



UNIVERSIDAD DE MARGARITA
SUBSISTEMA DE DOCENCIA
DECANATO DE INGENIERÍA Y AFINES
COORDINACIÓN DE INVESTIGACIÓN Y PASANTÍA

**DISEÑO DE RED DE ÁREA LOCAL ALÁMBRICA PARA LA OPTIMIZACIÓN DE
LA CONECTIVIDAD Y LA SEGURIDAD DE DATOS MEDIANTE UN
SERVIDORPROXY EN LA CONTRALORÍA DEL
MUNICIPIO ANTOLÍN DEL CAMPO**

Elaborado por:

David Moro Tineo

Danyelis Paz Castillo

Tutor: Ing. Hiram González Gómez

El Valle del Espíritu Santo, noviembre de 2022

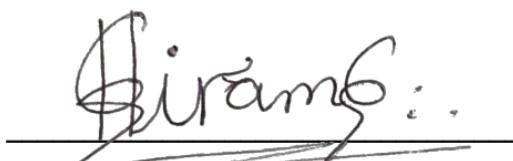


UNIVERSIDAD DE MARGARITA
SUBSISTEMA DE DOCENCIA
DECANATO DE INGENIERÍA Y AFINES
COORDINACIÓN DE INVESTIGACIÓN

CARTA DE APROBACIÓN DEL TUTOR

En mi carácter de Tutor del Trabajo de Investigación presentado por los ciudadanos **DANYELIS DEL VALLE PAZ CASTILLO OSIO** y **DAVID AUGUSTO MORO TINEO**, cedulados con los números: V.- 29.582.122 y V.- 28.189.215 respectivamente, para optar al Grado de *Ingeniero de Sistemas*, considero que dicho trabajo: **DISEÑO DE RED DE ÁREA LOCAL ALÁMBRICA PARA LA OPTIMIZACIÓN DE LA CONECTIVIDAD Y LA SEGURIDAD DE DATOS MEDIANTE UN SERVIDOR PROXY EN LA CONTRALORÍA DEL MUNICIPIO ANTOLÍN DEL CAMPO** reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Jurado Examinador que se designe.

Atentamente



Ing. Hiram González Gómez

TUTOR

El Valle del Espíritu Santo, noviembre de 2022

DEDICATORIA

Queremos dedicar este trabajo de investigación a nuestros padres, quienes nos han acompañado durante nuestro trayecto universitario brindándonos su apoyo incondicional en todo momento; quienes además nos han inculcado que nunca debemos rendirnos para cumplir nuestros objetivos. Sin su apoyo y sacrificio, no hubiésemos logrado llegar al final de la meta.

AGRADECIMIENTOS

A nuestros padres Alfonso Moro y Zoelys Tineo y, Jaime Paz Castillo y Gloria Osío, por ser parte fundamental en el desarrollo del presente trabajo. Igualmente, hacemos mención al señor Franklin Britos, por financiar la carrera de David.

A nuestros profesores Flavio Rosales y Jhonny Granado, quienes ayudaron a ampliar nuestros conocimientos en relación a las áreas de redes y telecomunicación, así como también en el área de simulación y estadística, respectivamente.

Así mismo, queremos agradecer a la Lic. Luzmeli Tineo quien nos permitió acceder a su lugar de trabajo para proponer una solución que resultó en la presente tesis.

Agradecemos a nuestro tutor, Ing. Hiram González, por guiarnos de la forma correcta para el desarrollo de nuestra tesis de grado, además de dedicarse a nosotros durante todo el proceso.

Finalmente, agradecernos el uno al otro por ser un apoyo incondicional durante el desarrollo de la tesis, además de mantenernos unidos y ser grandes amigos desde el inicio de la carrera.

ÍNDICE GENERAL

DEDICATORIA	iii
AGRADECIMIENTOS	iv
LISTA DE CUADROS.....	viii
LISTA DE FIGURAS	ix
LISTA DE ANEXOS.....	xii
RESUMEN.....	xiii
INTRODUCCIÓN.....	1
PARTE I.....	3
DESCRIPCIÓN GENERAL DEL PROBLEMA.....	3
1.1. Formulación del problema.....	3
1.2. Interrogantes	7
1.3. Objetivo general	7
1.4. Objetivos Específicos	8
1.5. Valor Académico de la Investigación.....	8
PARTE II	10
DESCRIPCIÓN TEÓRICA	10
2.1. Antecedentes.....	10
2.2. Bases Teóricas	12
2.2.1. Infraestructura de red	12
2.2.2. La red y tipos de redes	13
2.2.3. Red de área local (LAN)y sus componentes.....	13
2.2.4. Configuración de las Redes LAN	14
2.2.5. Protocolos TCP y UDP	18
2.2.6. La seguridad de datos en la red e implementación de servidores Proxy	18
2.2.7. Servidores Proxy y Firewall Proxy	20
2.3. Bases Legales	23
2.3.1. Constitución De La República Bolivariana De Venezuela (publicada en Gaceta Oficial Extraordinaria N° 36.860, de fecha30 de diciembre de 1999).....	23
2.3.2. Ley Orgánica De Ciencia, Tecnología E Innovación (publicada en Gaceta Oficial Extraordinaria N° 37.291, de fecha 26de septiembre de 2001)	24

