UNIVERSIDAD AMAZÓNICA DE PANDO

ÁREA CIENCIAS Y TECNOLOGÍA

CARRERA DE INGENIERÍA INFORMÁTICA

PROYECTO DE GRADO

"ADMINISTRACIÓN DE LA SEGURIDAD DE LA RED DE DATOS E INTERNET DE LA EMPRESA PÚBLICA MUNICIPAL DE SERVICIO DE AGUA POTABLE Y ALCANTARILLADO SANITARIO DE COBIJA (EPSA-COBIJA)"

Proyecto de Grado para Optar al Grado de Licenciatura en Ingeniería de Sistemas Informáticos

POSTULANTE: Univ. José Pacamia Valencia

TUTOR: MSc. Lic. Humberto Fernandez Calle

ASESOR: Ing. Abel Huaygua Chalco

Cobija - Pando – Bolivia

2019

AGRADECIMIENTO

A Dios.

Por bendecir mi vida a lo largo de mi carrera y demostrarme cada vez su amor, su poder y su misericordia, sosteniéndome en los momentos más difíciles y permitiéndome lograr una meta más, al mismo tiempo contar con mis padres, hermanos, esposa e hijos.

A mis padres.

Froilán y Hortencia a quienes amo mucho por su constante apoyo en el objetivo de culminar con éxitos mis estudios.

A mi esposa.

Yolanda Ramírez Ramallo, por su apoyo, compresión y amor en los momentos más difíciles.

A mis hijos.

Shainna y Saúl, por darme la comprensión y la fuerza en su amor incondicional en los momentos más difíciles.

A mi familia, docentes y otras personas.

A toda mi familia, porque me han brindado su apoyo y por compartir conmigo buenos y malos momento.

Finalmente, a mis docentes y compañeros que marcaron cada etapa del camino universitario y contribuyeron en mí formación, además por la ayuda brindada en la asesoría y dudas presentadas en la elaboración del presente proyecto de grado.

DEDICATORIA

A Dios.

Por su infinita bondad, amor y ser la luz que me guío en este largo camino, y por haberme brindado salud para culminar esta meta tan anhelada.

A mis Padres

A mi madre Hortencia que gracias a sus enseñanzas y ejemplo me permitió seguir adelante venciendo todas las dificultades que se han presentado, pero más que nada, por su amor incondicional.

A mi padre Froilán por sus consejos y motivación constante para estudiar y culminar esta carrera universitaria.

A mi esposa e hijos

A mi esposa quien amo y admiro mucho, gracias por creer en mi capacidad, aunque hemos pasados momentos difíciles siempre ha estado brindándome su compresión, ayuda, cariño y amor.

A mis queridos hijos Shainna y Saul por ser mi fuente de motivación e inspiración para poder superarme cada día más y así poder luchar para que la vida nos depare un futuro mejor.

RESUMEN

Unos de los aspectos más importantes en el camino hacia el éxito radican en el manejo de la información. La necesidad de compartir recursos e intercambiar información fue la inquietud permanente de los primeros tiempos de la informática. Los comienzos de las redes de datos se remontan a los años 60, cuando se perseguían fines exclusivamente militares o de defensa.

En nuestros días, Internet ha pasado a través de un largo proceso evolutivo, Siendo en la actualidad una de las principales fuentes de conocimiento, comunicación y una amplia plataforma para hacer negocios.

El uso de las redes influyó mucho en la forma de manejar los sistemas de información soportes vitales de las instituciones y empresas, delineando así un futuro particularmente importante en el campo de las redes y de la informática en general. Si anteriormente se utilizaba básicamente para compartir los recursos de las computadoras conectadas, hoy las redes son medio de comunicación internacional a través de los cuales se intercambia grandes volúmenes de datos, a velocidades de tráfico.

Gracias a los avances tecnológicos, hoy en día la Empresa Pública Municipal de Servicios de Agua Potable y alcantarillado Sanitario de Cobija (EPSA-COBIJA) está orientando al proceso de sistematización de sus datos, de forma que ayude a una buena gestión en administración pública y toma de decisiones. Para lograr este objetivo es necesario contar con una buena administración de redes de datos e internet, que permita una fácil y fluida circulación de información por todos y cada una de las oficinas que conforman la EPSA COBIJA, teniendo en cuenta una visión futurista.

En el desarrollo de este proyecto se pretende mejorar la comunicación existente, con la creación de la división de redes de datos y servicio de internet que se encargue de administrar y dar soporte técnico a los usuarios de todo el predio de la EPSA COBIJA.

ABSTRACT

One of the most important aspects on the road to success lies in the handling of information. The need to share resources and exchange information was the permanent concern of the early days of computing. The beginnings of data networks are traced back to the 1960s, when they were pursued exclusively for military or defense purposes.

In our days, the Internet has gone through a long evolutionary process, being currently one of the main sources of knowledge, communication and a broad platform to do business.

The use of networks has greatly influenced the way in which information vital institutions and companies, thus shaping a particularly important future in the field of networks and information technology in general, handle systems. If previously it was used basically to share the resources of connected computers, today networks are an international means of communication through which large volumes of data are exchanged at traffic speeds.

Thanks to technological advances, nowadays the Municipal Public Company of Drinking Water and Sewerage Sanitary Services of Cobija (EPSA COBIJA) is guiding the systematization process of its data, in a way that helps a good management in public administration and decision-making. To achieve this goal it is necessary to have a good administration of data and internet networks, which allows an easy and fluid flow of information for each and every one of the offices that make up the Cobija Epsa, taking into account a futuristic vision.

In the development of this project, it is intended to improve existing communication, with the creation of the division of data networks and internet service that is responsible for administering and giving technical support to the users of all the premises of the COBIJA EPSA.

ÍNDICE

1. INTRODUCCIÓN 1

1.1 ANTECEDENTES 2

1.2 DESCRIPCIÓN DEL PROBLEMA. 3

1.3 OBJETIVOS. 4

1.3.1 Objetivo General. 4

1.3.2 Objetivos Específicos. 4

1.4 ALCANCES. 4

1.5 METODOLOGÍA Y HERRAMIENTAS UTILIZADAS 5

1.5.1 Descripción de los procesos de la metodología. 5

1.5.2 Administración de la configuración. 5

1.5.3 Administración del rendimiento. 5

1.5.4 Administración de Fallas. 6

1.5.5 Administración de la Seguridad: 6

1.5.6 Herramientas a Utilizar 6

1.6 ORGANIZACIÓN DEL DOCUMENTO. 7

2. MARCO DE REFERENCIA 9

2.1. MARCO INSTITUCIONAL 9

2.1.1. Misión 10

2.1.2. Visión 10

2.1.3. Objetivo de la EPSA COBIJA. 11

2.1.4. Organigrama: 12
2.1.5. Área de Informática Epsa Cobija. 14
2.2. MARCO LEGAL 14
2.3. MARCO TEÓRICO 15
2.3.1. Administración de Redes 16
2.3.2. Objetivos de la Administración de Red 16
2.3.3. Funciones de un Administrador de Red Según OSI 17
2.3.4. Redes de computadoras 18
2.3.5. Clasificación de las redes 18
2.3.6. Clases de Direcciones IP 20
2.3.7. Direcciones IP, máscaras de red 21
2.3.8. Estándar TIA/EIA 568 A 22
2.3.9. TIA/EIA-568 A 22
2.3.10. Conectores RJ-45 23
2.3.11. Protocolos de comunicación 24
2.3.12. Protocolo TCP/IP 25
2.4. DISPOSITIVOS DE RED DE DATOS 27
2.4.1. Routers 27
2.4.2. Hub 28
2.4.3. Switch 28
2.4.4. Wireless 29
2.4.5. Patch Panels 29
2.4.6. Servicios De Red 30

2.4.7. Servidor de Electrónico Correo 30
2.4.8. Servidor FTP 30
2.4.9. Servidor de página Web 31
2.4.10. Servidor Proxy 31
2.5. SEGURIDAD DE DATO 32
2.6. ENDIAN FIREWALL 33
2.6.1. Lo Que Ofrece Endian Firewall. 34
2.6.2. ¿Qué es Internet? 35
2.6.3. Historia de Internet 35
2.6.4. Servicios que brinda internet 36
2.6.5. Web 36
2.6.6. Correo Electrónico (e-mail) 36
2.6.7. Chat 37
2.7. POLÍTICAS 37
2.7.1. Políticas de Seguridad 37
2.8. DESCRIPCIÓN DE LAS HERRAMIENTAS UTILIZADAS. 39
2.8.1. Herramienta para medir el rendimiento de la Red. 39
2.8.2. Herramienta de Administración de la Red. 39
2.8.3. Sistemas operativos. 40
2.8.4. Herramientas de red 40
3. MARCO APLICATIVO 43
3.1. ADMINISTRACIÓN DE LA CONFIGURACIÓN 47
3.1.1. Planeación y diseño de la Red 47

3.1.2. Diagnóstico total de la Red de Datos e Internet 47
3.1.3. Conclusiones del Diagnostico 51
3.1.4. Selección de la infraestructura de red 51
3.1.5. Selección de infraestructura de red de la primera fase 51
3.1.6. Clasificación de nuevos rangos de IP´S 55
3.1.7. Selección de infraestructura de red de la segunda fase 56
3.2. INSTALACIÓN Y ADMINISTRACIÓN DEL SOFTWARE 56
3.2.1. Instalación de Hardware 56
3.2.2. Políticas y procedimientos relacionados 60
3.2.3. Políticas de uso de la red de datos e internet 61
3.3. ADMINISTRACIÓN DEL RENDIMIENTO 61
3.3.1. Monitoreo 61
a) Monitoreo del servicio de Internet (Red Externa) 61
3.3.2. Análisis 67
a) Análisis del servicio de Internet (Red Externa) 67
3.4. ADMINISTRACIÓN DE FALLAS 70
3.4.1. Asistencia técnica por fallas de red. 70
3.4.2. Configuración de la dirección IP 70
3.4.3. Asistencia técnica de conexión a la red 71
3.4.4. Asistencia técnica por fallas de internet. 72
3.4.5. Asistencia técnica del servicio de internet 72
3.4.6. Fallas con relación a otros aspectos 72
3.4.7. Instalación del sistema operativo Windows, office, antivirus, otros. 72

3.4.8. Asistencia técnica por contaminación de virus. 73
3.5. ADMINISTRACIÓN DE LA SEGURIDAD 73
3.5.1. Prevención de ataques 73
3.6. DETECCIÓN DE INTRUSOS 76
3.7. RESPUESTA A INCIDENTES 79
3.8. POLÍTICAS DE SEGURIDAD 79
3.8.1. Políticas de uso aceptable 79
3.8.2. Políticas de cuentas de usuario 80
3.8.3. Políticas de listas de acceso 80
3.8.4. Políticas de acceso remoto 80
3.8.5. Políticas de contraseñas. 81
3.8.6. Políticas de respaldos. 81
4. CONCLUSIONES Y RECOMENDACIONES 82
4.1. CONCLUSIONES 83
4.2. RECOMENDACIONES 83
4.3. REFERENCIAS 84

ÍNDICE DE FIGURA

Ilustración 1 Estructura Organizacional de la EPSA COBIJA 12
Ilustración 2 Red de Datos e internet 18
Ilustración 3 Conector RJ-45 hembra y macho 23
Ilustración 4 Modelo de Protocolo de Comunicación 24
Ilustración 5 Modelo de referencia OSI 24
Ilustración 6 Modelo OSI vs. TCP/IP 26
Ilustración 7 Símbolo del Router (Se observa flechas entrantes y salientes 27
Ilustración 8 Router Cisco 1760 – 1600 27
Ilustración 9 Símbolo del Hub (Se encuentra en el centro) 28
Ilustración 10 Símbolo del Switch (Se observa flechas salientes) 29
Ilustración 11 Wireless 29
Ilustración 12 Patch Panels 29
Ilustración 13 Modelo OSI - Filtros Proxy 31
Ilustración 14 Función del servidor proxy 32
Ilustración 15 Endian 33
Ilustración 16 Etapas para el desarrollo de las políticas 38
Ilustración 17 Test de la red de datos 47
Ilustración 18 Diagnóstico de la red de datos y el servicio de internet 48
Ilustración 19 Torta de uso del internet en el trabajo 50
Ilustración 20 Diseño lógico anterior de la red de datos 57
Ilustración 21 Cableado del nuevo diseño en todas las Jefaturas y unidades 58
Ilustración 22 Diseño físico del cableado de la red "Jefatura Comercial" 58
Ilustración 23 Diseño físico de la red inalámbrica "Jefatura Financiera" 58
Ilustración 24 Diseño físico del cableado de red "Administración de Redes 59
Ilustración 25 Pantalla principal de la aplicación ubicada en http://www.speedtest.com probando la velocidad de transferencia sin usuarios 62
Ilustración 26 Pantalla principal de la aplicación ubicada en http://www.testdevelocidad.es 65

Ilustración 27 Resultados del Ancho de banda sin usuarios 68
Ilustración 28 Resultados del Ancho de banda con usuarios 69
Ilustración 29 Conclusión de los Resultados del ancho de banda..... 69
Ilustración 36 Propiedades de conexión de área local..... 71
Ilustración 37 Usuario o contraseña mal digitadaFuente: Elaboración Propia 72
Ilustración 30 Activación del módulo sistema de prevención de intruso..... 77
Ilustración 31 Creación y configuración de Reglas de Snort..... 77
Ilustración 32 Aplicar configuración 77
Ilustración 33 opción1 Traffic Monitoring 78
Ilustración 34 opción2 Traffic Monitoring 78
Ilustración 35 tráfico que circula en la red..... 78

ÍNDICE DE TABLAS

Tabla 1 Direcciones de clase A 20
Tabla 2 Dirección IP de clase B 20
Tabla 3 Dirección IP clase C 21
Tabla 4 Cantidad de Usuarios encuestados por Jefaturas, Unidades y Secciones que cuentan con un computador 48
Tabla 5 Infraestructura para los usuarios (Hardware 52
Tabla 6 Infraestructura para el funcionamiento de la red de datos e inter 55
Tabla 7 IP`s de Usuarios EPSA COBIJA 55
Tabla 8 Infraestructura para la segunda fas 56
Tabla 9 Datos técnicos de la instalación y configuración de Endian Firewall 59
Tabla 10 Instalación y configuración de Mikrotik ..... **¡Error! Marcador no definido.**
Tabla 11 Criterios de la configuración del protocolo TCP/IP 60
Tabla 12 Cronograma de fecha y hora para la medición del ancho de banda 62
Tabla 13 Resultados del testeo del ancho de banda, 2018 64
Tabla 14 Cronograma de medición del ancho de banda 65
Tabla 15 Resultado del testeo del ancho de banda con usuario, II/2018 67
Tabla 16 Resultado Ancho de Banda Parte 1° 67
Tabla 17 Resultado Ancho de Banda Parte 2° 68
Tabla 18 Protocolos utilizados 74
Tabla 19 Tecnología utilizada 74
Tabla 20 Actualizando la tecnología utilizada 75

CAPÍTULO I

1. INTRODUCCIÓN

1.1 ANTECEDENTES

En Bolivia existen instituciones públicas y privadas algunas con alcances nacionales, y una de ellas son las Empresa Pública Municipal de Servicio de Agua Potable y Alcantarillado Sanitario que existen en el país.

En vista de la creciente demanda de la ciudadanía hacia los servicios de la EPSA esta se ve obligada a tener una estructura de red de datos local y equipamiento para satisfacer los servicios requeridos, al igual que en las otras Empresa Pública Municipal de Servicio de Agua Potable y Alcantarillado Sanitario del país.

Actualmente existe una red de datos e internet con deficiencias y problemas, el cual perjudica el desempeño normal de sus funciones de los usuarios que son encargados de operar los diferentes sistemas de información como ser SINCOM, EPSA NET, EPSA COBRA y EL POSEIDON; la falta de políticas de uso y la inexistencia de la administración de los recursos de la red, (VER ANEXO A).

Se ha realizado una revisión bibliográfica en relación a otros proyectos de grado similares al proyecto, a continuación, se describe los proyectos relacionados:

Diseño de un Modelo de Gestión de Seguridad en Redes de Comunicación Inalámbricas Aplicado a Pequeñas Empresas del Sector Privado de la Ciudad Bogotá (Cifuentes, 2017)

En este informe de trabajo de grado se presenta una revisión sobre la seguridad la vulnerabilidad de la información, así como la necesidad de implantar medidas, procesos y procedimientos que velen por la integridad, disponibilidad y confidencialidad de la información. Se establece una guía, para mantener la seguridad de las redes inalámbricas, y garantizar a salvaguardar la información, debido a las constantes ataques que se presentan y vulnerabilidades a los que se encuentran expuestas las redes, y lo sistemas informáticos que interactúan en esta. El uso de herramientas de pruebas, permiten evaluar los diferentes escenarios que se pueden presentar en la realidad, ejecutar pruebas de seguridad en una red inalámbrica tiene el propósito de mejorar la calidad de los servicios de la red, encontrar huecos de seguridad a tiempo, realizar mantenimientos preventivos y no correctivos, igualmente encontrar soluciones de seguridad antes de perjudicar la información de un negocio.

Administración del servicio de internet del campus universitario de la U.A.P., desarrollado por la Univ. Lorena Calizaya L. (2012). Es un Trabajo Dirigido desarrollado División de Redes de Datos e Internet de la Universidad Amazónica de Pando con el objetivo de Administración del Servicio de

Internet y la implementación del servidor MikroTik para la administración de la Red de Datos y el servicio de Internet, de acuerdo al análisis que se realizó a los problemas presentados en la DRDI (División de Redes de Datos e Internet) se determina que el problema principal es la deficiente administración del servicio de Internet, para lo cual se plantea como objetivo principal Mejorar el servicio de Internet con la eficiente administración y el acceso a usuarios del Campus Universitario de la U.A.P. utilizando la metodología "Modelo Funcional Para la Administración de Redes", el cual se logra con la implementación del Servidor Mikrotik, permitiendo utilizar algunas de sus herramientas, para mejorar el servicio de Internet se trabaja con calidad de servicios QoS del MikroTik se utiliza Simples Queues, para restricción de ancho de banda por usuario, el Web Proxy para restricción de páginas web, el servicio de autenticación de usuarios a través ARP de amarre de IP/MAC para la Red LAN y HotSpot para la Wifi inalámbrica, etc. El servicio de Internet mejoro con la administración de la Red de Datos e Internet permitiendo el control de acceso de usuarios, regulando el ancho de banda, restringiendo páginas web, monitoreo y control del uso de internet, etc.

1.2 DESCRIPCIÓN DEL PROBLEMA.

Considerando el análisis realizado al personal administrativo se pudo obtener el siguiente análisis de problemas (VER ANEXO B) el cual se describe a continuación:

Las causas que se percutan en la institución son; estructura de la red de datos e internet que no cumple con los estándares de redes de datos e internet y cableado estructurado, problema de conectividad, traslado de información por memoria flash la inexistencia de políticas para el uso de los recursos de la red de datos y la no existencia de normas de seguridad en la red de datos e internet.

En base a los problemas causa antes mencionadas, se establece el siguiente problema principal:

"Deficiencia en la administración de la seguridad de la red de datos e internet de la Empresa Pública Municipal de Servicio de Agua Potable y Alcantarillado Sanitario de Cobija (EPSA COBIJA)"

Los efectos del problema principal son: Infección de virus en los equipos de computación, lentitud e inseguridad en el manejo de los sistemas SINCOM, SIAF, EPSA NET y EPSA COBRA y EL POSEIDON desconformidad y molestia en los usuarios por constantes caída de la red de datos e internet, provocando perdida de información.

