pensado en certificarse?

8.- ¿Qué tipo de certificado busca?

9.- ¿La clínica tiene normas o políticas de seguridad para el uso de la red o internet?

A.6. Configuración de los dispositivos intermediarios – Simulación Packet Tracer

ROUTER

```
Current configuration : 1640 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ROUTER_PRINCIPAL
!
enable secret 5 $1$mERr$0QA14Dh6V3G0nAujVTK/P/
enable password n0nFLV
!
ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX1524OGAZ
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
ip address 190.41.113.25 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2.1
no ip address
shutdown
!
interface GigabitEthernet0/2.10
encapsulation dot1Q 10
ip address 192.168.1.65 255.255.255.240
ip access-group 120 out
!
interface GigabitEthernet0/2.15
encapsulation dot1Q 15
ip address 192.168.1.1 255.255.255.192
!
interface GigabitEthernet0/2.20
encapsulation dot1Q 20
ip address 192.168.1.81 255.255.255.248
ip access-group 110 out
!
interface GigabitEthernet0/2.25
encapsulation dot1Q 25
```

```

ip address 10.0.0.1 255.255.255.0
!
interface Vlan1
no ip address
shutdown
!
router eigrp 1
network 192.168.1.0
network 190.41.113.0 0.0.0.255
network 10.0.0.0 0.0.0.255
!
ip classless
!
ip flow-export version 9
!
!
access-list 110 permit ip 192.168.1.64 0.0.0.15 host 192.168.1.82
access-list 110 deny ip 192.168.1.64 0.0.0.15 192.168.1.80 0.0.0.7
access-list 110 permit ip any any
access-list 120 deny ip 192.168.1.0 0.0.0.63 192.168.1.64 0.0.0.15
access-list 120 permit ip any any
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
end

```

SWITCHES

SWITCH PRINCIPAL

```

Current configuration : 1215 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_PRINCIPAL
!
enable secret 5 $1$mERr$0QA14Dh6V3G0nAujVTK/P/
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
switchport mode trunk

```

```
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
switchport mode trunk  
!  
interface Vlan1  
no ip address  
shutdown  
!  
line con 0  
!  
line vty 0 4  
login  
line vty 5 15  
login  
!  
end
```

SWITCH BK1-CT1-P1

Current configuration : 1530 bytes

```
!  
version 12.2  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname BK1-CT1-P1  
!  
enable secret 5 $1$mERr$0QA14Dh6V3G0nAujVTK/P/  
enable password momFLV  
!  
spanning-tree mode pvst  
!  
interface FastEthernet0/1  
switchport access vlan 15  
switchport mode access  
!  
interface FastEthernet0/2  
switchport access vlan 10  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security violation protect  
!  
interface FastEthernet0/3  
switchport access vlan 10  
switchport mode access  
switchport port-security mac-address sticky  
switchport port-security violation protect  
!  
interface FastEthernet0/4  
switchport access vlan 25  
switchport mode access  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!
```

```

interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
end

```

SWITCH BK2-CT1-P2

```

Current configuration : 1223 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname BK2-CT1-P2
!
enable secret 5 $1$mERr$0QA14Dh6V3G0nAujVTK/P/
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 25
switchport mode access
!

```

```

interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
end

```

SWITCH BK3-CT1-P3

```
Current configuration : 1223 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname BK3-CT1-P3
!
enable secret 5 $1$mERr$0QA14Dh6V3G0nAujVTK/P/
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
```



```

interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
end

```

SWITCH BK4-CT1-P4

```

Current configuration : 1660 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname BK4-CT1-P4
!
enable secret 5 $1$mERr$0QA14Dh6V3G0nAujVTK/P/
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
switchport port-security mac-address sticky
switchport port-security violation protect
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
switchport port-security mac-address sticky
switchport port-security violation protect
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!

```

```

interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login

```