2.3.3. Ley Orgánica De Telecomunicaciones (publicada en Gaceta Oficial No. 36.920, de fecha 28 de marzo del año 2000)	25
2.3.4. Ley Especial Sobre Delitos Informáticos (publicada en Gaceta Oficial No. 37.313, de fecha 30 de octubre del año 2001)	26
2.3.5. Ley de Infogobierno (publicada en Gaceta Oficial No. 40.274, de fecha 17 de octubre de 2013)	28
2.3.5. Ley Sobre el Derecho de Autor (publicada en Gaceta Oficial No. 4.638 Extraordinario, de fecha 1 de octubre de 1993)	29
2.4. Definición de Términos	30
PARTE III.....	33
DESCRIPCIÓN METODOLÓGICA	33
3.1. Naturaleza de la investigación	33
3.1.1. Tipo de investigación	33
3.1.2. Diseño de la investigación	33
3.1.3. Población y Muestra	34
3.2. Técnica de recolección de datos	35
3.3. Técnicas de análisis de datos	36
PARTE iv	38
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS.....	38
4.1. Estado actual de la infraestructura de red de la Contraloría del Municipio Antolín del Campo.....	38
4.2 Componentes necesarios para el diseño de la nueva de Red de Área Local alámbrica para la Contraloría del Municipio Antolín del Campo.....	62
4.3 Configuración óptima para garantizar la seguridad y conectividad de la nueva Red de Área Local alámbrica de la Contraloría del Municipio Antolín del Campo.	77
PARTE V	89
LA PROPUESTA	89
5.1. Importancia de la aplicación de la propuesta.....	89
5.2. Viabilidad de la propuesta	90
5.2.1. Viabilidad Técnica	90
5.2.2. Viabilidad operativa.....	96
5.2.3. Viabilidad económica	98

5.3. Objetivos de la propuesta	102
5.3.1. Objetivo General	102
5.3.2. Objetivos Específicos.....	102
5.4. Estructura y representación gráfica de la propuesta	102
CONCLUSIONES.....	145
RECOMENDACIONES.....	147
FUENTES REFERENCIALES	148
ANEXOS	153

LISTA DE CUADROS

Cuadro 1. Esquema de la red actual de la Contraloría del Municipio de Antolín del Campo	51
Cuadro 2. Nivel de proceso para el Análisis FODA.....	56
Cuadro 3. Puntación de los elementos del análisis FODA.	57
Cuadro 4. Ponderación general de cuadrantes de la Matriz FODA.....	57
Cuadro 5. Factores del análisis FODA.	58
Cuadro 6. Análisis DOFA de la Matriz FODA.....	60
Cuadro 7. Configuración del nivel de seguridad de los cortafuegos.	79
Cuadro 8. Configuración de las direcciones y servicios de los equipos administrativos de la nueva red.	82
Cuadro 9. Protocolo DHCP de la nueva red.	84
Cuadro 10. Configuración del CPU para la implementación del servidor Proxy.....	85
Cuadro 11. Configuración cámaras de seguridad de la nueva red.	87
Cuadro 12. Equipos de planta interna y externa de la nueva red.....	94
Cuadro 13. Personal necesario para la viabilidad operativa de la nueva red.....	96
Cuadro 14. Guía para los mantenimientos de la nueva red.....	97
Cuadro 15. Presupuesto para la compro de la equipos y elementos de la nueva red.....	99
Cuadro 16. Presupuesto para el contrato del personal, manteamientos y traslado de compra.	99
Cuadro 17. Costo total de la inversión.....	100
Cuadro 18. Esquematización de los equipos administrativos y de seguridad del nuevo diseño.	131
Cuadro 19. Materiales para la estructuración de la planta alta.	132
Cuadro 20. Materiales para la estructuración de la planta alta.	135