1.3 OBJETIVOS.

1.3.1 Objetivo General.

Administrar la seguridad de la red de datos e internet en la Empresa Pública Municipal de Servicio de Agua Potable y Alcantarillado Sanitario EPSA COBIJA, en base al modelo funcional que permita mayor seguridad a la información que se maneja en la institución.

1.3.2 Objetivos Específicos.

- ✓ Diagnosticar la situación de la seguridad de la red de datos e internet de la Empresa Pública Municipal de Servicio de Agua Potable y Alcantarillado Sanitario EPSA COBIJA.
- ✓ Configurar la Seguridad de datos a través de Endian Firewall.
- ✓ Administrar la Seguridad de la red de datos e internet, mediante la metodología funcional.

1.4 ALCANCES.

El alcance del proyecto contempla todo el predio central de la EPSA COBIJA, Áreas, Jefaturas, Unidades y Secciones que cuentan con un computador, ubicado en el barrio Progreso de la ciudad de cobija.

El presente proyecto abarcada metodológicamente los siguientes aspectos:

- ❖ Diagnóstico total de la seguridad de la red de datos e internet (el proceso de contabilidad que es parte de la metodología no se tomara en cuenta porque el presente proyecto no es lucrativo)
- ❖ Restructuración la red de datos e internet, para mejorar el servicio de internet y la seguridad de la red de datos.
- ❖ Implementación de un servidor proxy para la seguridad de la red de datos e internet.
- ❖ Elaboración de políticas y uso de la seguridad de la red de datos e internet.
- ❖ Control y monitoreo del servicio de la seguridad de la red de datos e internet.
- ❖ Asistencia técnica de capacitación a los usuarios del Predio de la EPSA COBIJA.

1.5 METODOLOGÍA Y HERRAMIENTAS UTILIZADAS

La metodología que se utilizó en este proyecto es el **"Modelo Funcional para la Administración Redes"**, este modelo detalla las tareas y funciones que deben ser ejecutadas en el proceso de administración **y** seguridad de la red de datos.

El motivo para elegir esta metodología es que está basada en un modelo con tareas bien definidas y complementarias. Este modularidad permite su mejor entendimiento y facilita su implementación y actualización.

Esta metodología tiene cinco procesos (Administración de la configuración, Administración de rendimiento, Administración de fallas, Administración de contabilidad y Administración de seguridad).

Para el desarrollo de este proyecto de grado se contemplará cuatro de los cincos procesos que se detallan a continuación en el punto 1.5.1, Descripción de los procesos de la metodología.

1.5.1 Descripción de los procesos de la metodología.

Actividades que se realizaron en cada proceso de las áreas funcionales.

1.5.2 Administración de la configuración.

Dentro del proceso de Administración de la Configuración se realizan las siguientes actividades:

1. Planeación y diseño de la red
2. Selección de la Infraestructura de la Red
3. Instalación y administración del software Administración del hardware
4. Políticas y Procedimientos Relacionados

1.5.3 Administración del rendimiento.

Para la administración del rendimiento se implementó un servidor proxy Endian Firewall como herramienta, que tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

1.5.4 Administración de Fallas.

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla, para lo cual se utilizara herramientas lógicas como ser un servidor proxy y el ping, y las herramientas de red como ser un tester y otras herramientas propias de la administración de red de datos y las técnicas a utilizarse son testeador de cable de red, alicate de red, utilización del ping y la verificación física.

1.5.5 Administración de la Seguridad:

Su objetivo es ofrecer servicios de seguridad a los sistemas e informaciones importante de la EPSA COBIJA y cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

En base a la metodología adoptada se toma en cuenta cuatro procesos las cuales son: Administración de la configuración, Administración del rendimiento, Administración de fallas y Administración de la seguridad para dar solución a las necesidades inmediatas de mayor importancia en el presente proyecto.

1.5.6 Herramientas a Utilizar.

A continuación, se detallan cada una de las herramientas utilizadas para la Seguridad en la Administración de la Red de Datos e Internet de la EPSA COBIJA.

Herramientas de Software

- **Herramientas de diagnóstico y monitoreo de red**
    - comando del sistema operativo Windows, para el monitoreo y diagnóstico de la red de datos.

- **Herramienta de seguridad de red**
    - Endian Firewall

1.6 ORGANIZACIÓN DEL DOCUMENTO.

Capítulo 1: En este capítulo se aborda la fase introductoria del proyecto de grado donde se consigna la introducción, la problemática objeto del estudio, la solución propuesta, los objetivos generales y específicos, el alcance, los aportes y la metodología empleada.

Capítulo 2: Se refiere a los fundamentos teóricos y conceptuales del tema, la metodología, herramientas y técnicas aplicadas en el desarrollo del proyecto.

Capítulo 3: Este capítulo consigna la implementación del proyecto en todas sus etapas, de acuerdo a la metodología establecida

Capítulo 4: En este capítulo se aborda las conclusiones del proyecto de grado en función de los objetivos planteados y las recomendaciones para su correcto funcionamiento.

CAPITULO II

2. MARCO DE REFERENCIA

2.1. MARCO INSTITUCIONAL

En Bolivia existen instituciones públicas y privadas algunas con alcances nacionales, y una de ellas son las Empresa Pública Municipal de Servicio de Agua Potable y Alcantarillado Sanitario que existen en el país.

En vista de la creciente demanda de la ciudadanía hacia los servicios de la EPSA COBIJA esta se ve obligada a tener una estructura de red de datos local y equipamiento para satisfacer los servicios requeridos, al igual que en las otras Empresa Pública Municipal de Servicio de Agua Potable y Alcantarillado Sanitario del país.

Actualmente existe una red de datos e internet con deficiencias y problemas, el cual perjudica el desempeño normal de sus funciones de los usuarios que son encargados de operar los diferentes sistemas de información como ser SINCOM, SIAF, EPSA NET, EPSA COBRA Y POSEIDON; la falta de políticas de uso y la inexistencia de la administración de los recursos de la red.

La empresa de servicio de agua potable y alcantarillado, Inicia sus actividades a partir del año 1982 con la participación de ocho empresas Prestadoras de Servicios de Agua Potable y Alcantarillado (EPSA) correspondientes a las capitales de departamento del País, como una respuesta a la necesidad de integrar las EPSA en busca de fortalecimiento y desarrollo del sector.

Mediante Resolución Suprema No. 199404 de fecha 29 de Octubre de 1984, se reconoce la Personería Jurídica de la Asociación.

La Empresa Pública Municipal de Servicios de Agua Potable y Alcantarillado Sanitario de Cobija cuya denominación es EPSA Municipal Cobija, es una empresa municipal descentralizada, con autonomía de gestión técnica, operativa, financiera y económica, patrimonio independiente y personalidad jurídica de derecho Público.

A la EPSA Municipal Cobija le corresponde la administración y prestación directa de los servicios de agua potable y alcantarillado sanitario de la ciudad de Cobija, Departamento de Pando, en sujeción a las disposiciones legales vigentes.

La EPSA Municipal Cobija fue creada por Ordenanza Municipal N° 44/2006 del Honorable. Concejo Municipal de Cobija de fecha 14 de junio de 2006, promulgada en el Despacho del Ejecutivo Municipal en la misma fecha y por Ordenanza Municipal N° 020/2007 del H. Concejo Municipal de Cobija de fecha 01 de marzo de 2007,en la misma fecha fue aprobando el Estatuto Orgánico de la

EPSA y su Reglamento y promulgada en el Despacho del Dr. Luís Adolfo Flores Roberts en su calidad de H. Alcalde Municipal de Cobija en fecha 02/03/2007, en consecuencia la EPSA Municipal Cobija se constituye en una Empresa que emerge a la vida jurídica como sujeto de Derecho Público a partir de noviembre de 2008.

2.1.1. Misión

Contribuir al fortalecimiento institucional y desarrollo empresarial de las EPSA COBIJA, a fin de mejorar la calidad de vida de la población, asegurando la sostenibilidad de los servicios y del medio ambiente.

La misión institucional es la razón de ser de la institución, es el elemento que la define, la distingue de otras, le da la razón de ser a la entidad, que fundamentalmente expresa su mandato social para la cual fue creada.

> Empresa pública municipal de servicios de agua potable y alcantarillado sanitario de cobija – epsa municipal de cobija, es una empresa pública municipal descentralizada con autonomía de gestión, que brinda los servicios de agua potable y alcantarillado sanitario o los usuarios de la ciudad de cobija, buscando el mejoramiento de la calidad de vida, conciencia ambiental de sus usuarios, mediante una gestión con calidad, eficiencia y eficacia.

2.1.2. Visión

La visión de desarrollo de la Empresa Pública Municipal de Servicios de Agua Potable y Alcantarillado Sanitario de Cobija – EPSA COBIJA apunta al desarrollo del ser humano en cuanto individualidad y en cuanto colectividad, como ciudadano con derechos y obligaciones, con relaciones y propuestas, con demandas y ofertas concretas y donde el interés del desarrollo abarca todas las dimensiones de lo humano.

> Empresa pública municipal de servicios de agua potable y alcantarillado sanitario de cobija – epsa municipal de cobija, es una empresa líder en la prestación del servicio de agua potable y alcantarillado sanitario a nivel departamental, comprometida con el desarrollo regional, auto sostenible y eficiente, que brinda un servicio continuo a sus usuarios en la ciudad de cobija y que realiza mejoramientos constantes a los sistemas que administra, cumpliendo con las normas y disposiciones vigentes, con responsabilidad, con vocación de servicio y preservando el medio ambiente y la salud de los ciudadanos.

2.1.3. Objetivo de la EPSA COBIJA.

Cooperar y asistir a las empresas socias y del sector para lograr el mejoramiento en la efectividad y eficiencia de la prestación de servicios de agua potable y alcantarillado a fin de mejorar la calidad de vida de la población.

El organigrama actual de la “EPSA COBIJA”, exponiendo las unidades más importantes como ser la Jefatura Administrativa Financiera, Sección de Contabilidad, Jefatura Comercial y Sección de Cobranza y Facturación.

2.1.4. Organigrama:

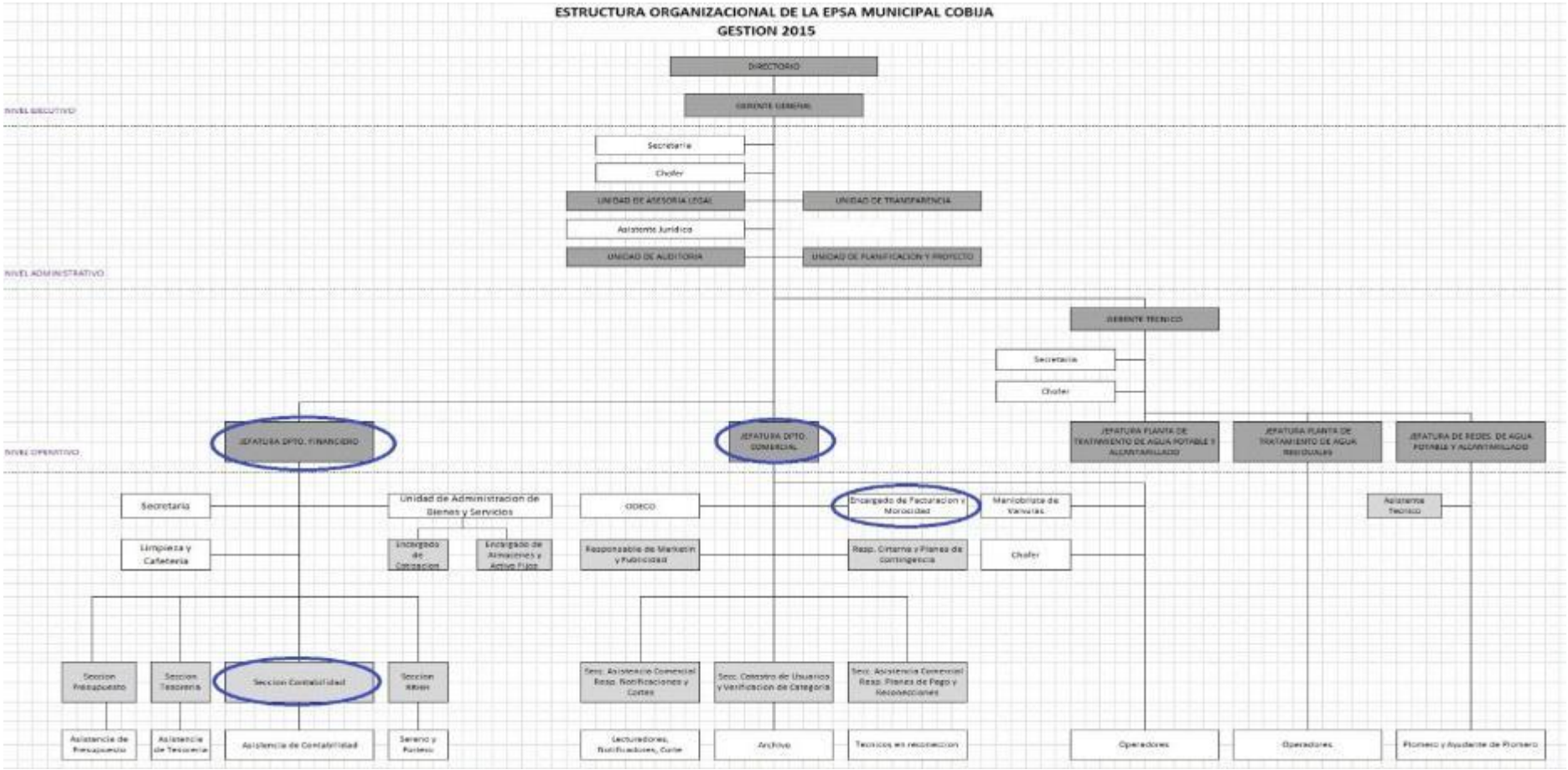


Ilustración 1 Estructura Organizacional de la EPSA COBIJA
Fuente: Elaboración propia

Las actividades realizadas por la Jefatura Administrativa Financiera son las siguientes:

- ✓ Coordinación para la ejecución económica financiera de los programas, proyectos y actividades desarrolladas por la EPSA COBIJA.

- ✓ Administración de los recursos propios de la Empresa, recursos externos y financiamiento de corto mediano y largo plazo para el funcionamiento y la ejecución de programas proyectos y actividades de la EPSA COBIJA.

- ✓ Administración y control del uso de los bienes materiales e inmateriales y servicios con que cuenta la empresa (propia y/o contratada), en función a los objetivos para los cuales fueron adquiridos.

Las actividades realizadas por la Sección de contabilidad:

- ✓ Dirigir, coordinar y controlar las labores de registro, validación y aprobación de la ejecución presupuestaria de gastos e ingresos de la EPSA COBIJA; aplicando conforme a su naturaleza jurídica, características operativas, requerimientos de información y metodología contable, de acuerdo a las normas de contabilidad integrada gubernamental que dicte la Sección de Contabilidad del Estado del Ministerio de Finanzas Públicas.

Las actividades realizadas por la Jefatura Comercial:

- ✓ Brindar información a la Ciudadanía de la distribución de agua potable los cortes y multas de agua por faltas cometida por el usuario, tan bien velar por el servicio de agua para que llegue a todos los puntos de los clientes.

Las actividades realizadas por la Sección de Cobranza y Facturación:

- ✓ Hacer llegar las facturas de cobranza a los domicilio de los usuario y ver que todos estén al día en sus mensualidades. Para así brindarle un mejor servicio con sus pagos.

Así mismo las demás Jefatura, Unidades y Secciones como ser: Jefatura de planta de tratamiento de agua potable, Jefatura de planta de tratamiento de aguas residuales, Jefatura de redes de agua potables y alcantarillado, Unidad de asesoría legal, Unidad de Transparencia, Unidad de Auditoria y otras cumplen actividades elementales donde hay circulación de informaciones importante.

Como se vio anteriormente, cada uno de las Jefatura y Secciones cumplen una tarea específica los cuales se mejorarán con la implementación del presente proyecto, porque facilitara muchas de las actividades antes mencionadas.

2.1.5. Área de Informática Epsa Cobija.

La Empresa Pública Municipal de Servicio de Agua Potable y Alcantarillado Sanitario de Cobija (EPSA-COBIJA) delegará al área de INFORMÁTICA para que dé seguimiento al cumplimiento de la normativa y propicie el entorno necesario para crear un SGSI, el cual tendrá entre sus funciones.

a. Velar por la seguridad de los activos informáticos.
b. Gestión y procesamiento de información.
c. Cumplimiento de políticas.
d. Elaboración de planes de seguridad.
e. Capacitación de usuarios en temas de seguridad.
f. Gestionar y coordinar esfuerzos, por crear un plan de contingencia,

que dé sustento o solución, a problemas de seguridad dentro de la

Epsa Municipal Cobija. El mismo orientará y guiará a los usuarios, la forma o métodos necesarios para salir adelante ante cualquier eventualidad

que se presente.

g. Informar sobre problemas de seguridad a la Gerencia General.

Poner especial atención a los usuarios de la Epsa Municipal Cobija sobre sugerencias o quejas con respecto al funcionamiento de los activos de información.

2.2. MARCO LEGAL

La EPSA COBIJA fue creada por Ordenanza Municipal N° 44/2006 DEL H. Concejo Municipal de Cobija de fecha 14 de junio de 2006, promulgada en el Despacho del Ejecutivo Municipal en la misma fecha y por Ordenanza Municipal N° 020/2007 del H. Concejo Municipal de Cobija de fecha 01 de marzo de 2007 que aprueba el Estatuto Orgánico de la EPSA y su Reglamento y promulgada en el Despacho del Dr. Luís Adolfo Flores Roberts en su calidad de H. Alcalde Municipal de Cobija en fecha 02/03/2007, en consecuencia la EPSA Municipal Cobija se constituye en una

Empresa que emerge a la vida jurídica como sujeto de Derecho Público a partir de noviembre de 2008, pues hasta octubre del mismo año era el Servicio de Agua Potable dependiente de la Prefectura de Pando quien era responsable del suministro de Agua Potable a la Ciudad de Cobija, en consecuencia nuestra Empresa tiene una reciente creación.

El Director Ejecutivo de la Autoridad de Fiscalización y Control Social de Agua Potable y Servicios Básicos con las atribuciones que le confiere la Ley N° 2066 y D. S. 071/09(VER ANEXO E,F yG). Otorga a la Empresa Pública Municipal de Servicio de Agua Potable y Alcantarillado Sanitario "EPSA COBIJA" de la Ciudad de Cobija - Pando el correspondiente Certificado de LICENCIA para la prestación de los Servicios de Agua Potable y/o Alcantarillado Sanitario y la Autorización para el Uso y Aprovechamiento del Recurso Hídrico mediante Resolución Administrativa Regulatoria AAPS No 49/2009 de fecha 26 de agosto de 2009, por cuanto la Empresa cuenta con el correspondiente "LICENCIA" que le faculta al uso y aprovechamiento del Recurso Hídrico y de esta manera poder hacer la venta del Servicio más no del agua.

2.3. MARCO TEÓRICO

Con el avance tecnológico de la comunicación en el área de seguridad de las redes de datos e internet, se ha podido evidenciar unos de los aspectos más importantes en el camino hacia el éxito, el cual radica en el manejo de la seguridad en las informaciones y las necesidades de compartir recursos e intercambiar información. El uso de las redes de datos e internet influye en la forma de manejar los sistemas de información que son los soportes vitales de las instituciones públicas y privadas como es la Empresa Pública Municipal de Servicio de Agua Potable y Alcantarillado Sanitario de Cobija (EPSA - COBIJA) y del resto del país, delineando así un futuro particularmente importante en el campo de las redes de datos e internet y de la informática en general. Si anteriormente se utilizaba básicamente para compartir los recursos de las computadoras conectadas, hoy las redes de datos e internet son medio de comunicación local, nacional e internacional a través de los cuales se intercambia grandes volúmenes de datos, a velocidades de tráfico a niveles casi inimaginables.

2.3.1. Administración de Redes

La definición etimológica de la palabra Administración viene del latín "AD" que significa Dirección - Tendencia y "MINISTERES" que significa Subordinación u Obediencia. Con la definición etimológica clara se puede deducir que la administración es el proceso de planear, organizar, dirigir, controlar los esfuerzos de los miembros de la organización y de aplicar los demás recursos de ella para alcanzar las metas establecidas (Andrew S. Tanenbaum y David J. Wethersll, 2012).

Una vez conocido la definición de la Administración se puede deducir que la Administración de red de datos es el proceso de planificar, organizar, dirigir y controlar los recursos tecnológicos de hardware (físicos) y software (lógicos) de una red de datos.

2.3.2. Objetivos de la Administración de Red

A continuación, se presenta un listado de los objetivos de una Administración de Red, poniendo:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

El sistema de administración de red opera bajo los siguientes pasos básicos:

- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.
- Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.
- Transportación de la información del equipos monitoreado al centro de control
- Almacenamiento de los datos coleccionados en el centro de control.
- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.
- Actuación para generar acciones rápidas y automáticas en respuestas a una falla mayor.

2.3.3. Funciones de un Administrador de Red Según OSI

El modelo OSI de telecomunicaciones está basado en una propuesta desarrollada por la Organización de Estándares Internacional (ISO), por lo que también se le conoce como modelo ISO – OSI, su función es la de definir la forma en que se comunican los sistemas abiertos de telecomunicaciones, es decir la ISO creó un modelo de administración de redes, donde define cinco áreas principales, que pueden especificar claramente las funciones de los sistemas de administración de redes.

Estas áreas son las siguientes:

- **Configuración:** Comprende las funciones de monitoreo y mantenimiento del estado de la red. En el proceso de la configuración, se realizan las actividades de: planeación, diseño de la red; la instalación y administración de software, administración de hardware y el aprovisionamiento.
- **Fallas:** Esta función consiste en: detectar la falla y dejar en antecedente, notificar el uso de herramientas y arreglar problemas automáticamente para mantener la red funcionando en forma adecuada.

  El proceso de la administración de fallas consiste en distintas fases:

- *Monitoreo de alarmas:* se realiza la notificación de la existencia de una falla y el lugar donde se ha generado.
- *Localización de fallas:* determinar el origen de una falla
- *Prueba de diagnóstico:* diseñar y realizar prueba que apoyen la localización de una falla.
- *Corrección de fallas:* tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.
- *Administración de reportes:* registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.
- **Contabilidad:** Es el proceso de recolección de información acerca de los recursos utilizados en la red, desde equipos de interconexión hasta los usuarios finales.

Rendimiento: Tiene como objetivo principal recolectar y analizar el tráfico que circula por la red, para determinar su comportamiento en diversos aspectos, ya sea en tiempo real o en intervalos de tiempo.

La administración del rendimiento se divide en 2 etapas:

- *Monitoreo*: consiste en observar y recolectar la información referente al comportamiento de la red.
- *Análisis:* una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar el desempeño.
- **Seguridad:** La función de seguridad provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves.

2.3.4. Redes de computadoras

Es el conjunto de componentes informáticos (computadora), que se encuentran físicamente conectados y programas informáticos empleados para conectar dos o más computadora. Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos (Stallings, 2004).

Ilustración 2 Red de Datos e internet
Fuente: https://www.elaltoesnoticia.com/quinto-poder/historia-de-la-internet.html

2.3.5. Clasificación de las redes

Las redes de datos se clasifican de acuerdo a su extensión geográfica y su distribución lógica: De acuerdo a la extensión geográfica, las redes se clasifican en: **PAN (Red de Administración Personal), que son** redes pequeñas, las cuales están conformadas por no más de 8 equipos, por ejemplo: La red que utiliza un café Internet para prestar servicio de Internet. **LAN (Red de Área Local),** es una red de computadoras, es decir, dos o más equipos conectados entre sí de manera que

pueden compartir todos los recursos del sistema **CAN (Red de Área Campus),** Es una colección de LAN's dispersadas geográficamente dentro de un campus (universitario, oficinas de gobierno, etc.) pertenecientes a una misma entidad en una área delimitada en kilómetros. **MAN (Red de Área Metropolitana),** Es un sistema de interconexión de equipos informáticos, distribuidos en una zona que abarca diversos edificios, por medios pertenecientes a la misma organización propietaria de los equipos. Este tipo de redes se utiliza normalmente para interconectar redes de área local. **WAN (Red de Área Extensa),** Son redes punto a punto que interconectan países y continentes. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos. El alcance es una gran área geográfica.

Las topología de una red local Según (José María Barceló Ordinas, Jordi Íñigo Griera, Ramón Martí Escalé, Enric Peig Olivé y Xavier Perramon Tornil, 2004) se entiende que es la distribución física en la que se encuentran dispuestos los ordenadores que la componen. De este modo, existen tres tipos, que podíamos llamar "puros" los cuales son: **Anillo**, es una topología de red en la que cada estación tiene una única conexión de entrada y otra de salida de anillo. Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación. En este tipo de red la comunicación se da por el paso de un *token* o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones. En un anillo doble (*Token Ring*), dos anillos permiten que los datos se envíen en ambas direcciones (*Token passing*). Esta configuración crea redundancia (tolerancia a fallos). **Bus,** es aquella topología que se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí y la **Estrella Extendida,** tiene una topología en estrella central, con cada uno de los nodos extremos de la topología en estrella.

La ventaja es que hace que el cableado sea más corto y limita el número de dispositivos necesarios para interconectar cualquier nodo central. Una topología en estrella extendida es muy jerárquica y se puede configurar (con el equipo apropiado) para "animar" a que el tráfico permanezca local.

2.3.6. Clases de Direcciones IP

Según (José María Barceló Ordinas, Jordi Íñigo Griera, Ramón Martí Escalé, Enric Peig Olivé y Xavier Perramon Tornil, 2004), para una mejor organización, en el reparto de rangos las redes se han agrupado en cuatro clases, de manera que según el tamaño de la red se optará por un tipo u otro.

a) Clase A

Las direcciones de la clase A, se diseñaron para crear redes extremadamente grandes. Debido a que las necesidades de este tipo de redes se supuso que serían mínimas, se desarrolló una arquitectura que maximizaba el numero posibles de direcciones de host, pero limitaba severamente, el numero potencial de redes de clase A que se podrían definirse.

La clase A comprende redes desde 1.0.0.0 hasta 127.0.0.0, el número de red está contenido en el primer octeto. Esta clase ofrece una parte para el puesto de 24 bits, permitiendo aproximadamente 16.777.214 posibles direcciones a otros tantos posibles dispositivos conectados a la red.

Clase	Tamaño de la dirección de red (en octetos)	Primer número	Número de direcciones locales
A	1	0 -127	16.777.214

Tabla 1 Direcciones de clase A
Fuente: Elaboración propia

b) Clase B

Las direcciones de clase B, se diseñaron para dar respuestas a las necesidades de las redes de tamaño medio o grande. Los dos primeros bits de una dirección de clase B son siempre 10 (1 y 0).

La clase B, comprende las redes desde 128.0.0.0 hasta 191.255.0.0, el número de red está en los dos primeros octetos. Esta clase permite 65.536 posibles direcciones IP a otros tantos posibles dispositivos conectados a la red.

Clase	Tamaño de la dirección de red (en octetos)	Primer número	Número de direcciones locales
B	2	128 -191	65.536

Tabla 2 Dirección IP de clase B
Fuente: Elaboración Propia

c) Clase C

El espacio de direcciones de clase C es, de lejos, el que más habitualmente se ha utilizado de las clases originales de direcciones de IP y se ideó para dar soporte a una red pequeña. Los tres primeros dígitos de una dirección de clase C son siempre son 110 (1,1 y 0).

Las redes de clase C, van desde 192.0.0.0 hasta 223.255.255.0, con el número de red contenido en los tres primeros octetos. Esta clase permite cerca de 2 millones de redes con más de 254 puestos.

Clase	Tamaño de la dirección de red (en octetos)	Primer número	Número de direcciones locales
C	3	192 -223	256

Tabla 3 Dirección IP clase C
Fuente: Elaboración Propia

d) CLASE D y E

Existen dos formatos especiales de direcciones, la clase D y la clase E. Las direcciones de clase D se usan para Multienvío de IP. El Multienvío permite distribuir un mismo mensaje a un grupo de computadoras dispersas por una red. Las direcciones de clase E se han reservado para uso experimental.

- Las direcciones de clase D empiezan con un número entre 224 y 239.
- Las direcciones de clase E empiezan con un número entre 240 y 255.

2.3.7. Direcciones IP, máscaras de red

Según (Andrew S. Tanenbaum y David J. Wethersll, 2012), el protocolo de red IP utiliza direcciones formadas por números de 32 bits. Se asigna un número único a cada máquina del entorno de red. Si funciona una red local que no tiene tráfico TCP/IP con otras redes, puede asignarse estos números de acuerdo con sus preferencias personales. Hay algunos rangos de direcciones IP que han sido reservadas para redes privadas. De cualquier modo, los números para los sitios en Internet los asigna una autoridad central, el Network Information Center (NIC).

Para facilitar la lectura, las direcciones IP se separan en cuatro números de ocho bits llamados octetos. Por ejemplo, quark.physics.groucho.edu tiene una dirección IP 0x954C0C04, que se escribe

como 149.76.12.4. Este formato se denomina normalmente notación de puntos divisorios.

Otra razón para usar esta notación es que las direcciones IP se dividen en un número de red, que es contenido en el octeto principal, y un número de puesto, que es contenido en el resto. Cuando se solicita al NIC una dirección IP, no se le asignará una dirección para cada puesto individual que pretenda usar. En cambio, se le otorgará un número de red y se le permitirá asig**n**ar todas las direcciones IP válidas dentro de ese rango para albergar puestos en su red de acuerdo con sus preferencias.

El tamaño de la parte dedicada al puesto depende del tamaño de la red. Para complacer diferentes necesidades, se han definido varias clases de redes, fijando diferentes sitios donde dividir la dirección IP.

2.3.8. Estándar TIA/EIA 568 A

Según (José María Barceló Ordinas, Jordi Íñigo Griera, Ramón Martí Escalé, Enric Peig Olivé y Xavier Perramon Tornil, 2004), afirma que: de todas las organizaciones que existen en estándares, la TIA/EIA tiene el mayor impacto en las normas relacionadas con los medios de red. Específicamente, los estándares TIA/EIA-568-A y TIA/EIA-568-B han sido y continúan siendo las más ampliamente utilizadas para la actuación técnica de los medios de red.

Los estándares TIA/EIA especifican los requisitos mínimos para entornos de múltiples productos y de múltiples fabricantes. Permiten la planificación y la instalación de sistemas LAN sin dictar el uso de equipos específicos, de modo que dan a los diseñadores de LAN la libertad de crear opciones de mejora expansión.

2.3.9. TIA/EIA-568 A

El Estándar TIA/EIA-568-A, trata de seis elementos del proceso de cableado para una red lan. Son los Siguientes: Cableado horizontal, Recintos de telecomunicaciones, Cableado del Backbone, Salas de equipamiento, Áreas de trabajo, Facilidades de entradas. El estándar TIA/EIA-568-A contiene especificaciones que rigen el rendimiento del cable. Requiere dos cables, uno para voz y otro para datos, por cada toma. De los dos cables, el de voz debe ser UTP de cuatro pares. El estándar TIA/EIA-

568-A, se utilizó para la reestructuración es la categoría 6(CAT 6, cable par trenzado sin apantallar UTP). Esta categoría fue la más recomendable para la aplicación de la instalación por que es la que se puede encontrar en el medio. el cable de par trenzado sin apantallar (UTP) es un cable regular de cuatro pares de cables que se utiliza en un gran número de redes. En el cable UTP, el material aislante cubre cada uno de los ocho cables de cobre individuales. Además, los pares de cables están trenzados entre sí. Este tipo de cable depende únicamente del efecto de cancelación, producido por los pares de cables trenzados, para limitar la degradación de la señal provocada por las EMI y las RFI. Para reducir más la diafonía entre los pares de cable UTP, el número de trenzas en los pares de cable varia. Cuando se utiliza una red media, el cable UTP tiene cuatro pares de hilo de cobre de calibre 22 o 24. El UTP tiene una impedancia de 100 Ohms. Como el UTP tiene un diámetro exterior de 0.43 cm. aproximadamente, su pequeño tamaño es una ventaja para las instalaciones. Debido a que el UTP se puede utilizar con la mayoría de las principales estructuras de red, sigue siendo el medio dominante para las LAN. (José María Barceló Ordinas, Jordi Íñigo Griera, Ramón Martí Escalé, Enric Peig Olivé y Xavier Perramon Tornil, 2004).

2.3.10. Conectores RJ-45

El conector RJ-45 es uno de los elementos indispensables para realizar el cableado de red. En la siguiente figura se observa los tipos de conectores RJ-45.

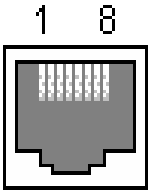
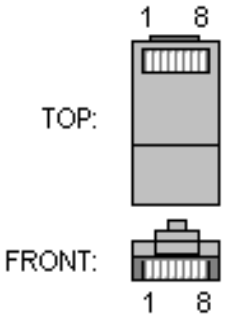
Hembra	Macho
Visto de Frente	Conector Visto de Frente y desde arriba
	

Ilustración 3 Conector RJ-45 hembra y macho
Fuente: (Andrew S. Tanenbaum y David J. Wethersll, 2012)

2.3.11. Protocolos de comunicación

Se denomina protocolo de comunicación al intercambio de información entre computadores, más comúnmente es conocido como Protocolo de comunicación entre computadores, (José María Barceló Ordinas, Jordi Íñigo Griera, Ramón Martí Escalé, Enric Peig Olivé y Xavier Perramon Tornil, 2004).

Ilustración 4 Modelo de Protocolo de Comunicación
Fuente: (Stallings, 2004)

El Modelo OSI tiene siete niveles que se pueden unir para desarrollar las utilidades de comunicaciones para una computadora.

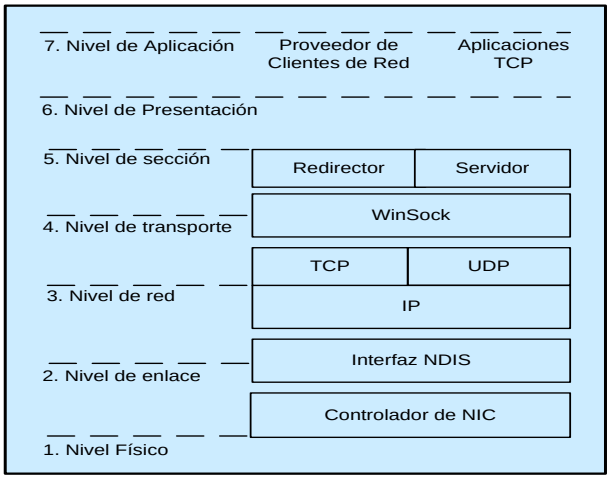


Ilustración 5 Modelo de referencia OSI
Fuente: (Estrada, 2016)

Nivel físico, este nivel transmite los bits por un canal de comunicación, interacciona con las interfaces mecánicas, eléctrica y funcionales del medio físico.

Nivel de enlace, este nivel se construye sobre los servicio de transmisión del nivel físico y agrupa los bits en una unidad lógica, dominada trama.

- Este nivel maneja los marcos perdidos, dañados o duplicados.
- Regula la velocidad del tráfico.
- En una red de broadcast, controla el acceso al canal compartido.

Nivel de red, determina el ruteo de los paquetes desde sus fuentes a sus destinos, manejando la congestión a la vez, el nivel de red define las direcciones de red.

Nivel de transporte, es el primer nivel que se comunica directamente con su par en el destino, provee varios tipos de servicio (por ejemplo, un canal punto-a-punto sin errores), podría abrir conexiones múltiples de red para proveer capacidad alta, se puede usar el encabezamiento de transporte para distinguir entre los mensajes de conexiones múltiples entrando en una máquina.

Nivel de sesión, este nivel se construye sobre los servicios del nivel de transporte y proporciona servicios especiales de secciones.

Nivel de presentación, este nivel gestiona la presentación de datos y define una sintaxis y una semántica común para la presentación de los mismos, de forma que puedan ser entendidos por sistemas.

Nivel de aplicación, define los protocolos y funciones que necesitan las aplicaciones individuales para efectuar tareas de comunicación; como por ejemplo e-mail, telnet, etc.

El modelo OSI es un modelo abstracto y sirve como norma para describir las distintas funciones de comunicación.

2.3.12. Protocolo TCP/IP

Según [G. Ulloa], es un conjunto de protocolos que han sido especificados para suplir las necesidades de interconectar las redes informáticas Internet.

Así como el modelo de referencia OSI, posee siete niveles o capas, la arquitectura TCP/IP viene definida por 4 niveles que lo veremos en la siguiente Figura.

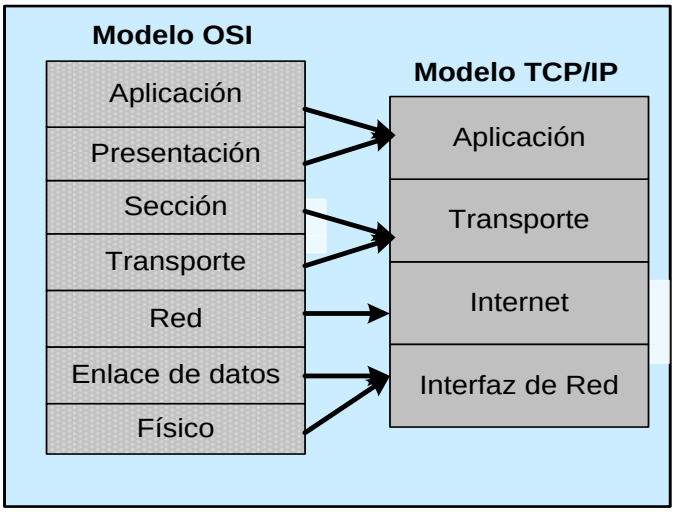


Ilustración 6 Modelo OSI vs. TCP/IP
Fuente: (Andrew S. Tanenbaum y David J. Wethersll, 2012)

Nivel de Interfaz de Red, los niveles físico y de enlace que juntos se llaman el "nivel de host a red".

Nivel de Internet, los hosts pueden introducir paquetes en la red, los cuales viajan independientemente al destino, no hay garantías de entrega ni de orden. Este nivel define el *Internet Protocol* (IP), que provee el ruteo y control de congestión.

Nivel de Transporte, permite que conjuntos de hosts de fuente y destino puedan conversar, existen dos protocolos:

Transmisión Control Protocol (TCP), provee una conexión confiable que permite la entrega sin errores de un flujo de bytes desde una máquina a alguna otra en la Internet, parte el flujo en mensajes discretos y lo monta de nuevo en el destino, maneja el control de flujo.

User Datagram Protocol (UDP), es un protocolo no confiable y sin conexión para la entrega de mensajes discretos, se pueden construir otros protocolos de aplicación sobre el UDP.

Nivel de aplicación, se presenta servicios de correo electrónico (*email*, *protocolo smtp*), transferencia de archivos (*ftp*), conexión remota (*telnet*), acceso web (http).

Protocolo de Internet (IP) el protocolo IP, es el principal del modelo OSI así como parte integral del TCP/IP, las tareas principales del IP son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas.