LISTA DE FIGURAS

Figura 1. Ubicación de la Contraloría Municipal de Antolín del Campo.....	39
Figura 2. Planta Alta de la Contraloría del Municipio de Antolín del Campo.....	40
Figura 3. Planta Baja de la Contraloría del Municipio de Antolín del Campo.....	41
Figura 4. Entrada del Cableado Coaxial por parte del ISP de la Contraloría.....	42
Figura 5. Conexión del servicio del ISP a los equipos de red de la Planta Alta de la Contraloría.....	43
Figura 6. Router Amplificar de la planta baja.....	45
Figura 7. Diagnóstico al equipo informático (Laptop) de la Contraloría Municipal de Antolín del Campo.....	46
Figura 8. Prueba de velocidad del equipo administrador de la Contraloría.....	47
Figura 9. Configuración del host central (servicio DHCP) de la red actual.....	48
Figura 10. Servidor local de Nómina de la Contraloría.....	49
Figura 11. Análisis FODA de la infraestructura de red de la Contraloría del Municipio de Antolín del Campo.....	58
Figura 12. Análisis de factores de oportunidad y riesgo.....	59
Figura 13. Cable Ethernet UTP Cat. 5e para interior.....	63
Figura 14. Conectores Rj45 Cat. 5e	63
Figura 15. Canaleta para cableado de red.....	64
Figura 16. Jack Coupler Cat5e	65
Figura 17. Tomas para cableado de red.....	65
Figura 18. Botas de red CAT/5e.....	66
Figura 19. Modem Motorola.....	67
Figura 20. Router Neutro.....	67
Figura 21. Switch TP-Link color negro de 24 puertos Gigabit Ethernet	68
Figura 22. ASA 5505 para seguridad web.....	68
Figura 23. Máquina HP Z640.....	69
Figura 24. Máquina HP.....	70
Figura 25. Monitor HP full HD.....	70
Figura 26. Fuente de alimentación ininterrumpida (UPS) APC.....	71
Figura 27. Detector de humo y monóxido de carbono. Kidde.....	72
Figura 28. Extintor de incendios	72
Figura 29. Desagüe de aguas para baños.....	73
Figura 30. Aire acondicionado para refrigeración.....	74
Figura 31. Relesta protectora/reguladora CRST.....	74
Figura 32. Cámara de seguridad Swann.....	75
Figura 33. Protector de voltaje 220 V.....	76
Figura 34. Rack StarTech.....	76
Figura 35. Topología de la nueva red.....	77

Figura 36. Capas para la nueva red	78
Figura 37. Zona DMZ de la nueva red	86
Figura 38. Adaptación de las cámaras de seguridad en la topología de la nueva red	87
Figura 39. Topología de red detallada con las segmentaciones de red	103
Figura 40. VLAN de Entrada a la red, punto de acceso WiFi al público.....	104
Figura 41. Configuración Wireless del Router para acceso público.....	105
Figura 42. Configuración Network del Router para acceso público.....	105
Figura 43. Configuración LAN del Router para acceso público.....	105
Figura 44. Configuración básica del Wireless	106
Figura 45. Restricciones de seguridad para Router público.....	106
Figura 46. Restricciones de seguridad 2 para Router público.....	107
Figura 47. Restricciones de seguridad 3 para Router público.....	107
Figura 48. Activación del Switch n°0	108
Figura 49. VLAN 5 de la nueva red.....	109
Figura 50. Activación servicios HTTP/HTTPS y TFTP.....	110
Figura 51. Activación protocolo FTP.....	111
Figura 52. Activación protocolo DHCP.....	112
Figura 53. Activación protocolo NTP.....	113
Figura 54. Activación protocolo DNS	114
Figura 55. VLAN Equipos de Seguridad Física.....	115
Figura 56. Activación del Switch n°5	116
Figura 57. Configuración de las cámaras de seguridad.....	116
Figura 58. Configuración de los detectores de monóxido de carbono.....	116
Figura 59. VLAN Dirección de Control de Administración Central	117
Figura 60. Activación del Switch n°4	118
Figura 61. VLAN Dirección de Control de la Administración de Entidades Descentralizadas.	119
Figura 62. Activación del Switch n°3	119
Figura 63. VLAN Administración Central y Recursos Humanos.....	120
Figura 64. Activación del Switch n°2	121
Figura 65. VLAN Coordinación de Despacho Auditoría Interna Atención al Cliente	122
Figura 66. Activación del Switch n° 1	122
Figura 67. VLAN Despacho Central.....	123
Figura 68. Configuración Network del router para acceso wifi privado.....	124
Figura 69. Configuración LAN del router para acceso wifi privado.	124
Figura 70. Configuración Wireless del router para acceso wifi privado.....	124
Figura 71. Configuración Network del router para acceso wifi privado (SSID).	125
Figura 72. Restricciones de seguridad para el router wifi privado.	125
Figura 73. Restricciones de seguridad 1 para el router wifi privado.	126
Figura 74. Restricciones de políticas para el router wifi privado.	126
Figura 75. Restricciones de política para el Router wifi privado.....	127

Figura 76. Velocidades de la nueva red (half-dúplex).....	128
Figura 77. Velocidades de la nueva red (full-dúplex).....	129
Figura 78. Estructuración y representación física de la planta alta para la nueva red.	133
Figura 79. Estructuración y representación física de la planta baja para la nueva red.	136
Figura 80. Distribución física para las conexiones de las máquinas de la Contraloría.	137
Figura 81. Vista aérea de la zona de resguardo de la nueva red.	139
Figura 82. Vista lateral (3D) de la zona de resguardo.....	140
Figura 83. Distribución completa (3D) de la zona de resguardo.	141
Figura 84. Estructura del armario de red.....	143

LISTA DE ANEXOS

Anexo 1. Formato de entrevista realizada al personal administrativo de la Contraloría del Municipio Antolín del Campo.....	153
Anexo 2. Formato de entrevista realizada al personal de soporte técnico externo de la Contraloría del Municipio Antolín del Campo.....	155
Anexo 3. Vista exterior de la ventana de entrada del cableado coaxial proveniente del ISP	158
Anexo 4. Vista interior de la planta baja de la sede de la Contraloría del Municipio Antolín del Campo	159
Anexo 5. Estaciones de trabajo del personal administrativo de la Contraloría del Municipio Antolín del Campo	160

UNIVERSIDAD DE MARGARITA
SUBSISTEMA DE DOCENCIA
COORDINACIÓN DE INVESTIGACIÓN

**DISEÑO DE RED DE ÁREA LOCAL ALÁMBRICA PARA LA OPTIMIZACIÓN DE
LA CONECTIVIDAD Y LA SEGURIDAD DE DATOS MEDIANTE UN
SERVIDOR PROXY EN LA CONTRALORÍA DEL
MUNICIPIO ANTOLÍN DEL CAMPO**

Autores:

David Moro Tineo

Danyelis Paz Castillo

Tutor: Ing. Hiram González Gómez

Noviembre de 2022

RESUMEN

En toda institución, donde constantemente se maneja una gran cantidad de información y se tienen diversos equipos de trabajo, es de suma importancia contar con un sistema de red que sea seguro, facilite el envío de dicha información y, además, permita aprovechar los recursos que se tienen; es por esto, que las Redes de Área Local (LAN) representan la mejor opción para cualquier institución. En la Isla de Margarita, específicamente en la Contraloría del Municipio Antolín del Campo, existe una situación preocupante en cuanto a su red actual, puesto que, primeramente, no cumple con los estándares que amerita el organismo para ejecutar sus tareas diarias y no posee un nivel de seguridad adecuado para la protección de la información. En consecuencia, se propone el diseño de una Red de Área Local bajo un enfoque cuantitativo y orientado como proyecto factible; con la finalidad de potenciar la productividad de dicha institución.

Descriptores: infraestructura de red, red de área local, red alámbrica, servidor proxy, conectividad, seguridad de datos

INTRODUCCIÓN

Entre los avances tecnológicos más importantes que se han creado en el siglo XX se encuentran las redes informáticas, las cuales se implementan actualmente en las más grandes empresas o incluso en pequeños hogares. La aparición de estas redes significó un cambio radical en el día a día, pues dio inicio a una nueva forma de comunicarse y, sobre todo, de enviar cualquier tipo de información desde cualquier lugar y de manera inmediata. Asimismo, existen diversos tipos de redes, siendo las más comunes las Redes de Área Local o simplemente LAN; a su vez, dentro de las redes LAN se hallan las redes Ethernet, siendo aquellas que se conectan por cableado. Hoy en día, las redes Ethernet son altamente implementadas en las empresas por dos razones primordiales: primero, el cableado permite transportar grandes cantidades de información mucho más rápido; y segundo, permite aprovechar el uso de los recursos que tiene la empresa, ya que se puede conectar un mismo equipo para varios departamentos.

Así pues, en Venezuela las redes LAN Ethernet están presentes en empresas, hogares, centros educativos, locales y demás entidades, en las cuales se requiere de una infraestructura de red capaz de interconectar todos los equipos de trabajo entre sí y, al mismo tiempo, proveerles conexión a internet. Por otra parte, la mayoría de las empresas e instituciones nacionales optan por este tipo de red debido a su costo accesible y su fácil instalación y mantenimiento; puesto que, si bien se necesita más cableado para un mayor alcance, permiten agregar diferentes dispositivos como amplificadores y switches que faciliten la distribución de la señal de internet a diferentes espacios.

En el caso de la Isla de Margarita, específicamente en la Contraloría del Municipio Antolín del Campo, se vive una problemática con su red wifi la cual afecta notablemente en la realización de las operaciones y tareas diarias del organismo. La Contraloría cuenta con un modem y un Router principal, encargado de repartir la señal de internet en todo el lugar; sin embargo, el Router está configurado de tal manera que solo un número muy limitado de equipos se puedan conectar a la red. Esto ocasiona que, cuando están conectados todos los ordenadores, la señal de internet se debilite y retrase el envío de documentos importantes; por lo que los trabajadores tienen que optar por desconectar los equipos que no se estén utilizando en el momento de la red, y así otros trabajadores puedan ejecutar cualquier operación.