Las características de este protocolo son:

- No orientado a conexión
- Transmisión en unidades denominadas datagramas
- Sin corrección de errores, ni control de congestión
- No garantiza la entrega en secuencia.

2.4. DISPOSITIVOS DE RED DE DATOS

2.4.1. Routers

El router es el principal dispositivo con el que se trabaja cuando se está en la capa de red OSI, permite al router tomar decisiones basándose en las direcciones de red. Los routers también pueden conectar diferentes tecnologías, sin embargo, debido a su capacidad de **enrutar paquetes**, los routers se han convertido en el **backbone** de Internet, ejecutando el protocolo IP. (Nicolás Álvarez S. Juan Monsalve Z., 2008).

Ilustración 7 Símbolo del Router (Se observa flechas entrantes y salientes
Fuente: (Nicolás Álvarez S. Juan Monsalve Z., 2008)

El propósito de un router es examinar los paquetes entrantes, elegir la mejor ruta para ellos a través de la red y después conmutarlos al mejor puerto de salida. Los routers son el dispositivo regulador de tráfico más importante en las redes grandes. Permiten que cualquier tipo de computadora se comunique con otra en cualquier parte del mundo (Nicolás Álvarez S. Juan Monsalve Z., 2008).

Ilustración 8 Router Cisco 1760 – 1600
Fuente: (Estrada, 2016)

2.4.2. Hub

En general, el termino hub se emplea en lugar de repetidor cuando se refiere al dispositivo que sirve como centro de la red, como se puede observar en la figura 2.9. Aunque un hub opera en una topología física en estrella, crea el mismo entorno de contención que un bus. Esto se debe a que cuando un dispositivo transmite, el resto de dispositivos le escuchan y la contención crea un bus lógico. (Nicolás Álvarez S. Juan Monsalve Z., 2008)

El propósito de un hub es regenerar y reenviar señales de red. Esto se hace a nivel de bits con gran número de host. Esta acción se conoce como concentración. Estas son las propiedades más importantes de un hub:

- Regenerar y repetir las señales.
- Propagar las señales por la red.
- No pueden filtrar el tráfico de la red.
- No pueden determinar la mejor ruta.
- Se utilizan como puntos de concentración de la red.

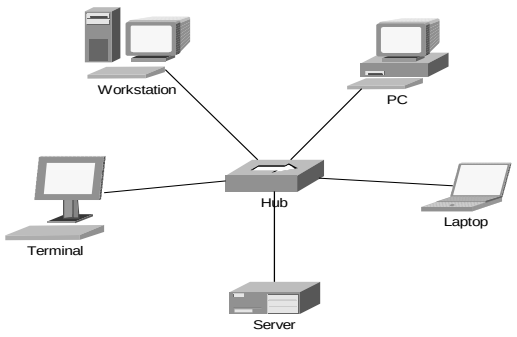


Ilustración 9 Símbolo del Hub (Se encuentra en el centro)
Fuente: (Stallings, 2004)

2.4.3. Switch

La diferencia entre un hub y un switch reside en lo que se sucede en el interior del dispositivo. La Figura 2.11 muestra el símbolo de un switch. Las flechas de la parte superior presentan los datos de rutas separadas que pueda haber en un switch, a diferencia del hub, donde los datos fluyen en todas las rutas. (Andrew S. Tanenbaum y David J. Wethersll, 2012)

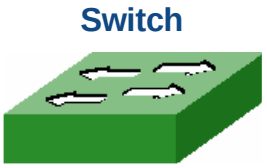


Ilustración 10 Símbolo del Switch (Se observa flechas salientes)
Fuente: (Nicolás Álvarez S. Juan Monsalve Z., 2008)

2.4.4. Wireless

Se denomina Wireless a las comunicaciones inalámbricas, en las que se utilizan modulación de ondas electromagnéticas, radiaciones o medios ópticos. Estás se propagan por el espacio vacío sin medio físico que comunique cada uno de los extremos de la transmisión.

Ilustración 11 Wireless
Fuente: (Stallings, 2004)

2.4.5. Patch Panels

Los patch panels son agrupaciones de racks RJ-45. Los hay de 12 y 48 puertos y normalmente están montados en racks (véase Figura siguiente). Los lados anteriores son racks RJ-45; los lados posteriores son bloques de empuje que proporcionan rutas de conectividad o de conexión. Se clasifican como componentes de la Capa 1. (Estrada, 2016)

Ilustración 12 Patch Panels
Fuente: (Estrada, 2016)

2.4.6. Servicios De Red

Los servicios de red son la fundación de una red de trabajo en un ambiente de computadoras. Generalmente los servicios de red son instalados en uno o más servidores para permitir el compartir recursos a computadoras clientes.

Los servicios de red más comunes son:

2.4.7. Servidor de Electrónico Correo

Según (Andrew S. Tanenbaum y David J. Wethersll, 2012), es una aplicación, que nos permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Es así que un servidor de correo, consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

Smtp (Simple Mail Transfer Protocol): Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.

Pop (Post Office Protocol): Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

Imap (Internet Message Access Protocol): Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

2.4.8. Servidor FTP

Según (Andrew S. Tanenbaum y David J. Wethersll, 2012), FTP es uno de los diversos protocolos de la red Internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Archivos) y es el ideal para transferir grandes bloques de datos por la red. Por defecto utiliza los puertos 20 y 21. El puerto 20 es utilizado para el flujo de datos entre el cliente y el servidor y el puerto 21 para el flujo de control, es decir, para enviar las órdenes del cliente al servidor.

El FTP, en la mayoría de los servidores, es la única manera de conectar con nuestro sitio, para así, poder subir (cargar) y bajar (descargar) archivos.

2.4.9. Servidor de página Web

Según (Andrew S. Tanenbaum y David J. Wethersll, 2012), es un programa que implementa el protocolo HTTP (hypertext transfer protocol). Este protocolo está diseñado para transferir lo que llamamos hipertextos, páginas web o páginas HTML (hypertext markup language)

Sin embargo, el hecho de que HTTP y HTML estén íntimamente ligados no debe dar lugar a confundir ambos términos. HTML es un formato de archivo y HTTP es un protocolo.

Un servidor Web, se encarga de mantenerse a la espera de las peticiones http, llevada a cabo por un cliente HTTP que solemos conocer como navegador.

2.4.10. Servidor Proxy

Es un ordenador[1], que facilita el acceso a internet a varios usuarios al mismo tiempo cuando están compartiendo una solo conexión a internet.

Según (Estrada, 2016), un proxy también es un dispositivo de firewall que examina los paquetes en las capas superiores del modelo de referencia OSI, que suelen ser en la capa 4 y 7, para más detalle ver en la Figura siguiente.

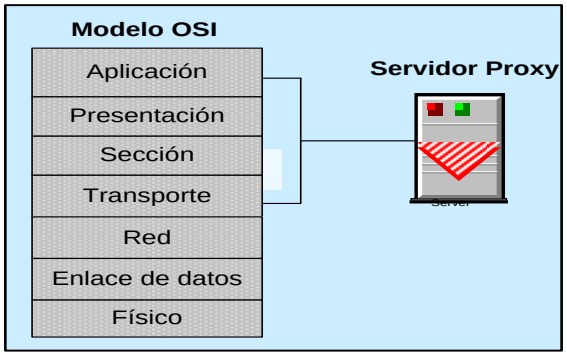


Ilustración 13 Modelo OSI - Filtros Proxy
Fuente: (Estrada, 2016)

Este dispositivo oculta datos valiosos exigiendo que los usuarios se comuniquen con un sistema seguro a través de un proxy. Los usuarios obtienen acceso a la red, pasando por un proceso que establece el estado de la sesión, la autenticación del usuario y la política autorizada, esto implica que los usuarios se conecten con servicios externos a través de programa de aplicación (squid).

Una forma de que funcione un firewall del filtro de proxy consiste en exigir que el usuario del

[1]Aparato informático capaz de procesar información, ya sea para archivarla o transmitirla. Necesita aplicaciones o programas para poder funcionar.

interior del firewall, construya primero una sección en el propio firewall (el Proxy es el destino de la sesión). El usuario deberá autenticarse en ese momento. En base a su Dirección IP, al usuario se le permite tener un acceso específico al exterior. Cuando se usa un firewall de proxy como este, se construyen dos secciones únicas (una desde el usuario al proxy y la otra desde el proxy hasta el destino), en el siguiente esquema se ve reflejado la función principal del servidor proxy ver la Figura siguiente.

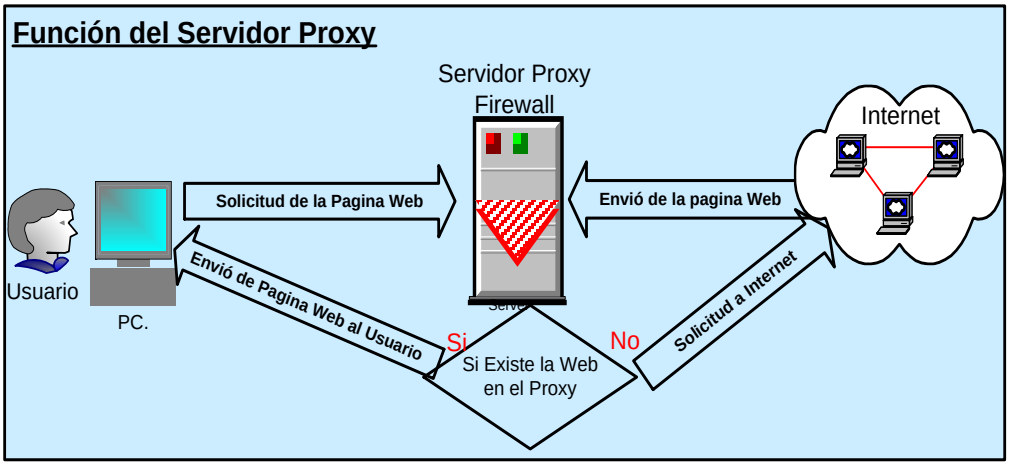


Ilustración 14 Función del servidor proxy
Fuente: (Estrada, 2016)

Una vez conocida la función principal del servidor Proxy, se comprende que es lo más posible para optimizar el ancho de banda y minimizar el riesgo de la red de datos de la EPSA COBIJA.

2.5. SEGURIDAD DE DATO

Según (Estrada, 2016), el objetivo de la seguridad, es fundamentalmente en pensar en las diferentes soluciones de seguridad de datos para que desde el inicio de todo dispositivos, plataforma, infraestructura, software etc. Se consideren sus parámetros de seguridad. El planteamiento debe definir el siclo de vida de la seguridad (SGSI: Sistema de Gesrion de la seguridad de la Información) y Diseñar la Implementación de las medidas técnicas y aplicar para la mitigación de los riesgo que el nivel Estratégico de la Organización.

2.6. ENDIAN FIREWALL

Según (SRL, 2019), Es una distribución GNU/Linux libre especializada en cortafuegos (Firewall), ruteo y gestión unificada de amenazas. Está siendo desarrollado por el italiano Sr Endian y la comunidad Endian está basado originalmente en IPCop, que además es un fork de SmoothWall.

Endian Firewall es una "llave en mano" de distribución de seguridad para Linux que convierte a todo el sistema en un dispositivo de seguridad con todas las funciones con gestión unificada de amenazas (UTM) funcionalidad. El software ha sido firmado con la de "pensando en el usuario" y es muy fácil de instalar, utilizar y gestionar, sin perder su flexibilidad.

Ilustración 15 Endian
Fuente: (http://www.i-t-m.com/productos-servicios/seguridad/endian-firewall

La misión de Endian Firewall es proteger la comunicación entre redes a nivel global y proveer acceso seguro a la información para su variada clientela. Los dispositivos Endian UTM para el control unificado de amenazas protegen las redes de más de 3000 clientes en alrededor de 40 países del mundo.

La principal característica de Endian es proveer un firewall de inspección de paquetes, proxies a nivel de aplicación para los distintos protocolos (HTTP, FTP, POP3, SMTP) con el apoyo de antivirus, virus y spamfiltering para el tráfico de correo electrónico (POP y SMTP), filtrado de contenido detráfico Web y una molestia " libre "solución VPN (basada en OpenVPN).

2.6.1. Lo Que Ofrece Endian Firewall.

Inspección de estados:

Endian Firewall es un appliance (sistema de búsqueda universal) basado en tecnología de inspección de estados que identifica cada paquete entrante, reconociendo la fuente y el contenido de cada paquete. Endian puede proteger contra intrusiones no deseadas o ataques externos de hackers.

Seguridad Integral:

Endian Firewall es un Appliance (sistema de búsqueda universal) de Seguridad Integral que protege su red y mejora la conectividad, ofreciendo todos los servicios que necesita y más, seguros y fácil de configurar. Endian Firewall es 100% open source e incluye, entre sus funciones principales una variedad de características:

- Firewall con inspección de estados.
- Antivirus HTTP/FTP.
- Filtro de Contenido Web.
- Antivirus POP3/SMTP, Anti-Phishing y Antispam.VPN SSL/TLS.
- IDS.

Seguridad de Correos:

Endian Firewall asegura cualquier servidor o cliente de correos, gracias a proxi es transparentes. Cualquier servidor de correos, como Microsoft Exchange o clientes como Outlook o Mozilla Thunderbird automáticamente serán protegidos y filtrados por Endian Firewall antivirus y antispam, no hay necesidad de modificar configuraciones de su servidor o cliente de correos.

Seguridad Web:

El filtro de contenidos de Endian Firewall mantiene una experiencia de navegación web de forma segura, protegiendo contra virus y contenidos no deseados como violencia, pornografía o software pirata. Permite al administrador de la red monitorizar accesos, mejorando así la productividad. También es útil en aquellas compañías que buscan que sus empleados naveguen solo por sitios bien definidos, asegurando así la integridad de los negocios y un uso adecuado de los recursos.

VPN Fáciles y Rápidas:

Gracias a OpenVPN, se puede rápidamente y sin complicaciones levantar un túnel seguro encriptado con SSL entre sucursales de tu compañía o entre agentes remotos hacia la red corporativa de la Empresa. Los clientes soportados abarcan una gran cantidad de Sistemas Operativos como lo son Linux, Mac OSX o Windows.

Hot Spot para Navegar en Áreas Públicas:

La solución Endian Host spot es una completa y flexible herramienta para manejar el acceso a Internet. Endian Hotspot permite a hoteles, librerías, escuelas, aeropuertos, bancos, ciber-cafes, entre otros, entregar a sus clientes acceso fácil y seguro a navegación Web.

Escoja la forma en que sus clientes navegan: sesiones basadas en tiempo o tráfico, con tickets de prepago o post pago o incluso acceso liberado.

2.6.2. ¿Qué es Internet?

Internet es una red de computadoras u ordenadores interconectados, capaces de compartir información y que permite comunicar a distintos usuarios sin importar su ubicación geográfica. Para que estas computadoras puedan compartir cualquier información, es preciso que tengan un "lenguaje en común" y esto es posible gracias a la existencia de un protocolo de comunicación, además de la infraestructura y los equipos necesarios. También se le conoce como "**superautopista de la información**". (Andrew S. Tanenbaum y David J. Wethersll, 2012)

2.6.3. Historia de Internet

Según (José María Barceló Ordinas, Jordi Íñigo Griera, Ramón Martí Escalé, Enric Peig Olivé y Xavier Perramon Tornil, 2004): Internet probablemente ha revolucionado el mundo, la industria informática y la de las telecomunicaciones como ningún otro invento lo haya hecho jamás. Podemos basar su gran eclosión a mediados de los años noventa debido a la introducción de multimedia y a la simplificación radical de la búsqueda de información con la introducción del World Wide Web (www). Por vez primera las búsquedas de un concepto se independizan de la ubicación geográfica de los contenidos a encontrar. Y el esfuerzo del usuario para hallar determinada información es idéntico si esta se encuentra en su ciudad como si reside en un servidor del otro lado del globo.

2.6.4. Servicios que brinda internet

Existe un sin fin número de servicios que brinda internet entre los cuales se menciona los siguientes:

2.6.5. Web

Según (Andrew S. Tanenbaum y David J. Wethersll, 2012), la World Wide Web (la "telaraña" o "maraña mundial") es tal vez el punto más visible de Internet y hoy en día el más usado junto con el correo electrónico, aunque también es de los más recientes.

La WWW puede definirse básicamente como tres cosas: hipertexto, que es un sistema de enlaces que permite saltar de unos lugares a otros; multimedia, que hace referencia al tipo de contenidos que puede manejar (texto, gráficos, vídeo, sonido y otros) e Internet, las base sobre las que se transmite la información.

El aspecto exterior de la WWW son las conocidas "páginas web". La Web es el lugar de Internet que más crecimiento está experimentando últimamente: se calcula que hay más de 50 millones de páginas Web en la Red, y su número crece a un ritmo vertiginoso. La Web, al facilitar la búsqueda de información, ha hecho que otros servicios de Internet como Gopher, Archie o WAIS se usen cada vez menos.

Cada vez son más las empresas que publican información en la Web. Y encontrarla es también cada vez más fácil: casi todos los nombres de los sitios Web comienzan por el URL que indica que se trata una página Web en formato HTML (http://) seguido de las letras características de la Web (www), el nombre de la institución (por ejemplo, .UAPNET) y terminan con el identificador de empresa (.EDU) o país (.BO). Es decir, si usted conecta con http://www.uapnet.edu.bo visitará las páginas de la Universidad Amazónica de Pando en Bolivia.

2.6.6. Correo Electrónico (e-mail)

Según (Estrada, 2016), el correo electrónico es un servicio de correspondencia (nacional e internacional), el cual por medio de una cuenta o buzón que posea usted en Internet, puede enviar o recibir documentos, gráficas, vídeos, sonidos, entre otras, de manera sencilla y rápida. Es también una dirección electrónica que sirve para enviar o recibir correo desde cualquier parte del mundo.

Una nueva forma de enviar cartas o mensajes electrónicos a personas, es haciendo uso de las

computadoras, a través del sistema de redes que componen Internet. Estos mensajes electrónicos viajan por las redes hasta alcanzar su destinatario, que puede ser un amigo conocido en cualquier parte del mundo, con un costo bastante reducido, sin tener que colocarlos una vez escrito, en un sobre y echarlos al buzón de correos.

2.6.7. Chat

Según (Stallings, 2004), tres de cada cinco usuarios Bolivianos de Internet pasaron al menos una vez por las salas de Chat. Uno de cada dos chatea con frecuencia.

Chat es una palabra en ingles cuya traducción significa conversar, pero a esta altura se convirtió en un término específico para designar el encuentro entre dos o más personas en Internet que mantienen una conversación en tiempo real. Para chatear basta con tener una PC, con conexión a Internet, elegir un apodo o nick e ingresar en alguna sala.

El chat fue evolucionando y paso desde los precarios BBS (Bulletin Board System, una de las formas más primitivas de establecer conexiones entre computadoras) a los universos virtuales, que incluyen audio y video. En poco tiempo se convirtió en una verdadera pasión de multitudes.

¿Por qué? Probablemente porque reúne las tres características del éxito: es fácil, divertido y gratis. Además, el chat es útil para crear un espacio de reunión entre personas con los mismos intereses y se puede contactar a las personas que están a mucha distancia por bastante menos que una comunicación telefónica.

2.7. POLÍTICAS

Son normas y procedimiento que nos sirven para orientar la acción; criterios o lineamientos generales a observar en la toma de decisiones, sobre problemas que se repiten una y otra vez en el ambiente de una organización.

2.7.1. Políticas de Seguridad

Según (Estrada, 2016), son los documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos tanto de usuarios como administradores, describe lo que se va a proteger y de lo que se está tratando de proteger.