Es por lo anteriormente expresado, que en el presente trabajo se desarrolla una investigación de campo de tipo proyectos factible con el objetivo último de proponer el diseño de una Red de

Área Local para la Contraloría con la finalidad de mejorar la conectividad de los equipos de trabajo, además de establecer un sistema de control interno que proteja los datos que se envían por la red. En cuanto a la estructura del presente trabajo de investigación, este se divide en cinco partes que se describen a continuación:

La **Parte I**, denominada Descripción General del Problema, en la cual se desarrolla a profundidad la formulación del problema estudiado. Luego, le siguen las interrogantes derivadas de dicha formulación; seguidamente los objetivos, desglosados en general y específicos y, por último, el valor académico de la investigación.

La **Parte II**, llamada Descripción Teórica, consta de los antecedentes o trabajos relacionados con el tema estudiado, las bases teóricas y legales que sustentan la investigación y, la definición de términos.

La **Parte III**, llamada Descripción Metodológica, compuesta por la naturaleza de la investigación, dentro de la cual se especifica el tipo y diseño de la investigación y la población y muestra de las cuales se obtendrán los datos a analizar; seguido de las técnicas de recolección y análisis de los mismo.

La **Parte IV**, denominada Análisis y Presentación de Resultados, en donde se describen y explican detalladamente los resultados obtenidos del proceso de investigación, organizados de acuerdo a las necesidades de información de las interrogantes y objetivos específicos de la investigación.

Finalmente, la **Parte V**, correspondiente a la Propuesta, en la cual se describe la importancia de la aplicación de la propuesta realizada y la viabilidad de la misma, desglosada a su vez en viabilidad Técnica, operativa y económica; los objetivos que se desean alcanzar con dicha propuesta, comprendido por objetivo general y específico. Además, se exponen la estructura y representación gráfica de la propuesta.

A estas cinco partes se le suman las **Conclusiones**, que no son más que una síntesis de la información obtenida durante el desarrollo del trabajo con la que se da respuesta a las interrogantes formuladas al principio de la investigación; luego las **Recomendaciones** hechas por los investigadores en concordancia con los resultados obtenidos. Por último, la lista de **Fuentes Referenciales** consultadas durante la elaboración de la investigación.

PARTE I

DESCRIPCIÓN GENERAL DEL PROBLEMA

Pino, R. (2010) describe el planteamiento del problema como: “una situación de la realidad de una manera clara y transparente. Tiene que ser expuesto en términos honestos tal como ocurre y se observa sin agregar o quitar detalles de índole subjetiva”. Por consiguiente, la descripción general del problema permite poder describir la problemática que presenta el objeto de estudio en un entorno micro, meso y macro, enfocándose en las causas y consecuencias que presentaría el mismo.

1.1. Formulación del problema

Desde hace varios años los avances tecnológicos a nivel mundial han provocado un cambio en la estructura de redes en conjunto a la conectividad de los equipos de trabajo, permitiendo enviar información entre los dispositivos mediante impulsos eléctricos. Debido a esta innovación tecnológica se ha buscado la manera de poder intercomunicar los equipos dentro de una red. Dordogne, J. (2008: 7) define a una red como “un esquema constituido por ordenadores y sistemas operativos heterogéneos, que a menudo se interconectan a través de Internet”.

De esta manera, las redes se basan en un flujo de información, la cual puede viajar mediante conductos que transportan electricidad o también por la transmisión mediante ondas. Igualmente, existen numerosos equipos que brindan diversas funcionalidades a la red tales como: los Switches, Routers, hubo, balanceadores de carga, entre otros; los cuales, dependiendo de la infraestructura, se pueden implementaren redes alámbricas o inalámbricas. A su vez, se presentan las redes de datos, las cuales implementan nodos para el flujo o transporte de información (conjunto de datos); por lo que, según Pérez, J y Merino, M. (2014: párr.4) exponen que una red de datos es una “una estructura que cuenta con un patrón característico (...) mediante la interconexión de computadoras y otros dispositivos que comparten recursos (...) que permite el flujo de información de un equipo a otro”.

Debido a esto, las redes de datos permiten poder recibir y enviar información en un entorno controlado de dispositivos, mediante diversos procesos como: la red de transmisión de datos que permiten poder transportar señales analógicas a digitales mediante impulsos electromagnéticos. Briceño, J. (2005: 14) establece que una transmisión de datos es un “(...) proceso mediante el cual transcurre la información de un punto hacia otro”; lo que permite generar una unión entre los

dispositivos conectados en la red, que dependiendo de su forma e infraestructura llega a dividirse en diversos tipos.