Es importante resaltar que las políticas de seguridad tienen un ciclo de vida completo mientras está vigente. Este ciclo de vida incluye un esfuerzo de investigación, la labor de escribirlas, lograr que las directivas de la organización la acepten, conseguir que sea aprobada, lograr que sea diseminada a través de la organización, concienciar a los usuarios de la importancia de las políticas, conseguir que la acaten, hacerle un seguimiento, garantizar que esté actualizada y finalmente suprimirla cuando haya perdido vigencia.

Según (Andrew S. Tanenbaum y David J. Wethersll, 2012), existen varias razones por las cuales es recomendable tener políticas escritas en la EPSA COBIJA Describimos algunas razones importantes.

1. Para aplicar con regulaciones legales o técnicas.
2. Como guía para el comportamiento profesional y personal.
3. Permite unificar la forma de trabajo de personas en diferentes lugares o momentos que tengan responsabilidades y tareas similares.
4. Permite recoger comentarios y observaciones que buscan atender situaciones anormales en el trabajo.
5. Permite encontrar las mejores prácticas en el trabajo
6. Permite asociar la filosofía de una organización (lo abstracto) al trabajo (lo concreto).

En muchas ocasiones, el término "política" es utilizado en un sentido genérico para aplicarlo a cualquier de los tipos de requerimientos de seguridad expuestos, para elaborar políticas de seguridad existen varias etapas para su desarrollo.

i) Etapas en el Desarrollo de una Política

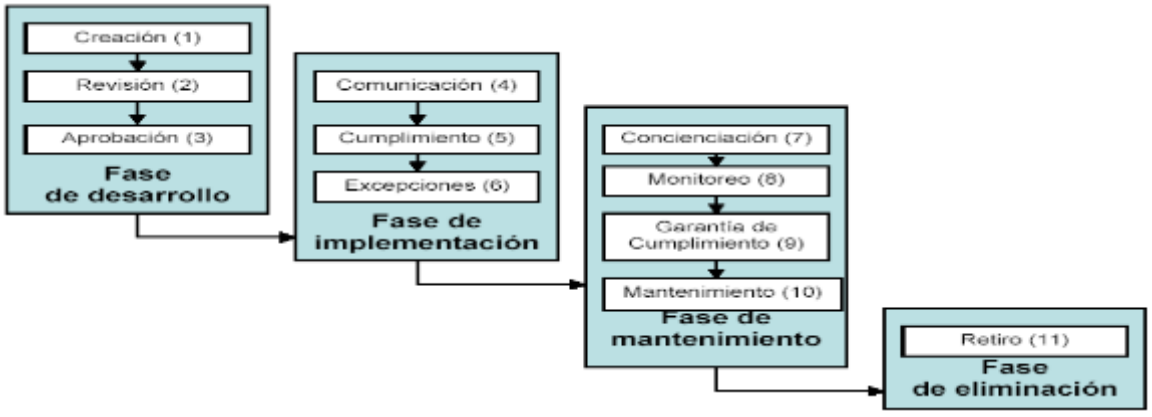


Ilustración 16 Etapas para el desarrollo de las políticas
Fuente: (José María Barceló Ordinas, Jordi Íñigo Griera, Ramón Martí Escalé, Enric Peig Olivé y Xavier Perramon Tornil, 2004)

Existen 11 etapas que se deben realizarse a través de la "vida" de una política, estas etapas pueden ser agrupadas en 4 fases.

1. **Fase de desarrollo:** Durante esta fase es creada, revisada y aprobada.
2. **Fase de implementación:** En esta fase la política es comunicada y acatada (o no cumplida por algunas excepciones).
3. **Fase de mantenimiento:** Los usuarios deben ser conscientes de la importancia de las políticas, su cumplimiento debe ser monitoreada, se debe garantizar su cumplimiento y se le debe dar mantenimiento (Actualización).
4. **Fase de eliminación:** Las políticas se retira cuando no se requiera más.

Para garantizar que todas las etapas del ciclo de vida sean realizadas se manera apropiada y las responsabilidades para la ejecución sean asignadas adecuadamente, la universidad debe establecer un marco de referencia para facilitar el entendimiento, promover la aplicación consistente, establecer una estructura jerárquica para soportar mutuamente los distintos niveles de políticas y acomodar afectivamente los frecuentes cambios tecnológicos y organizacionales.

Una vez concluido todas las etapas del desarrollo de las políticas, solo nos resulta poner en práctica el buen uso adecuado de las mismas.

2.8. DESCRIPCIÓN DE LAS HERRAMIENTAS UTILIZADAS.

2.8.1. Herramienta para medir el rendimiento de la Red.

✓ Ping

Ping es la herramienta por excelencia para comprobar la conectividad. Esta herramienta viene por defecto incluida en todas las versiones de Windows, por lo que su uso no requiere ningún software adicional ya que se ejecuta como símbolo de sistema desde una ventana de MS-DOS. Esta herramienta realiza por defecto 4 conexiones seguidas a un servidor y nos devuelve el estado de dicho servidor, así como el tiempo de cada una de dichas conexiones.

2.8.2. Herramienta de Administración de la Red.

✓ Endian Firewall

Endian Firewall está basado en Red Hat Enterprise Linux, por lo cual Endian Firewall es 100% de código abierto. Esta distribucion de Linux incluye una amplia variedad de funciones, como firewall

de inspección con estado, antivirus HTTP / FTP, filtro de contenido, antivirus POP3 / SMTP, antiphishing y herramientas de contra el spam, SSL / TLS VPN, IDS y otras características.

Al contar con un Firewall, podemos establecer reglas de DE REGLAS DE ENTRADA Y SALIDA, también podemos crear una puerta de enlace VPN con ayuda de OpenVPN o IPsec.

Esta distribución es una solución opensource ya que como les comento, está orientada para actuar como un Firewall, siendo así una solución totalmente integral para la protección de redes ofreciendo todos los servicios que brinda un UTM (Gestión Unificada de Amenazas) además es muy fácil de usar e instalar.

2.8.3. Sistemas operativos.

- ✓ Windows 7 Pro.

Windows 7 es una versión de Microsoft Windows, línea de sistemas operativos producida por Microsoft Corporation. Esta versión está diseñada para uso en PC, incluyendo equipos de escritorio en hogares y oficinas, equipos portátiles, tabletas, netbooks y equipos multimedia.2 El desarrollo de Windows 7 se completó el 22 de julio de 2009, siendo entonces confirmada su fecha de venta oficial para el 22 de octubre de 2009.

2.8.4. Herramientas de red

- ✓ Cable de red Cat. 6

El Cable de categoría 6, o Cat 6 (ANSI/TIA/EIA-568-B.2-1) es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es retro compatible con los estándares de categoría 5/5e y categoría 3. La categoría 6 posee características de onda y especificaciones para evitar la diafonía (o crosstalk) y el ruido. El estándar de cable se utiliza para 10BASE-T, 100BASE-TX y 1000BASE-TX (Gigabit Ethernet). Alcanza frecuencias de hasta 250 MHz en cada par y una velocidad de 1 Gbps. La conexión de los pines para el conector RJ45 que en principio tiene mejor inmunidad a interferencia arriba de 100Mbps es el T568A

- ✓ Patch Panel Categoría 6

El Patch Panel o Panel de Parcheo es el elemento encargado de recibir todos los cables del cableado estructurado. Desde los puntos de red (rosetas) de cada puesto de trabajo hasta los Racks

(armarios) donde se encuentran estos paneles de parcheo. Sirven para organizar las conexiones de red mediante los Patch Cords, para que se puedan realizar de forma fácil y cómoda modificaciones en la interconexión de los elementos relacionados de la red LAN y los equipos de conectividad como ser hubs, switches, routers, etc.

✓ Ponchadora Impacto

Una ponchadora de impacto es una herramienta de precisión y punción con carga de resorte utilizado para empujar los hilos entre los pins de metal, permitiendo pelar al mismo tiempo el revestimiento del cable de red UTP. Funciona por compresión e impacto, ya que su resorte interno golpea los hilos de los cables UTP una vez que se ordenan según un código de colores específico sobre las cuchillas que tiene un módulo RJ45 hembra. A esta técnica de conectorizado se le llama IDC conexión por desplazamiento de aislación.

✓ Conectores RJ45

El conector RJ45 (Registered Jack) o plug RJ45 es el principal conector usado en la conexión de tarjetas de red Ethernet. Este conector se emplea con cables de par trenzado, por lo que el mismo conector se puede emplear para tipos de comunicación diferente, dependiendo del orden de conexión de los pares trenzados. Es un conector estándar de red, que permite la interconexión de dispositivos de red entre sí mediante un cable UTP de 4 pares (8 hilo de cables). Existen dos formas de unir estos conectores a los cables:

- De forma manual mediante el crimpado con una tenaza o alicate de Red.
- Mediante un proceso industrial de vacío que fija los contactos y el conector al cable.

Normalmente este conector se fabrica en plástico, y sus conexiones metálicas. Se usa plástico trasparente para los conectores que se unen a los cables de forma manual, de esta forma, se puede visualizar si los pares trenzados se conectan correctamente.

Algunos conectores tienen un recubrimiento metálico utilizado como pantalla electromagnética para evitar interferencias. Estos conectores se utilizan para cables UTP con malla o recubrimiento electromagnético. De esta forma, cuando el conector es crimpado en el cable UTP, el apantallamiento del cable se extiende también hasta el conector.

✓ Alicate de Mantenimiento de Red RJ45

Es una pinza que se utiliza para colocar el plug de RJ45 en el cable UTP, tiene una navaja para cortar el cable y una mueca para pelar el cable; en la parte central se encuentra la parte donde se mete el conector armado.

- ✓ Instrumento de Medición Tester de Red

  Es la herramienta que nos permite verificar la continuidad de un cable UTP que se haya armado, así como también detectar cruzamientos de los alambres.

- ✓ Racks (mural).

  Es un término inglés que se emplea para nombrar a la estructura que permite sostener o albergar un dispositivo tecnológico. Se trata de un armazón metálico que, de acuerdo a sus características, sirve para alojar una computadora, un router u otra clase de equipo lo habitual es que los racks puedan ensamblarse para contener, en conjunto, una gran cantidad de equipos. De este modo, aquello que se entiende por rack suele ser utilizado en instituciones científicas o educativas, oficinas gubernamentales o grandes corporaciones.

  Por lo general, los racks (que también se conocen como cabinas o bastidores) se hallan en los centros de datos que disponen de muchos servidores. El correcto armado de la estructura es esencial para el funcionamiento de los equipos, ya que los cables deben organizarse de manera adecuada para lograr las conexiones.

  La finalidad de los racks es el aprovechamiento del espacio. Gracias a estas estructuras, es posible ordenar muchos dispositivos en un espacio físico reducido, facilitando también el acceso a los mismos. Tanto su instalación, que requiere de la elaboración de una compleja red de cableado y la correcta fijación de los equipos para evitar daños, como su mantenimiento son complejos y un mínimo descuido puede poner en riesgo el trabajo de mucha gente.

- ✓ Roseta de superficie de conector red hembra RJ45.

  La roseta es el conector que nos permite conectar el cable de Red y sirve para transmitir voz y datos, permite transmitir información a través del cable de par trenzado. Las rosetas de superficie son herramientas que nos ofrecen una solución económica y una rápida instalación en cualquier situación. Incluye tornillos de montaje, cinta adhesiva, atadura de cables para el alivio de la tensión y la etiqueta para escribir en ella con el titular

- ✓ Switch gigabit

  Los Switch es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3) (VER ANEXO H).

CAPÍTULO III

3. MARCO APLICATIVO

3.1. ADMINISTRACIÓN DE LA CONFIGURACIÓN

3.1.1. Planeación y diseño de la Red

Como parte de la planificación se vio la necesidad de contar con información inicial del estado en el que se encontraba la red de datos y el servicio de internet. Para la obtención de esa información se realizó un diagnostico total el cual trajo consigo resultados que se detallan a continuación.

3.1.2. Diagnóstico total de la Red de Datos e Internet

El diagnóstico de la red de datos e internet sirvió para apreciar la situación en la que se encontraba la red de datos e internet, todo el relevamiento de la información que se obtuvo fue concerniente a la estructura física y lógica de la red de datos, así como la consulta a los usuarios de la EPSA municipal, de los requerimientos y/o reclamos que tenían cada uno de ellos con respecto a la red de datos y el servicio de internet.

A continuación, se muestra figuras la cual se evidencia el estado de la conexión de la red de datos al hacer un ping a otro equipo de computación existe retardación y perdidas de información esto producido por interferencias eléctricas el cual no cumplía ciertas normas de cableado y el deterioro de los cables producidos por los pisotones.

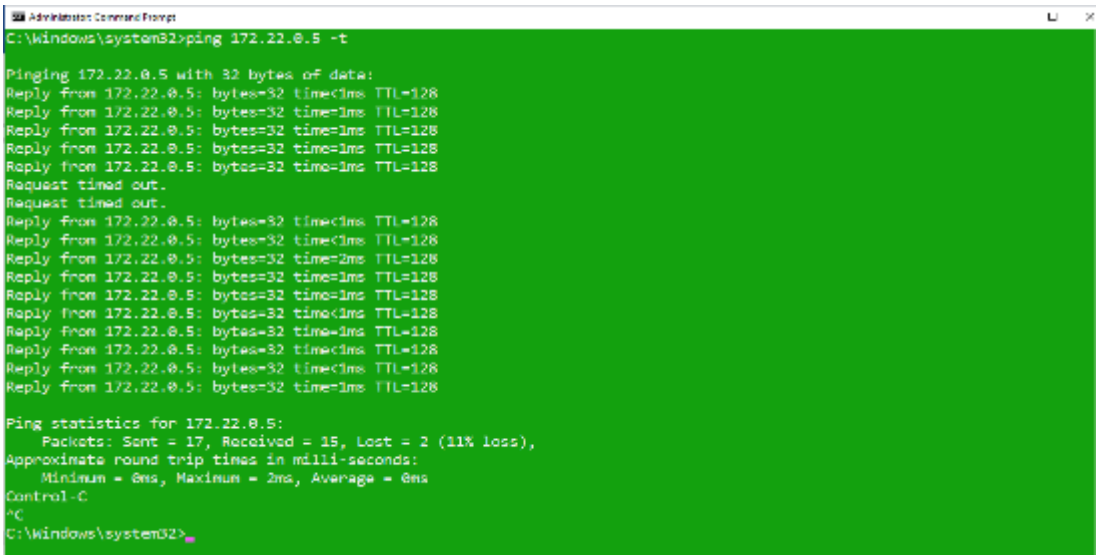


Ilustración 17 Test de la red de datos
Fuente: Elaboración propia

A continuación, se muestra una representación gráfica que resume los resultados obtenidos en el diagnóstico de la red de datos y el servicio de internet.

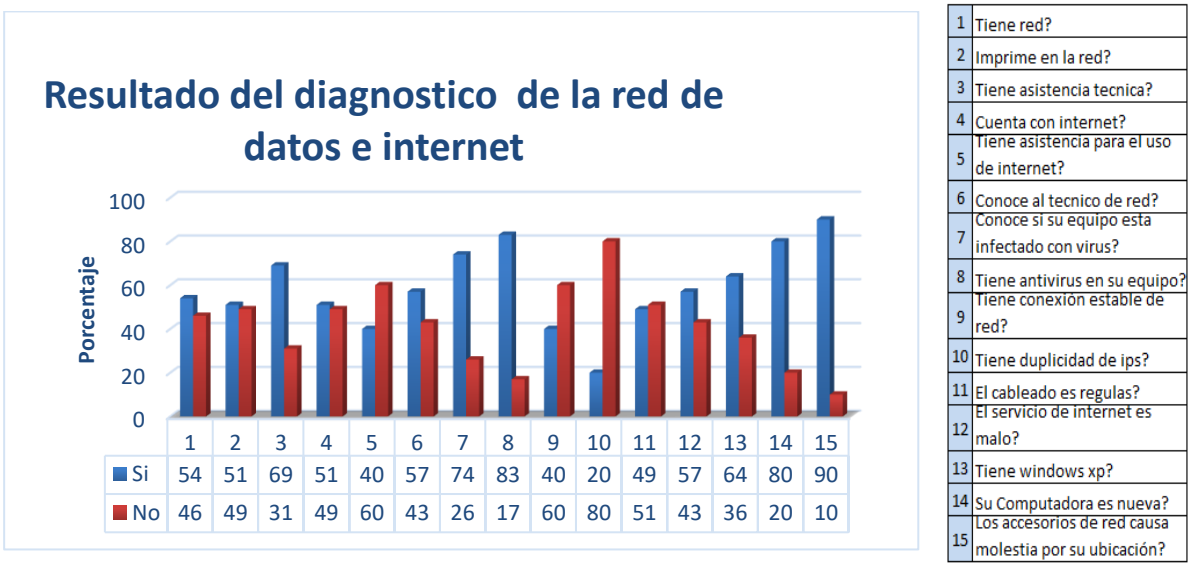


Ilustración 18 Diagnóstico de la red de datos y el servicio de internet
Fuente: Elaboración propia

El diagnóstico total de la red de datos e internet ayudó a detectar un conjunto de problemas los cuales surgen como una necesidad por parte de los usuarios. Para obtener información fiable se vio por conveniente centralizar en un solo grupo; esto para saber la situación actual de la red de datos de la EPSA COBIJA.

Se entrevistó a cada Jefaturas, Unidades y Secciones de forma aleatoria una muestra representativa los cuales se puede evidenciar en la Tabla siguiente.

Oficinas	**Usuarios**
Gerencia General	2
Gerencia Técnica	3
Jefatura Financiera	4
Jefatura Comercial	5
Asesoría legal	2
RRHH	2
Odeco	2

Tabla 4 Cantidad de Usuarios encuestados por Jefaturas, Unidades y Secciones que cuentan con un computador
Fuente: Elaboración propia

Para el planteamiento de las preguntas se decidió subdividirlas en cuatro aspectos: el primer aspecto concerniente a los conocimientos del usuario, el segundo aspecto concerniente a la red de datos, el tercer aspecto concerniente al servicio de internet y el cuarto aspecto en asuntos varios. Las preguntas realizadas concernientes al primer aspecto fueron 4, del segundo aspecto fueron 9, del tercer aspecto fueron 8 y respecto al cuarto aspecto fueron 4 haciendo un total de 25 preguntas cerradas, de las cuales se seleccionó las más representativas y son analizadas en la Siguiente Figura Para la comprensión de la Figura se desarrollan las siguientes interpretaciones:

1. Del total de personas entrevistadas, 54% cuenta con la conexión a la red de datos y el 46% no tiene este servicio.
2. Del total de personas entrevistadas, 51% utiliza el servicio de impresión a través de la red de datos y el 49% restante no utiliza esta forma de impresión.
3. Del total de personas entrevistadas, 69% cuenta con asistencia técnica con problemas relacionados a la red de datos y el 31% no cuenta con este elemental servicio.
4. Del total de personas entrevistadas, 51% cuenta con el servicio de internet en su equipo y el 49% no tiene este elemental servicio.
5. Del total de personas entrevistadas, 40% cuenta con asistencia técnica cuando tiene algún problema o duda referente al servicio de internet y el 60% no cuenta con la mencionada asistencia técnica.
6. Del total de personas entrevistadas, 57% conoce quien es el responsable de dar asistencia técnica a la red de datos o al servicio de internet y el 43% no conoce al responsable de la mencionada asistencia técnica.
7. Del total de personas entrevistadas, 74% conoce cuando una computadora está infectada de virus y el 26% no se da cuenta si su equipo está con virus.
8. Del total de personas entrevistadas, 83% tiene instalado en su equipo (computadora) algún antivirus y sabe dar uso a esta herramienta, y el 17% no tiene instalado ningún antivirus y por lo tanto no da uso de esta herramienta.
9. De toda la observación realizada a la Epsa Municipal cobija, 40% de los usuarios tiene una conexión estable a la red de datos, y el 60% permanentemente tiene problemas de conexión.
10. De toda la observación realizada a la Epsa Municipal cobija, 20% de los usuarios tiene problemas de duplicidad de ip´s, y el 80% no tiene problemas de ip´s.
11. Del total de las personas entrevistadas, 49% observa la conexión del cableado de la red de datos regular, y el 51% les parece malo.

12. Del total de las personas entrevistadas, 57% califica el servicio de internet malo, y el 43% regular.
13. Del total de las personas entrevistadas, el 64% utiliza sistema operativo Windows 7, y el 36% utiliza otro sistema operativo como y Windows 8.1 y 10.
14. De toda la observación realizada a la Epsa Municipal cobija, 80% son equipos de computación de última generación, y el 20% son equipos antiguos.
15. De toda la observación realizada a la Epsa Municipal cobija, 90% de los equipos de red están mal ubicados causando molestia al usuario, y el 10% está en buena ubicación.

Con respecto al uso del servicio de Internet se puede ver en la gráfica el tiempo que el usuario utiliza diariamente el mencionado servicio.

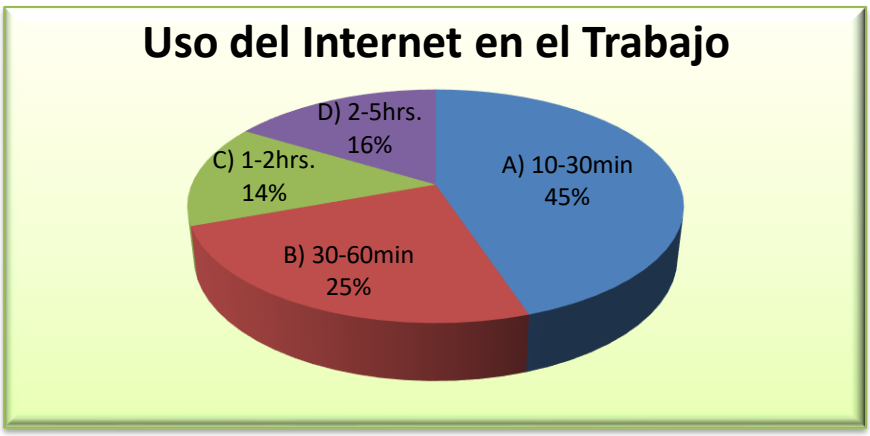


Ilustración 19 Torta de uso del internet en el trabajo
Fuente: Elaboración propia

En el parámetro de tiempo se observó que los usuarios usan el internet, en un promedio mayor a una hora diaria, aun teniendo en cuenta que el internet no es constante, en la que la mayoría de los usuarios usan paginas informativas de acorde a su labor de trabajo, pero se obtuvo un porcentaje considerado de las personas que usan y visitan páginas pornográficas y descargar de videos de youtube en la que es desventajoso para el tráfico de ancho de banda.

Toda la secuencia de resultados parciales que implican el diagnostico puede observarse con más detalle en (ANEXO I).

3.1.3. Conclusiones del Diagnostico

De acuerdo al análisis que se obtuvo del levantamiento de la información se concluyó las siguientes:

- Diseñar e implementar la nueva red de datos.
- Elaborar nuevos rangos de ip´s.
- Mejorar la conexión de la red de datos.
- Elaborar e implementar políticas de uso de la Red de Datos y el Servicio de internet.
- Implementar el servidor proxy para mejorar el servicio de internet.
- Combatir los virus informáticos.
- Brindar asistencia técnica a los usuarios de forma rápida e inmediata.
- Controlar y monitorear el servicio de internet.

3.1.4. Selección de la infraestructura de red

La selección de la infraestructura de red está en función a dos fases, la primera fase se hizo la selección de los equipos de computación y de red existentes que estaban en buen funcionamiento para reorganizar sus posiciones y avanzar en la implementación en un 30% de acuerdo al nuevo diseño de red.

La segunda fase se adquiero la infraestructura de red y se logró completar el diseño de la red, cada una de las fases requería diferente infraestructura de red (equipos informáticos y equipos de red).

3.1.5. Selección de infraestructura de red de la primera fase

Equipos informáticos y de red básicos (mínimos y necesarios) para el funcionamiento de la **primera fase** se detallan a continuación:

- **Infraestructura para los usuarios (Hardware):** Los requerimientos de hardware para los usuarios es el siguiente:

PC EQUIPO DE ESCRITORIO	
TARJETA MADRE	ASUS P8P67 M-PRO
MEMORIAS RAM	2 GB. DDR2
DISCO DURO	500 GB SAMSUNG
PROCESADOR	INTEL CORE 2 DUO 2.93 GHZ.
MONITOR	LG 14 PULG.
MOUSE	OPTICO
TARJETA DE RED	Intel Graphics Media accelerator 3100

Tabla 5 Infraestructura para los usuarios (Hardware
Fuente: Elaboración Propia.

- **Infraestructura utilizada para el servidor proxy (Hardware):** La selección de la infraestructura utilizada en el servidor proxy se describe a continuación:

Microprocesador: Intel Core 2 Duo 2.93 Ghz.
Memoria RAM: 4 GB.
Disco duro: 80 GB.
Tarjeta de Red: Intel Graphics Media accelerator 3100
Tarjeta Madre: ASRock G31M-VS2.
Monitor: LG- FLATRON L1753T
Teclado: Genius
Mouse: Óptico Genius

- Infraestructura para el funcionamiento de la red de datos y el servicio de internet (Equipos de Red): Todos los equipos seleccionados se detallan en la Tabla siguiente.

Nro.	DESCRIPCION	CARACTERISTICA	CANT.	UNIDAD
1	Racks (mural).	Alturas: 6U Anchos: 550 mm Fondos: 335 mm (1 cuerpo), Puertas: Cristal	1	PZA
2	Patch Panel	24 puertos Cat. 6	1	PZA
3	Switch Gigabit TP-LINK modelo TP-SG2224WEB	24 puertos 10/100/1000 Mbps más 2 puertos SFP administrable.	1	PZA
4	Switch TP-LINK modelo TL-SL2428WEB	24 puertos 10/100Mbps más 4 puertos Gigabit Web administrable.	1	PZA
5	Switch D-LINK modelo DES-1016D.	Switch no administrable de 16 puertos 10/100Mbps	1	PZA
6	Modem Router inalámbrico TP LINK	Modelo TD W8101G 54 Mbps ADSL.	1	PZA
7	Cable de Red	Categoría 6.	1	CAJA
8	Conectores RJ45	Categoría 6.	100	PZA
9	Roseta de superficie de conector red hembra RJ45.	Categoría 6.	35	PZA
10	Tester de Red	Categoría 6.	1	PZA
11	Alicate de Mantenimiento de Red RJ45	RJ45	1	PZA
12	Ponchadora Impacto	Herramienta de precisión y punción con carga de resorte	1	PZA
13	Alicate pela cable	Auto Ajustable	1	PZA
14	Canaleta enganchable para	Plástica 40mm x 20mm x 1,5mts	50	PZA

	dos cables			
15	Canaleta	50x50mm 2M (ductos ranurados)	20	PZA
16	Canaleta	20x10 2M (ductos ranurados)	15	PZA
17	Ducto de piso para cables	Opcional	10	PZA
18	Precintos plásticos ajustables 4.8x20cm	Opcional	5	BOLSAS
19	Precintos plásticos ajustables 7.6 x 30cm	Opcional	5	BOLSAS
20	Cinta aislante de 3M	Opcional	5	UNIDAD
21	Codos para empalme de ducto o canaletas	Opcional	20	PZA
22	Tijera corta canaleta	Opcional	1	PZA
23	Grapas curvas para guía de cable	Opcional	5	BOLSAS
24	Estilete grande o navaja (Cutter)	Opcional	1	PZA
25	Taladro	Opcional	1	PZA
26	Broca para madera larga 1/2 x 12	Opcional	2	PZA
27	Broca para concreto Larga 1/2 x12	Opcional	2	PZA
28	Broca para concreto 6mm.	Opcional	2	PZA
29	Mandril para cota	9 cm de 3/8 pulg.	1	PZA

	círculo de concreto			
30	Cierra corta círculos de concreto	3 pulg.	1	PZA
31	Tornillos Chip 35x30	Opcional	4	DOCENA
32	Ramplús Nro.6	Opcional	4	DOCENA
33	MikrotTik	RB/750r2	1	PZA

Tabla 6 Infraestructura para el funcionamiento de la red de datos e inter
Fuente: Elaboración Propia

3.1.6. Clasificación de nuevos rangos de IP´S

La distribución de rangos de direcciones IP, de la red de datos de la EPSA COBIJA, pertenece a una red de clase B, por su tamaño que habitualmente se utiliza para redes pequeña.

Los que se define de la siguiente manera de acuerdo a los grupos de usuarios clasificados más detalle ver la Tabla siguiente.

IP's EPSA COBIJA	
Rango de IP	Tipo de Usuario
172.22.0.1	Servidor Proxy
172.22.0.2 – 8	Gerencia General
172.22.0.9 – 15	Gerencia Técnica
172.22.0.16 – 25	Jefatura Financiera
172.22.0.26 – 40	Jefatura Comercial
172.22.0.41 – 45	Asesoría Legal
172.22.0.46 – 55	RR.HH.
172.22.0.56 – 62	Odeco
172.22.0.63 – 254	Libres

Tabla 7 IP`s de Usuarios EPSA COBIJA
Fuente: elaboración propia

3.1.7. Selección de infraestructura de red de la segunda fase

Los equipos informáticos y de red necesarios para el funcionamiento de la **segunda fase** son los siguientes:

- **Infraestructura para la red de datos (Equipos de Red):** Todos los equipos necesarios para la reestructuración total se detallan a continuación en la Tabla siguiente.

N°	DESCRIPCION	CARACTERISTICA	CANT.	UNIDAD
1	Cable Canal con adesivo	Plástica 10mm x 10mm x 2 mts	25	PZA
2	Cable de Red	Categoría 6.	3	CAJA
3	Tornillos Chip 35x30	Opcional	5	DOCENA
4	Ramplús Nro.6	Opcional	5	DOCENA

Tabla 8 Infraestructura para la segunda fas
Fuente: Elaboración Propia

3.2. INSTALACIÓN Y ADMINISTRACIÓN DEL SOFTWARE

Esta actividad consigue un manejo adecuado de los recursos de la red de datos, para lo cual se divide en dos partes de acuerdo a la metodología de administración de redes, la instalación de hardware y administración de software.

3.2.1. Instalación de Hardware

Antes de realizar el análisis de la red de datos e internet el diseño lógico era tal cual se muestra en la Figura siguiente:

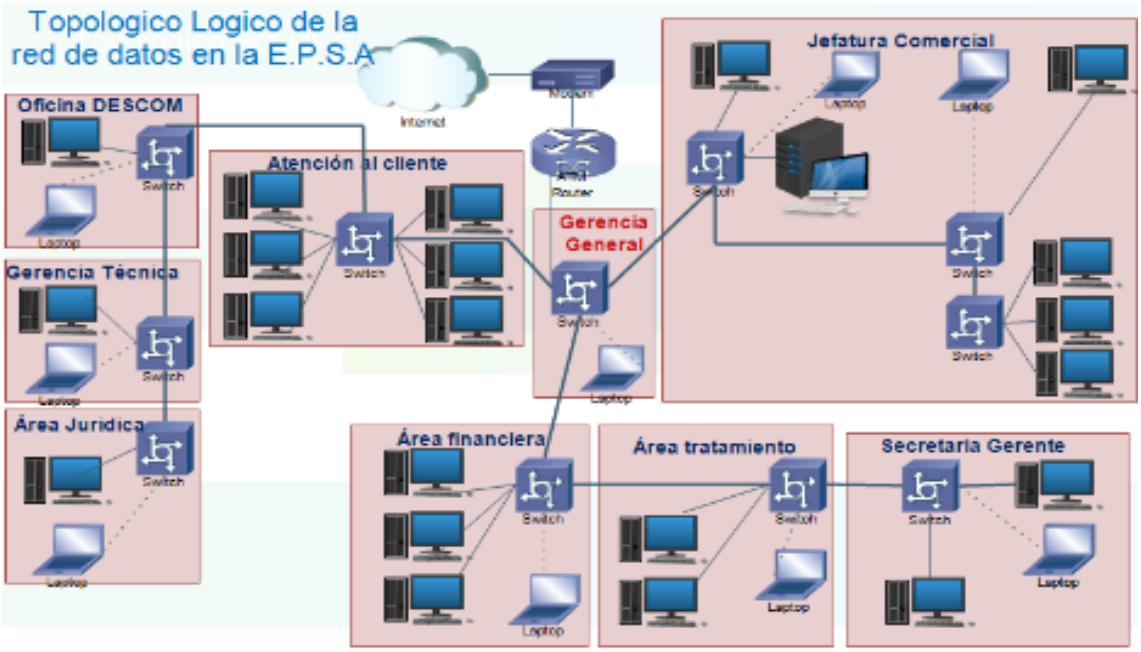


Ilustración 20 Diseño lógico anterior de la red de datos
Fuente: Elaboración propia

Este diseño lógico de red tenía deficiencia con el servicio de internet e intranet porque no existía control de acceso a dichos servicios y a ciertas páginas web, la inexistencia de políticas de uso y la mala ubicación que tenían los accesorios de red para brindar un buen servicio.

Para la instalación del hardware se trabajó en base al nuevo diseño propuesto que enlaza todas las Jefaturas, Unidades y Secciones de la Epsa Municipal Cobija.

a) **Cableado del nuevo diseño de la red de datos de la Epsa municipal.**

Para garantizar el funcionamiento de la red de datos y del servicio de internet y del servidor se vio por conveniente reorganizar el cableado de todo el predio de la EPSA COBIJA de acuerdo al nuevo diseño.

A continuación, puede observar en las figuras el diseño físico de todos los ambientes de la EPSA COBIJA.

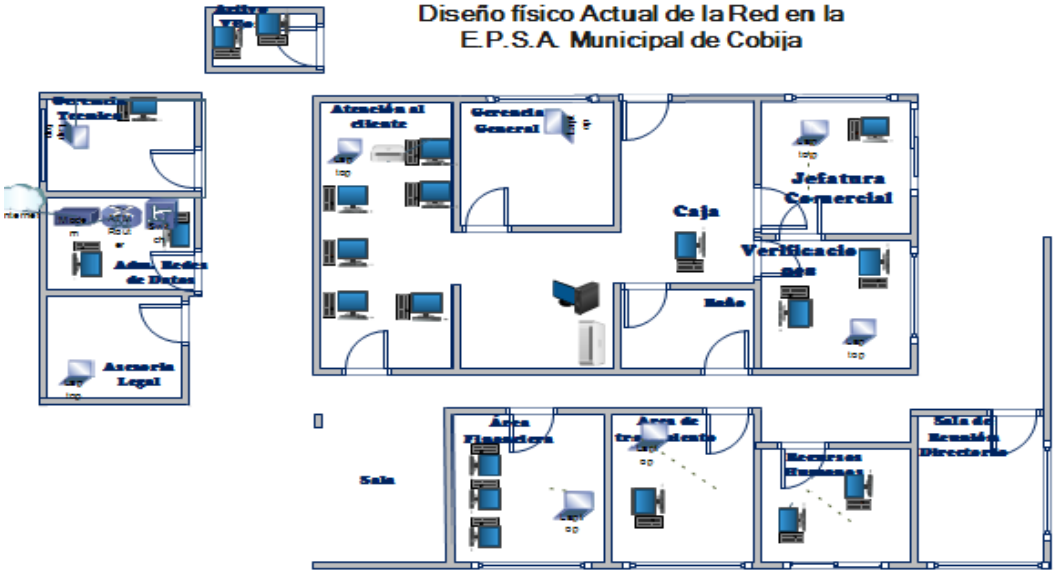


Ilustración 21 Cableado del nuevo diseño en todas las Jefaturas y unidades
Fuente: Elaboración propia

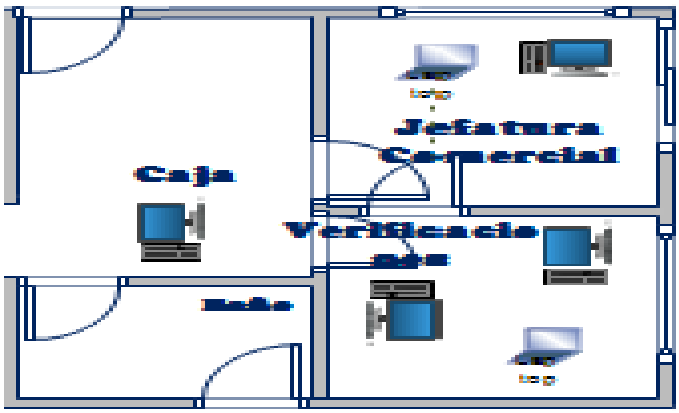


Ilustración 22 Diseño físico del cableado de la red "Jefatura Comercial"
Fuente: Elaboración propia

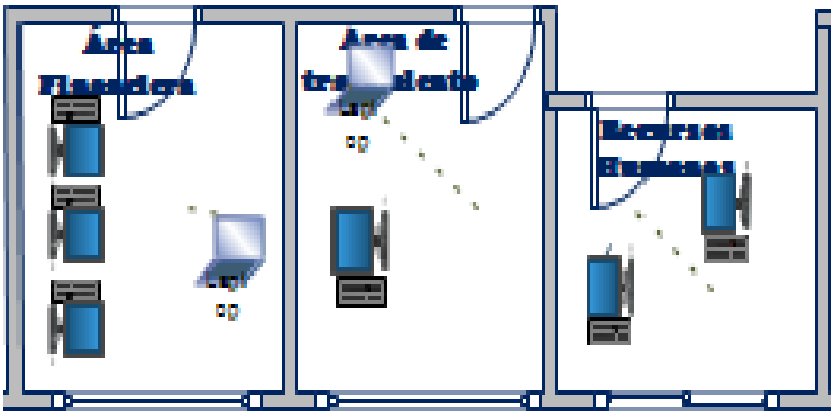


Ilustración 23 Diseño físico de la red inalámbrica "Jefatura Financiera"
Fuente: Elaboración propia

Ilustración 24 Diseño físico del cableado de red "Administración de Redes
Fuente: Elaboración propia

- **Instalación de software**

La instalación de software comprende cuatro actividades las cuales son detalladas a continuación:

a) Instalación y configuración de Endian Firewall.

Los aspectos técnicos para la instalación y configuración del Endian Firewall se detallan en la siguiente Tabla.

Nº	Actividad	Detalle	Observaciones
1	Instalación del Endian Firewall	Antes de comenzar con la instalación debemos descargarnos la ISO de Endian desde su página oficial. https://www.endian.com/community/overview/	Para realizar la instalación de Endian se debe seguir los pasos que se detallan en el Anexo J.
2	Configuración del Endian Firewall	Configurar la interfaz de red eth0 con la dirección IP para la distribución de Internet y la eth1 para el acceso a la red LAN.	Este servidor fue configurado para el control y distribución del servicio de Internet.

Tabla 9 Datos técnicos de la instalación y configuración de Endian Firewall
Fuente: Elaboración Propia

b) Configuración del Protocolo TCP/IP en los equipos informáticos (computadoras) de los usuarios

Para la configuración del protocolo TCP/IP se siguió los criterios que se detallan en la Tabla siguiente.