En el mismo orden de ideas, Tanenbaum, A. (2012:15), en su libro Redes de computadoras, establece que:

(...) las redes alámbricas se conectan mediante cableado eléctrico UTP (...) utilizando conectadores RJ-45... siempre y cuando se conozca la infraestructura de la red ... mediante un diseño de mapa de red ... Por lo contrario, una red inalámbrica (...) se puede obtener a una cierta distancia del punto receptor (...). Sin necesitar un plan demasiado extenso (...) y diferenciándose por no utilizar cableado para comunicarse, sin embargo, para poder llevar a cabo la comunicación del emisor con el receptor es necesario establecer conexiones manuales a cada equipo que conforma nuestra infraestructura de red.

Por lo tanto, se debe determinar la infraestructura de cualquier entorno antes de establecer soluciones óptimas, mediante la aplicación de protocolos o elementos que permitan definir qué tipo de red se debe ejecutar mediante una topología diseñada, que logre cumplir con sus procesos regulados por un equipo central o servidor. Dentro de cada infraestructura de red, existe un delimitado tipo de red, siendo de las más conocidas la Red de Área Local (LAN), la Red de Área Personal (PAN), la Red de Área Metropolitana (MAN), la Red de Área Amplia (WAN), la Red de Área Global (GAN) y la Red de Área Local Inalámbrica (WLAN). De acuerdo con Turcios, K. (s/f:1), la Red de Área Local (LAN) es un:

Conjunto de equipos que pertenecen a la misma organización y, además, están conectados dentro de un área geográfica pequeña mediante una red, generalmente con la misma tecnología. (...) pueden definir dos modos operativos diferentes:

- En una red "de igual a igual", la comunicación se realiza de un equipo a otro sin un equipo central y cada equipo tiene la misma función.
- En un entorno "cliente/servidor", un equipo central brinda servicios de red para los usuarios.

En este sentido, este tipo de red está formada por un proceso o configuración específica, interconectados mediante cableado de red (Ethernet) que, dependiendo de sus factores, lleva a determinar una forma de implementación; por otra parte, las LAN no presentan conexiones mediante ondas eléctricas. Los datos que se emiten y transportan mediante este tipo de red deben presentar un proceso de seguridad de información para poder prevenir posibles fallas o problemas que pueden afectar de alguna manera al propietario de dicha red. En relación a lo anterior, la empresa IBM señala que a seguridad de datos es “la práctica de proteger la información digital de

acceso no autorizado, corrupción o robo en todo su ciclo de vida”. La información contenida dentro de esta red es delicada para una organización, por lo que es necesario que pase por una serie de procesos comolos: encriptación, confidencialidad, integridad, firewall, análisis, verificaciones, entre otros, para poder tener un control del flujo en su transmisión.

Es por esto, que para poder generar una red de conexiones en cualquier ente u organización se necesita contar con un elemento vital para la regulación y control de los datos, uno de estos puede llegar a ser un servidor. Mateu, L. (2004:06), define a un servidor como: “(...) un programa que atiende y responde a las diversas peticiones de los ordenadores que conforman su sistema”. Dicho equipo permite regular, controlar y administrar las direcciones IP a donde quieran acceder cada dispositivo, siendo un parámetro de seguridad debido a que permite identificar y conocer el paso de un elemento de infraestructura en la web, garantizando precisar su ubicación exacta en un momento determinado, así como también los procesos que ha realizado, ya sea de descarga o subida de datos.

Para un ente gubernamental, poder implementar una red que presente un proceso de trasmisión y seguridad de los datos es vital hoy en día, debido que existen nuevas formas de comunicación, lo que genera que los procesos de redes estén en constante apogeo, ya que son una de las fuentes de transmisión de información más completas; además de contar con una amplia variedad cuya elegibilidad depende en gran medida de la configuración física del recinto donde se implementarán y de la conectividad que se busca, de manera que se garantice un manejo sencillo de la información.

A nivel mundial, se han implementado redes de comunicaciones que solventaron las problemáticas para las cuales fueron elaborados. En Quito - Ecuador, Carrasco, C. (2009) implementó una LAN con la finalidad de centralizar y optimizar los procesos administrativos en la Unidad Educativa Quito Sur. Actualmente dicho sistema sigue estando operativo logrando alcanzar las expectativas propuestas en el estudio e implementación del mismo. Por otra parte, en San Luis, Lima - Perú, la ingeniera Viloria, J. (2018) llevó a cabo una infraestructura LAN con cableado estructurado para las oficinas de Trainees de la Empresa IDI ELECTRÓNICA. Dicha red sigue abarcando parte fundamental de la empresa junto a nuevas instalaciones, considerando un proceso flexible para diversos cambios estructurales.