Nº	Descripción	Especificación Técnica	Observaciones
1	Dirección IP	172.22.0.x, perteneciente a la clase B, donde x es el número que se incrementa en 1 cada vez que se asigna una nueva dirección IP.	Esta asignación se la realizo de acuerdo a la nueva clasificación de IP tabla 3.2.
2	Gateway o puerta de enlace	La puerta de enlace asignada es la dirección IP: 172.22.0.1	La dirección IP asignada es la del servidor proxy, mediante el cual los usuarios de la Epsa podrán acceder al servicio de internet.
3	DNS	DNS Preferido: 200.87.100.10 DNS alterno: 172.22.0.1	La IP asignada para el DNS preferido es la dirección IP del proveedor de servicio de Internet y el DNS alterno es la dirección IP del servidor principal.

Tabla 10 Criterios de la configuración del protocolo TCP/IP
Fuente: Elaboración Propia

3.2.2. Políticas y procedimientos relacionados

Esta actividad de acuerdo a la metodología utilizada permite la incorporación de políticas particulares como son: procedimientos de instalación de aplicaciones más utilizadas, políticas de respaldo de configuraciones, etc.

La División de Redes de datos y Servicio de Internet de la Epsa no contaba con políticas y procedimientos relacionados al uso y manejo de la red de datos y del servicio de internet, debido a esta dificultad se vio por conveniente trabajar en este sentido cuyo resultado se detalla en seguida.

3.2.3. Políticas de uso de la red de datos e internet

Las políticas de uso de la red y el servicio de internet fueron presentados a las Jefatura de la Epsa con la revisión de la Unidad de Sistema del Municipio de Cobija para que a partir de esa instancia se corrija y/o modifique si se tienen algunos errores y/o fallas y luego ser presentado a instancias superiores para su posterior aprobación. Porque no hay que olvidar que serán aplicados para todos los usuarios de la EPSA COBIJA y tiene que ser abalados por las máximas instancias y autoridades superiores, ver las Políticas de uso de la red de datos ir (ANEXO K).

3.3. ADMINISTRACIÓN DEL RENDIMIENTO

La administración de la red de datos e internet se realizó en dos fases porque se vio la necesidad de recolectar y analizar el tráfico que circula por la red de datos en un momento en particular y en un intervalo de tiempo. Esto permitió tomar decisiones pertinentes de acuerdo al comportamiento encontrado. La administración del rendimiento se dividió en dos etapas:

3.3.1. Monitoreo

El monitoreo de la red de datos de la EPSA COBIJA realiza el **contro**l del servicio de Internet que provee la cooperativa Coteco (con un ancho de banda de 128 kbps), servicio que desde el mes de Enero es suministrada por un proveedor particular (con un ancho de banda de 1024 kbps). El Monitoreo también controla la red de datos interna, con el fin de efectuar un seguimiento del servicio de Internet.

Este control y monitoreo se dividió en tres procesos:

a) Monitoreo del servicio de Internet (Red Externa)

El Proceso de Monitoreo del servicio de Internet, se realizó bajo un plan de actividades para el testeo del ancho de banda. El plan se divide en dos partes:

1ª PARTE: Monitoreo del ancho de banda sin usuarios

1. Se desconectan físicamente todos los equipos de la red de datos y del servicio de internet de la Epsa.
2. Se conecta un equipo (libre de virus) directamente al conmutador (switch) principal, el cual recibe la señal de internet por medio de una mini estación repetidora (Nano Station).

3. Las herramientas que se utilizan para la verificación del ancho de banda, están disponibles de forma gratuita en las siguientes direcciones web.

http://www.testdevelocidad.es/

Ilustración 25 Pantalla principal de la aplicación ubicada en http://www.speedtest.com probando la velocidad de transferencia sin usuarios
Fuente: Elaboración propia

También se elaboró un cronograma de hora y fecha para realizar el testeo del ancho de banda en del Segundo periodo de la gestión 2018 para más detalle ver en la Tabla siguiente.

NRO.	FECHA	HORA
1	9 / Julio / 2018	11:30 am
2	10 / Julio / 2018	9:00 am
3	11 / Julio / 2018	10:00 am
4	23 / Julio / 2018	9:30 am
5	27/ Julio / 2018	16:10 pm
6	11 / Agosto / 2018	17:30 pm
7	13 / Agosto / 2018	18:30 pm
8	15 / Agosto / 2018	9:30 am
9	16/ Agosto / 2018	10:30 am
10	20/ Agosto / 2018	10:00 am
11	31 / Agosto / 2018	18:00 pm
12	04 / Septiembre /2018	10:15 am
13	14/ Septiembre /2018	17:20 pm
14	17 / Septiembre /2018	10:00 am

Tabla 11 Cronograma de fecha y hora para la medición del ancho de banda
Fuente: Elaboración Propia

Como resultado de la primera parte de la medición del ancho de banda, se observa los siguientes datos en las diferentes fechas y horas del Segundo periodo de la gestión 2018, para más detalle ver la Tabla siguiente.

MES	FECHA	HORA	RESULTADOS
Julio	09/07/2018	11:30 AM	92 Kbps
	09/07/2018	11:30 AM	84 Kbps
	10/07/2018	9:00 AM	118 Kbps
	10/07/2018	9:00 AM	98 Kbps
	11/07/2018	10:00 AM	122 Kbps
	23/07/2018	9:30 AM	78 Kbps
	27/07/2018	16:10 PM	114 Kbps
		Promedio	**101 Kbps.**
Agosto	11/08/2018	8:30 AM	112 Kbps
	11/08/2018	8:35 AM	104 Kbps
	11/08/2018	9:40 AM	93 Kbps
	11/08/2018	11:30 AM	75 Kbps
	11/08/2018	16:00 PM	72 Kbps
	11/08/2018	17:30 PM	87 Kbps
		Promedio	**90,5 Kbps.**
Agosto	13/08/2018	9:30 AM	98 Kbps
	13/08/2018	18:30 PM	92 Kbps
		Promedio	**95 Kbps.**
MES	**FECHA**	**HORA**	**RESULTADOS**
Agosto	15/08/2018	08:30 AM	114 Kbps
	15/08/2018	09:30 AM	86 Kbps
	15/08/2018	16:30 PM	78 Kbps
	15/08/2018	16:35 PM	81 Kbps
		Promedio	**89,75 Kbps.**
Agosto	16/08/2018	10:00 AM	104 Kbps
	16/08/2018	10:30 AM	96 kbps
	16/08/2018	10:50AM	78 Kbps
	16/08/2018	11:30 AM	84 Kbps

		Promedio	**90,5 Kbps.**
Agosto	31/08/2018	18:00 PM	73 Kbps
	31/08/2018	18:10 PM	89 Kbps
	31/08/2018	18:13 PM	77 Kbps
		Promedio	**79,6 Kbps.**
Septiembre	04/09/2018	10:15 AM	884 Kbps
	04/09/2018	15:30 PM	969 Kbps
	04/09/2018	15:50 PM	1114 Kbps
		Promedio	**989 Kbps.**
Septiembre	14/09/2018	17:20 PM	860 Kbps
	14/09/2018	17:22 Pm	1112 Kbps
	14/09/2018	17:30 Pm	993 Kbps
	14/09/2018	17.35 Pm	774 Kbps
		Promedio	**934,75 Kbps.**
Septiembre	17/09/2018	10:00 Am	866 Kbps
	17/09/2018	11:30 Am	879 Kbps
	17/09/2018	11:50 Am	882 Kbps
		Promedio	**875,66 Kbps.**

Tabla 12 Resultados del testeo del ancho de banda, II/2018
Fuente: Elaboración Propia

2ª PARTE : Monitoreo del ancho de banda con usuarios

1. Se conectan todos los equipos (libres de virus) a la Red de datos al tiempo que usan el servicio de Internet de la EPSA.
2. Se tendrá un equipo de computación principalmente para realizar el testeo del ancho de banda, el cual deberá estar libre de virus.
3. Las herramientas a utilizar para la verificación del ancho de banda serán las siguientes direcciones web, que se encuentran disponibles gratuitamente en el servicio de Internet:

http://www.testdevelocidad.es/

http://www.speedtest.com

http://www.internauta.com

Ilustración 26 Pantalla principal de la aplicación ubicada en http://www.testdevelocidad.es
Fuente: Elaboración Propia

También se elaboró un cronograma de hora y fecha para realizar el testeo del ancho de banda con usuario, para el Segundo periodo de la gestión 2018. Detalles en la Tabla siguiente.

NRO.	FECHA	HORA
1	12 / Julio/ 2018	10:00 am
2	16 / Julio/ 2018	15:30 pm
3	24/ Julio/ 2018	11:00 am
4	15 / Agosto/ 2018	10:00 am
5	27 / Agosto/ 2018	17:00 pm
6	30 / Agosto / 2018	18:30 pm
7	04/Septiembre/2018	09:00 am
8	07/Septiembre/2018	16:00 pm
9	11/Septiembre/2018	17:43 pm

Tabla 13 Cronograma de medición del ancho de banda
Fuente: Elaboración Propia

Como resultado de la segunda parte de la medición del ancho de banda (Segundo periodo de la gestión 2018) se tiene la Tabla siguiente.

MES	FECHA	HORA	RESULTADOS
Julio	12/07/2018	10:00 AM	19 Kbps
	12/07/2018	10:05 AM	31.10 Kbps
	12/07/2018	10:12 AM	32 Kbps
		Promedio	**27,36 Kbps.**
Julio	16/07/2018	15:30 Pm	38 Kbps
	16/07/2018	15:40 Pm	38:40 Kbps
		Promedio	**38,2 Kbps.**
Julio	24/07/2018	11:00 AM	94 Kbps
	24/07/2018	11:05 AM	72 Kbps
	24/07/2018	11:11 AM	78,08 Kbps
	24/07/2018	11:16 AM	89,60 Kbps
		Promedio	**83,42 Kbps**
Agosto	15/08/2018	10:00 AM	117 Kbps
	15/08/2018	11:30 AM	64,40 Kbps
MES	**FECHA**	**HORA**	**RESULTADOS**
	15/08/2018	17:13 PM	70,32 Kbps
		Promedio	**83,77 Kbps.**
Agosto	27/08/2018	8:30 AM	81 Kbps
	27/08/2018	8:36 AM	33 Kbps
	27/08/2018	17:00 PM	25 Kbps
	30/08/2018	10:05 AM	30 Kbps
	30/08/2018	10:20 AM	51,04 Kbps
	30/08/2018	18:30 PM	40,60 Kbps
		Promedio	**43,44 Kbps.**
Septiembre	04/09/2018	09.00 AM	662 Kbps
	04/09/2018	16:20 PM	514 Kbps

	04/09/2018	16:25 PM	482 Kbps
		Promedio	**552.66 Kbps.**
Septiembre	07/09/2018	10:00 AM	673 Kbps
	07/09/2018	16:00 PM	567 Kbps
	11/09/2018	9:41 AM	643 Kbps
	11/09/2018	17:43 PM	586 Kbps
		Promedio	**617,25 Kbps.**

Tabla 14 Resultado del testeo del ancho de banda con usuario, Segundo periodo de la gestión 2018
Fuente: Elaboración Propia

3.3.2. Análisis

El análisis de los datos se realiza una vez recolectada la información del proceso de monitoreo, este análisis ayuda a determinar el comportamiento del uso del servicio de Internet para la toma de decisiones. El análisis se divide de acuerdo a las etapas del monitoreo.

a) Análisis del servicio de Internet (Red Externa)

El proceso de análisis de la información realizada en la actividad del monitoreo del servicio de Internet. El análisis se divide en dos partes.

1º PARTE : Análisis del ancho de banda sin usuarios

El análisis del ancho de banda real, se realizó obteniendo el promedio total en cuento a los resultados del monitoreo de la 1º parte, que se describió en el anterior tabla, promedio mensual del primer periodo de la gestión 2018, para más detalle ver la figura siguiente.

MES	RESULTADO ANCHO DE BANDA
Julio	101 Kbps
Agosto	89,07 Kbps
Septiembre	933,14 Kbps

Tabla 15 Resultado Ancho de Banda Parte 1°
Fuente: Elaboración Propia

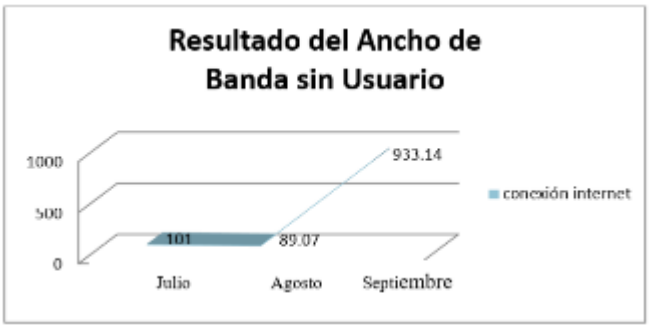


Ilustración 27 Resultados del Ancho de banda sin usuarios
Fuente: Elaboración Propia

Como se observa en la figura 34, de acuerdo al análisis de los resultados obtenidos del monitoreo del ancho de banda real, se obtiene las siguientes conclusiones:

1. Durante los meses de julio y agosto el ancho banda del servicio de internet. es buena, porque se mantiene arriba del 60%. de lo contratado. El proveedor se mantiene al margen del monitoreo del servicio que suministra a la red de datos de la Epsa.

2º PARTE: Análisis del ancho de banda con usuarios

El análisis de los resultados del monitoreo del ancho de banda real, se realizó obteniendo el promedio total de los resultados de la segunda parte, que se describió en la anterior tabla, Promedio total de cada mes del segundo periodo de la gestión 2018, para más detalle ver la figura siguiente.

MES	RESULTADO ANCHO DE BANDA
Julio	49,66 Kbps
Agosto	63,61 Kbps
Septiembre	584,96 Kbps

Tabla 16 Resultado Ancho de Banda Parte 2°
Fuente: Elaboración Propia

Ilustración 28 Resultados del Ancho de banda con usuarios
Fuente: Elaboración Propia

Como se observa en la Figura Nº 35, de acuerdo al análisis de los resultados obtenidos del monitoreo del ancho de banda real, que nos proveen la Empresa del servicio de internet se obtiene las siguientes conclusiones:

- Durante el mes de julio, el ancho banda que nos provee la empresa del servicio de internet disminuye, cuando todos los usuarios se encuentran conectados a la red de datos interna de la Epsa, causando que el servicio de internet se vuelva insuficiente para todos los usuarios de la red de datos.
- Durante los meses de agosto y septiembre el ancho de banda aumenta llegando a ofrecer un buen servicio de internet para la red de datos de la Epsa.

Conclusión del análisis del ancho de banda

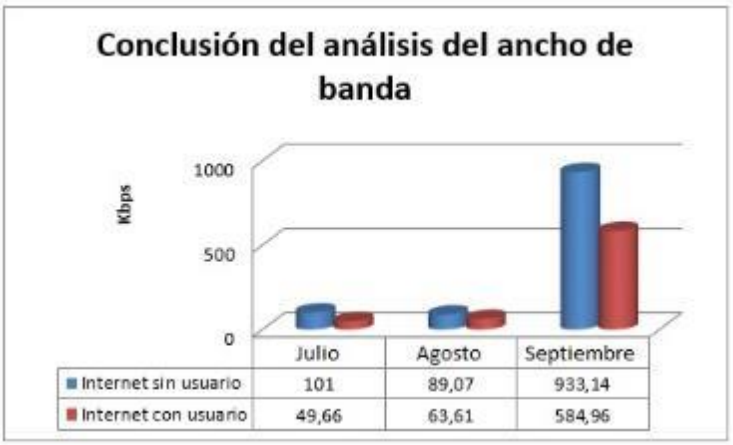


Ilustración 29 Conclusión de los Resultados del ancho de banda
Fuente: Elaboración Propia

De acuerdo al análisis de los resultados obtenido del monitoreo, podemos observar que los resultados son totalmente diferentes para ambas partes, por lo cual se llega a las siguientes conclusiones:

- Insuficiente ancho de banda asignado a la red de la EPSA COBIJA en el mes julio y agosto.
- El mes de septiembre mejoro el servicio de internet con la incorporación de un nuevo proveedor.

3.4. ADMINISTRACIÓN DE FALLAS

La administración de fallas también llamada asistencia técnica para el Desarrollo del Proyecto de Grado (Administración de la Red de Datos y el Servicio de Internet) fue una actividad constante en todo el segundo periodo de la gestión 2018 tal como se mostró en la primera parte del presente capitulo. Esta actividad se la clasifico en tres partes las cuales son: Asistencia técnica con relación a la red de datos, asistencia técnica con relación al servicio de internet y asistencia técnica con relación con otros aspectos.

3.4.1. Asistencia técnica por fallas de red.

Existen un sin fin de problemas causados por la falla de conexión de la computadora con la red de datos de los cuales a continuación mencionamos los más frecuentes ocurridos en el transcurso de la implementación del proyecto de grado son detallados en los acápites 3.8.2 y 3.8.3.

3.4.2. Configuración de la dirección IP

Este trabajo se realizó cada vez que el usuario lo requería y simplemente se configuraba su protocolo TCP/IP asignándole una dirección IP para poder identificar a cada uno de los equipos informáticos (computadoras) de los usuarios.

La configuración se realiza de la siguiente forma:

- Entrar a mi centro de red y recursos compartidos escoger cambiar la configuración de mi adaptador.
- Escoge tu adaptador de red que utilizas y hacer clic derecho escoger propiedades
- Elegir Protocolo de Internet versión 4(TCP/IPv4) y el botón propiedades

- Elegir Usar la siguiente dirección IP y se va habilitar los demás campos a llenar.

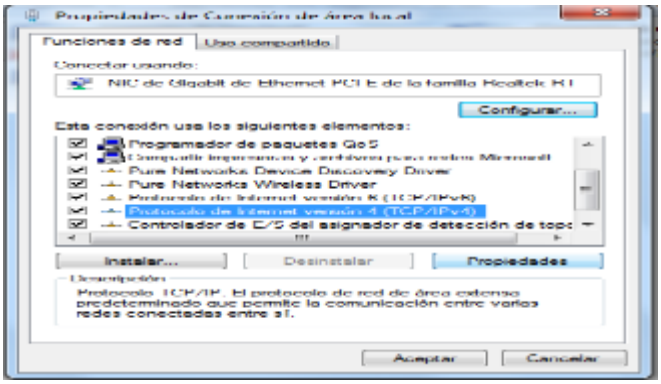


Ilustración 30 Propiedades de conexión de área local
Fuente: Elaboración propia

3.4.3. Asistencia técnica de conexión a la red

Las causas para este tipo de fallas se las clasifico en tres grupos:

a. Tarjeta de red mal acomodada

Este es un problema típico cuando se mueve la unidad central de procesamiento (Case) de posición y además el Case sufre algún golpe. De alguna forma el movimiento y el golpe hacen que la tarjeta de red sufra movimientos, cuando la tarjeta de red sufre el más mínimo movimiento hace que pierda la conexión entre sócalo de la placa madre y la peineta de la tarjeta de red y no exista la conexión física, suficiente motivo por el cual pierda la conexión con la red de datos.

Una forma de comprobar que existe una conexión física es observando el led que viene incorporada en la tarjeta de red, este led tiene que estar encendida con eso nos garantiza que hay la respectiva conexión. En caso que este apagado el led ya se encontró el problema buscado.

b. Eliminación de archivos de configuración de la red.

Este problema es muy frecuente cuando un virus ataca a la computadora, el antivirus instalado detecta al virus y enseguida elimina los archivos contagiados y en algunos casos dentro de los archivos contagiados están inmersos los archivos que se instalan juntamente con el controlador de red, generalmente los archivos dll.

Para dar solución al problema se procede a reinstalar le controlar de la tarjeta de red

Y configurar las propiedades de la mencionada anteriormente.

c. Adición de puntos de red

La adición de nuevos puntos fue una actividad muy importante debido que mediante esta se amplió la red de datos de la Epsa Municipal Cobija.