En el caso de Venezuela, se ha visto influenciada por el alcance de las redes LAN, que lograron abarcarse en la ciudad de Caracas, mediante implementaciones de sistemas de Red para

mejora de servicios de comunicación de los equipos de red en las grandes empresas y organizaciones del Distrito Capital, donde al pasar del tiempo han ido evolucionando dependiendo del uso que se necesite de la misma, desatancando entonces la utilidad de la LAN para la optimización y mejora el flujo de la información de aquella empresas u organismo que la implemente.

Así mismo, en estos últimos años, en los entes gubernamentales se ha comenzado a implementar, reestructurar, mejorar y optimizar las redes de datos, debido a que presenta en la actualidad un proceso fundamental para flujo de información en un entorno de trabajo; por lo que, en la mayoría de los casos, termina formando parte fundamental de la institución. En la Isla de Margarita, las redes de datos se han presentado en los organismos de trabajo de nivel público, siendo uno de los principales la Alcaldía del Municipio Mariño, donde desde hace varios años contaban con una infraestructura LAN, la cual actualmente se ha modificado y transformado en una WLAN, demostrando que la implementación de este modelo de red se mantiene vigente.

Por su parte, en la Contraloría del Municipio Antolín del Campo se están suscitando fallas en los procesos de comunicación de sus equipos de red, debido a que la estructura e implementación de su diseño de red no presenta una acorde configuración que satisfaga las necesidades de la institución. Así mismo, cuentan con una conectividad limitada al servicio de internet, siendo suministrado por una línea conmutada conectada hacia un equipo central, que es el único con acceso a dicho servicio.

Debido a que la infraestructura de red no abarca todo el espacio de trabajo de la Contraloría, ocasiona problemas de conectividad, reflejándose directamente en la disminución de la amplitud de su ancho de banda, causando la caída constante del internet, generando retraso en el envío de documentos como: planes de trabajo, nóminas de personal y presupuestos de acción. Además, la arquitectura de la red no está diseñada para la conexión de otros equipos, puesto que al intentar agregar un nuevo dispositivo provocaría una mayor atenuación, lo que terminaría repercutiendo a su vez en que los procesos de transacciones bancarias se vean afectados, al no lograr efectuar los pagos a tiempo, lo que conllevaría a desajustes de sus planes de trabajo.

En este mismo orden de ideas, se puede hablar de pérdida de paquetes de datos, debido a que no existe un camino idóneo para el transporte de la información que viaja entre los equipos, trayendo como consecuencia que, en las conferencias mediante videos llamadas, la información no llegue de manera correcta. Por otra parte, ocasionan interrupción en carga y descarga de

archivos, generando una latencia inestable entre el emisor y el receptor. Así mismo, la Contraloría no presenta un servidor principal que permita el resguardo y protección de los datos de su red, el cual se encargue de regular la entrada y salida de información de cada equipo de trabajo, lo que podría devenir, en el peor de los casos, en robo de datos de cuentas bancarias, documentos de fiscales y, también, infecciones en los equipos de trabajo mediante la ejecución de algún virus.

Lo que repercute, que pueda llegar a generar en este ente gubernamental procesos de inestabilidad de la infraestructura de su red, junto a la caída del internet en su equipo principal de trabajo, donde por consecuencia generaría retrasos en su proceso de trabajo, alargando así las labores diarias de sus empleados. Dicho esto, se considera como una posible solución el diseño de una Red de Área Local alámbrica para la optimización de la conectividad y la seguridad de datos mediante un servidor Proxy, para así lograr mejorar los procesos de comunicación entre los equipos de trabajos que, permitiendo compartir su información mediante transmisión de datos, generando reorganización en su configuración de red brindado que sus niveles de atenuación y latencia sean las necesarias para poder realizar sus procesos, y finalmente lograr mejorar la seguridad de la información que suministra la Contraloría.

1.2. Interrogantes

En correspondencia con lo expuesto en el apartado anterior, surge la siguiente interrogante: ¿Cómo será diseño una Red de Área Local Alámbrica para la optimización de la conectividad y seguridad de datos mediante un servidor Proxy en la Contraloría del Municipio Antolín del Campo? Así mismo, partiendo de dicha interrogante, se desglosan las siguientes:

1. ¿Cómo es el estado actual de la infraestructura de red de la Contraloría del Municipio Antolín del Campo?
2. ¿Qué componentes se necesitarían para el diseño de una nueva Red de Área Local Inalámbrica para la Contraloría del Municipio Antolín del Campo?
3. ¿Cuál sería la configuración óptima para garantizar la seguridad y conectividad de la nueva Red de Área Local Inalámbrica de la Contraloría del Municipio Antolín del Campo?