Todos los equipos de computación que no tenían una conexión a la red de datos se les

adiciono un punto de red para que pueda disfrutar las ventajas de estar conectado a la red de datos.

3.4.4. Asistencia técnica por fallas de internet.

Existen un sin fin de problemas causados por falla del servicio de internet las cuales son detallados en los acápites 3.4.5.

3.4.5. Asistencia técnica del servicio de internet

a. Usuario y contraseña mal escrita.

Este tipo de error es común cuando digitan de forma herrada su usuario o la contraseña no van a poder acceder a internet, a continuación, se muestra en la figura siguiente cuando digita mal su usuario o la contraseña.

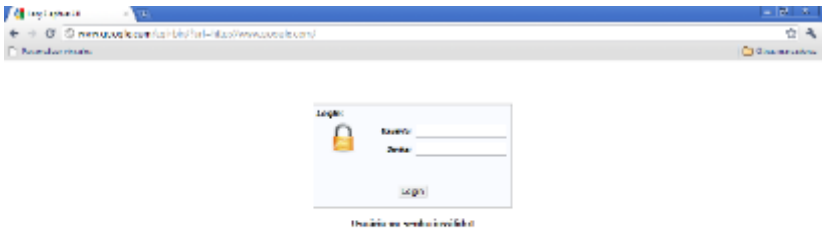


Ilustración 31 Usuario o contraseña mal digitadaFuente: Elaboración Propia
Fuente: Elaboración propia

3.4.6. Fallas con relación a otros aspectos

Aparte de las fallas ocurridas por la red de datos y el servicio de internet también existen otros más los cuales son detallados en los acápites 3.4.7 y 3.4.8.

3.4.7. Instalación del sistema operativo Windows, office, antivirus, otros.

Este problema es causado cuando el usuario formatea su disco duro y solicita la asistencia técnica al Administrador de la División de la Red de datos y Servicio de Internet para la solución de esta falla.

3.4.8. Asistencia técnica por contaminación de virus.

Este trabajo fue constante cuando las computadoras eran contagiadas con virus, la solución del problema fue inmediata utilizando distintos tipos de antivirus como son Eset Nod 32 y Avast free. Cada uno de estos detectaba distintos tipos de virus.

Otra forma de combatir los virus fue formateando las computadoras realizando una previa copia de información (backup), e instalando el software indispensable para el funcionamiento de la computadora.

Este trabajo se desarrolló a lo largo de la Administración de la red de datos e internet y se utilizó software antivirus como herramienta, en algunos casos se tuvo que formatear el disco duro de la computadora por el motivo que los discos duros en su totalidad estaban infectados.

3.5. ADMINISTRACIÓN DE LA SEGURIDAD

La seguridad en redes de datos debe ser vista como un sistema completo, por lo tanto, se debe hablar de toda su infraestructura. En redes datos existen diversas vulnerabilidades, desde el software que utiliza, la arquitectura sobre la cual se trabaja y el manejo de los diferentes dispositivos y servicios.

En ese contexto se aplicaron medidas de seguridad desde el rediseño de la red hasta su implementación con el objetivo de ofrecer servicios de seguridad a cada uno de sus elementos, creando estrategias para la prevención y detección de ataques, así como para dar respuesta ante cualquier incidente de seguridad.

3.5.1. Prevención de ataques

El procedimiento que se siguió para mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos consistió en la implementación de algunas estrategias de control de accesos para ello se realizaron tres etapas: Identificación de los protocolos, Identificación de las tecnologías y establecimiento de la medida de seguridad. Estas estrategias nos ayudaron a reducir los ataques.

- **Identificación de los protocolos utilizados.**

El primer paso es seleccionar los protocolos utilizados. En la siguiente tabla siguiente se detallan los protocolos utilizados para la transmisión de datos a la que se le implementó la seguridad.

En esta tabla se listan los protocolos utilizado en la red implementada, en la primera columna se encuentran cuatro capas del modelo OSI sobre la cual se trabajó, y la segunda columna los protocolos de comunicación utilizados por la capa correspondiente.

Capa OSI	Protocolo utilizado
Aplicación	HTTP, SSH, DNS, DHCP
Transporte	RTP, UDP, TCP
Red	IP, ARP, ICMP

Tabla 17 Protocolos utilizados
Fuente: Elaboración propia

- **Identificación de las tecnologías utilizadas.**

A continuación, en la tabla siguiente se describen las tecnologías utilizadas en la red de datos donde se aplicará las medidas de seguridad. En la primera columna, se describen los componentes de la red de datos a los cuales corresponde cada dispositivo y en la segunda, se señala la versión del software instalado.

Dispositivos	Versión
Computador de escritorio	Windows 7 Ultimate Windows 8 pro
Impresora	HP desjeck
Servidor de seguridad	Endian Firewall

Tabla 18 Tecnología utilizada
Fuente: Elaboración propia

- **Establecimientos de medidas de seguridad para la prevención ante cualquier ataque.**

A continuación, se describe como fueron implementadas las medidas de seguridad capa por capa del modelo OSI.

a) Capa De Aplicación

El primer paso, para esta capa, es realizar proceso de asegurar un sistema mediante la reducción de vulnerabilidades a todos los dispositivos utilizados en la red. A continuación, se listan los pasos aplicados para el aseguramiento de estos dispositivos.

1. Instalar la última versión y luego realizar una actualización.

Se revisó la versión del sistema operativo, firmware y el software de las aplicaciones utilizadas. Esto varió dependiendo del componente que se esté revisando y actualizando.

Dispositivo	Últimas versiones 20/05/2019	Como actualizar
Computador de escritorio	Microsoft Windows 7, 8 y 10	https://www.microsoft.com/es-es/download Windows Update y el gestor de actualizaciones de Windows
Impresora	Firewall	Actualización del firewall

Tabla 19 Actualizando la tecnología utilizada
Fuente: Elaboración propia

En la tabla anterior se pueden observar las últimas versiones de los dispositivos utilizados y como se puede actualizar. Las actualizaciones se pueden realizar a través de descargas actualizadas, para ese efecto, se agregó el link de descarga.

2. Proteger archivos de sistema. La mayor parte del malware, en la red, modifica archivos de sistema. Esto les permite acceso a muchas funcionalidades del computador de la víctima. Es por esto que, los archivos claves de configuración del sistema, debiesen contar con permisos acotados de lectura y escritura.

3. Establecer cuentas de usuarios a cada equipo y bridar permisos necesarios. Solo el administrador debe tener acceso a la configuración del sistema, no debiesen existir otros usuarios con acceso. Sin embargo, es común que más de una persona tenga acceso a la configuración del sistema. Es por esto que se deben establecer diferentes cuentas de usuarios y brindar los permisos correspondientes en caso que sea necesario.

4. Cerrar todos los puertos no utilizados. Los puertos que no sean utilizados deben ser cerrados, debido a que, mientras más puertos abiertos haya, más posibilidades hay de un ataque.

5. Restringir el acceso a la interfaz web y SSH a todos los servidores.

6. Para las aplicaciones de acceso remoto, establecer contraseñas y limitar errores de su ingreso, para evitar el uso de herramientas de ataques.

El segundo paso realizado, para la capa de aplicación, es la configuración y actualización de la herramienta de seguridad. Este paso, está enfocado en resguardar los equipos de computación perteneciente a la red de datos y se realizó bajo la solución de seguridad ESET Security

Management Center en su versión Dynamic Endpoint Protection. Esta aplicación incluye todas las tecnologías necesarias para proteger a clientes frente a cualquier amenaza y suministra una visión general en tiempo real de todas las endpoints locales y externas desde una consola de nivel corporativo. Le ofrece informes completos y administración de la seguridad para todos los sistemas operativos, gestiona eficientemente los parches que evita que las vulnerabilidades de los programas instalados que se conviertan en la puerta de entrada. Esta herramienta es importante para la seguridad ya que el 99% de las terminales funcionan sobre sistema operativo Windows y a la hora de instalar un software en un computador se impedirá parcialmente la contaminación de este terminal con malware.

b) Capa De Red

En la capa de red, se establecieron las zonas. La primera zona es la naranja que corresponde al enlace de la zona desmilitarizada (conocida también como DMZ, sigla en inglés de *Demilitarized Zone*), esta zona no se encuentra expuesta a Internet. La segunda zona es la red interna. En la institución se cuenta con dos servidores que prestan servicios de facturación electrónica y gestión de documentación y hojas de rutas que son catalogados como servidores críticos y son ubicados detrás del firewall de Red, la tercera zona es la Roja que nos provee servicio de internet, En el (ANEXO L) se detalla la configuración realizada para la seguridad en la capa de red.

3.6. DETECCIÓN DE INTRUSOS

En esta fase se procedió a configurar el módulo Sistema de Prevención de Intrusos en Endian Firewall, debido a que se dispone de este servicio en el servidor de protección y seguridad, además se procedió a activar otra característica como el de mantener el historial del host se muestra en la Figura siguiente, para luego acceder a las gráficas que nos proporciona esta herramienta sobre el análisis y registro del tráfico que circula en la red que indican el momento en que se detecte una situación anormal.

A continuación, se puede observar los pasos realizado para la configuración del sistema de prevención de intrusos.

- **Activación del módulo sistema de prevención de intruso**

Dentro de la interfaz web de Endian nos dirigimos a la pestaña de Servicios luego seleccionamos Prevención de Intrusos y habilitamos el modulo como se puede observar en la siguiente figura.

Ilustración 32 Activación del módulo sistema de prevención de intruso
Fuente: elaboración propia

- **Creación de Reglas**

En este paso se procedió a realizar la activación de las reglas que viene implementadas en esta herramienta de seguridad, y luego aplicamos la configuración como se muestra en las figuras siguientes.

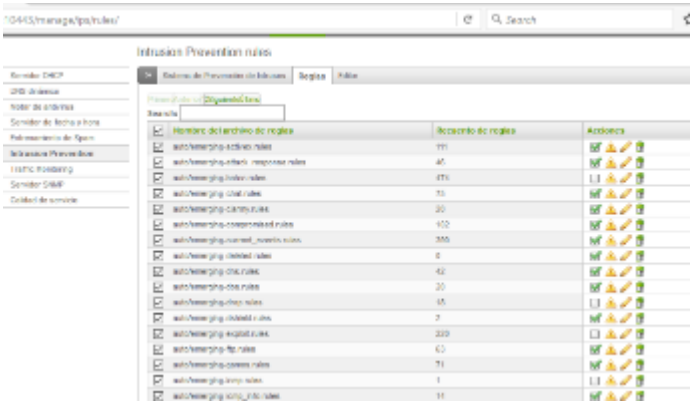


Ilustración 33 Creación y configuración de Reglas de Snort
Fuente: elaboración propia

Ilustración 34 Aplicar configuración
Fuente: elaboración propia

- **Activar característica para mantener el historial del host.**

En este paso se procedió a configurar el módulo Analizador de tráfico de Red que se encuentra en la pestaña Servicios opción *Traffic Monitoring*.

A continuación, en las figuras siguientes se puede observar la configuración realizada.

Ilustración 35 opción1 Traffic Monitoring
Fuente: elaboración propia

Ilustración 36 opción2 Traffic Monitoring
Fuente: elaboración propia

Esta herramienta permite visualizar el tráfico que circula en la red, así como también ver las mediciones técnicas de acceso a todo el sistema de prevención de intruso. Una vez realizado todos estos procedimientos, se accedió al servidor mediante un navegador web al módulo Estado en su menú gráfico del tráfico, donde puede obtener una gráfica que detalla la evolución del tráfico a lo largo del tiempo en día, semanas, mes y año.

Ilustración 37 tráfico que circula en la red
Fuente: elaboración propia

3.7. RESPUESTA A INCIDENTES

El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en la red de datos, cuando éste hay sido detectado, para este caso se creó un formulario para la forma de manejo de incidentes.

3.8. POLÍTICAS DE SEGURIDAD

La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de red y la información ahí contenida. Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. En este contexto se elaboró las políticas de seguridad previo análisis de las necesidades en la red de datos de la EPSA COBIJA.

A continuación, se detallan las políticas de seguridad elaboradas e implementadas:

3.8.1. Políticas de uso aceptable

El objetivo de esta política es de especificar o dar a conocer los actos prohibidos en la red de datos de la EPSA COBIJA a sus usuarios de Internet, entendiéndose por usuarios los "clientes o cualquiera que utilice el servicio de Internet o acceda a ellos por medio de la red interna de la institución". La EPSA podrá realizar modificaciones a esta política en cualquier momento si lo estima procedente, y publicar dichas modificaciones, en cuyo caso las mismas entrará a regir a partir de su publicación. El usuario será responsable de mantenerse actualizado de tales modificaciones una vez hayan sido publicadas.

- El Usuario que acceda al servicio de Internet a través de la red de datos debe hacerlo lícitamente. El usuario no podrá introducir modificaciones a los equipos, ni conectar elementos adicionales a los especificados por el personal autorizado al momento de la instalación.
- El servicio de Internet de la EPSA COBIJA solo podrá utilizarse únicamente para fines institucionales, quedando prohibida la transmisión, distribución o almacenamiento de materiales para beneficio propio o de terceros.
- Los usuarios que atenten contra la seguridad de sistemas o redes podrán incurrir en responsabilidad penal y civil. El área de Informática cooperará plenamente en la

investigación de cualquier presunto delito o violación de la seguridad de sistemas o redes, bajo la dirección de las autoridades competentes.

3.8.2. Políticas de cuentas de usuario

Los usuarios son responsables de seguir las políticas de seguridad y procedimientos para su uso de los servicios de la red de datos e Internet y abstenerse de cualquier práctica que podría poner en peligro los sistemas de cómputo, la información o los datos de la EPSA COBIJA.

- Se crea una cuenta temporal del usuario, en caso de olvido o extravió de información de la cuenta personal, para brindarse al usuario que lo necesite, siempre y cuando se muestre un documento de identidad personal.
- El usuario al ser contratado como empleado de la EPSA COBIJA, se le asigna una cuenta de usuario personal a su equipo de computación para que así se le haga la entrega de la documentación necesaria para cubrir todas las necesidades inherentes a su cargo.
- El no cumplimiento de las disposiciones de seguridad y responsabilidad sobre sus acciones por parte de los usuarios de la red interna de la institución, se obliga a la suspensión de su cuenta de usuario de los servicios.
- El registro del equipo de computación se lo administra mediante su dirección MAC con el Endian Firewall.

3.8.3. Políticas de listas de acceso

- Se prohíbe estrictamente el acceso a páginas web como www.youtube.com y www.xxx.com.
- Queda determinadamente prohibido el acceso a redes sociales durante el horario laboral.
- No descargar música, películas y videos.

3.8.4. Políticas de acceso remoto.

El acceso remoto es la conexión a distancia entre dos o más equipos, donde uno de ellos permite acceder al otro como si se estuviese trabajando directamente en frente uno del otro, por lo cual se recomienda que cuando se requiera acceder remotamente a los ordenadores de la EPSA

COBIJA, se deberán utilizar conexiones seguras como TeamViewer y así evitar servicios tales como, Telnet, ftp y otros que se sabe son de alto riesgo

- Se Usa TeamViewer solo cuando sea necesario y no dejarlo en funcionamiento si no se usa.
- No se debe guardar autorizaciones de conexión ni pasarlas a otros en forma descodificada.
- Se debe informar inmediatamente al departamento de seguridad informática si se sospecha de un ciberataque.

3.8.5. Políticas de contraseñas.

La contraseña o clave de un usuario es el mecanismo que se utiliza para autenticar en todos los sistemas informáticos, la calidad de la contraseña es un factor importante a ser considerado. Si las contraseñas pueden adivinarse o robarse, alguien ingresando con su usuario puede causar problemas a la institución o sus recursos. Por ello, la contraseña es de uso personal e individual, no debe ser compartida con otras personas y debe ser mantenida en forma segura.

- La longitud mínima de caracteres permisibles en una contraseña se establece en 6 caracteres, los cuales tendrán una combinación alfanumérica, incluida en estos caracteres especiales.
- La longitud máxima de caracteres permisibles en una contraseña se establece en 12 caracteres, siendo esta una combinación de Mayúsculas y minúsculas.

3.8.6. Políticas de respaldos.

Las políticas de Backups de la EPSA Municipal Cobija. Describe que los datos de informaciones de importancia se resguardan mediante el personal autorizado a operar los backups y restauraciones, los datos a resguardar, el momento en que se ejecutan lo backups, el manejo de los datos almacenados, y las responsabilidades de los operadores y demás personas involucradas.

- Se realiza respaldos de la información, diariamente, para los sistemas de mayor importancia o críticos, un respaldo semanal que se utilizará en caso de fallas y un tercer respaldo efectuado semestralmente, el cual debe ser guardado y evitar su utilización a menos que sea estrictamente necesaria.
- El área de Informática tiene la obligación de efectuar un respaldo de los archivos de registro o logs, fuera de los dispositivos que les creen.
- Los archivos de logs deben ser respaldados en tiempo real, sus nombres deben contener la hora y la fecha en la que fueron creados sus originales.

CAPÍTULO IV

4. CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

Como resultado del desarrollo del Proyecto de Grado, se ha llegado a las siguientes conclusiones.

- Se diagnosticó la seguridad de la red de datos identificando las necesidades de la Empresa Municipal de Agua Potable y Alcantarillado Sanitario de Cobija.
- Se reestructuró el cableado de acuerdo al nuevo diseño de la red de datos para su buen funcionamiento.
- Se implementó un servidor proxy para la administración de la seguridad de la red de datos y del servicio de Internet logrando mejorar con la contratación de 10 megas más de ancho de banda de Internet.
- Se elaboró la propuesta de las políticas de uso de la seguridad de red de datos e Internet de la EPSA COBIJA. Presentándolo Asesoría Legal para su aprobación.

4.2. RECOMENDACIONES

Concluido el presente Proyecto de Grado, se pone en consideración las siguientes recomendaciones:

- Realizar la implementación de un Servidor de Dominio de Red (PDC) para tener más control de los usuarios.
- Investigar e implementar herramientas para la automatización de reportes del tráfico y consumo de la Red de Datos e Internet de la EPSA COBIJA.
- Investigar e implementar herramientas de monitorización del tráfico de la Red de datos.
- Investigar e implementar seguridad física en la Red de datos de la EPSA COBIJA.

4.3. REFERENCIAS

Bibliografía

Andrew S. Tanenbaum y David J. Wethersll. (2012). *Redes de Computadoras.* Mexico: Pearson Educacion.

Cifuentes, R. J. (2017). *DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD EN REDES DECOMUNICACIÓN INALÁMBRICAS APLICADO A PEQUEÑAS EMPRESAS DEL SECTOR PRIVADO DE LA CIUDAD BOGOTÁ.* BOGOTÁ D.C: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Obtenido de http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAS2281.pdf

Estrada, A. C. (2016). *Seguridad en Redes.* Madrid, España: Darfe Learning Consulting.

José María Barceló Ordinas, Jordi Íñigo Griera, Ramón Martí Escalé, Enric Peig Olivé y Xavier Perramon Tornil. (2004). *Redes de Computadores.* Barcelona España: UOC Formacion de Posgrado.

Nicolás Álvarez S. Juan Monsalve Z. (1 de marzo de 2008). *Introducción a las Redes de Computadores*. Obtenido de http://www2.elo.utfsm.cl: http://www2.elo.utfsm.cl

SRL, E. (8 de Abril de 2019). *http://www.endian.com/Endian%20Firewall%20-%20Wikipedia,%20la%20enciclopedia%20libre.html*. Obtenido de http://www.endian.com

Stallings, W. (2004). *Comunicaciones y redes de computadores.* España: Grupo Anaya Publicaciones Generales.