1.3. Objetivo general

Diseñar una Red de Área Local alámbrica para la optimización de la conectividad y seguridad de datos mediante un servidor Proxy en la Contraloría del Municipio Antolín del Campo.

1.4. Objetivos Específicos

1. Identificar el estado actual de la infraestructura de red de la Contraloría del Municipio Antolín del Campo.
2. Precisar los componentes que se necesitarían para el diseño de la nueva Red de Área Local alámbrica para la Contraloría del Municipio Antolín del Campo.
3. Analizar la configuración óptima para garantizar la seguridad y conectividad de la nueva Red de Área Local alámbrica de la Contraloría del Municipio Antolín del Campo.

1.5. Valor Académico de la Investigación

Debido a que en la actualidad las instituciones buscan abordar grandes proyectos, se ven en la necesidad de implementar una infraestructura de red ajustada a las necesidades que correspondan. Esto se debe a que regularmente se evidencian dificultades para el flujo de datos dentro de los organismos, generalmente ocasionada por una mala implementación de la red. De allí, el valor de contar con la infraestructura de red adecuada, pues de esta depende el buen funcionamiento de la misma, permitiéndole a sus empleados el poder trabajar de manera cómoda, eficiente y rápida sin ningún tipo de interrupción o retraso.

En el caso concreto de las instituciones de gobierno, estas manejan información delicada de personas asociadas, así como también de otros entes gubernamentales, siendo fundamental el hacer énfasis en el tema de la seguridad de datos, pues estos representan el principal activo de cualquier organización; por ende, no aplicar las medidas de seguridad correctas puede conllevar a consecuencias perjudiciales para la misma. Teniendo en cuenta lo anterior, sale a relucir la importancia de la protección de datos sensibles de una organización, garantizándoles fiabilidad, buena reputación y, sobre todo, confianza a sus asociados. De la misma forma, contar con una infraestructura LAN que permita la interacción con los equipos de trabajo de dichas instituciones es fundamental para su desarrollo, además de implementar elementos tecnológicos óptimos que ayuden a las organizaciones a no mal gastar su capital en recursos innecesarios y, por ende, garantizar el ahorro de tiempo en las labores de la misma, junto a facilidad de poder compartir información hacia otro departamento u organización.

Siguiendo este orden de ideas, la presente investigación brindará un conocimiento general de cómo estaría constituida una Red de Área Local, identificando aquellos elementos que la conforman junto a las funcionalidades que presentan a nivel de infraestructura, contemplando

además el manejo seguro de la información mediante la implementación de servicios, logrando conocer el proceso de trabajo de la red anteriormente mencionada. También, se recalca en la misma la importancia de poder contar con datos seguros dentro de un ambiente de trabajo en una institución o ente gubernamental.

Así mismo, destaca la necesidad de poder implementar redes de computadora que logren innovar, debido a que brindan soluciones a los desafíos que abarcan los organismos o entes gubernamentales, bajo los recursos que presentan. Por consiguiente, se busca con esta investigación generar conciencia en la comunidad académica sobre la importancia que representa el poder contar con procesos de redes para Instituciones Gubernamentales, que permitan administrar de manera eficiente sus recursos. De igual forma, se busca que, en el futuro, esta investigación sirva como antecedente para aquellos objetos de estudio relacionados con la temática en cuestión.

Por último, para los investigadores conlleva un valor académico de gran importancia, debido que genera expectativas del cómo debería funcionar de manera eficiente una red LAN, utilizando un servidor o host principal que funcione como ente regulador de toda la red, pero sobre todo el lograr determinar cómo administrar la infraestructura de red para que así todos los equipos que se encuentren en uso estén interconectados de la mejor manera posible, aprovechando en su totalidad dicha conectividad. Además, permite reflexionar sobre los protocolos o permisos de seguridad de la red apoyándose en diversos medios, sabiendo que siempre se tiene por objetivo final el llegar a entender el funcionamiento general de la infraestructura de una red mediante un servidor regulador.

PARTE II

DESCRIPCIÓN TEÓRICA

Según Hernández, R, Fernández, C y Baptista, M. (2006), definen la descripción teórica como: “un compendio escrito de artículos, libros y otros documentos que describen el estado pasado y actual del conocimiento sobre el problema de estudio. Nos ayuda a documentar cómo nuestra investigación agrega valor a la literatura existente”. En esta parte, se muestra lo pertinente a la literatura encontrada y relacionada con la temática de la presente investigación; exponiendo trabajos o investigaciones realizadas que sirven de guía para la misma, además de las bases teóricas y legales que la sustentan, siempre que tenga relación con la temática estudiada.

2.1. Antecedentes

García (2020), realizó un trabajo de grado para optar al título de Tecnólogo en Sistemas, intitulado: *REDISEÑO DE LA RED LAN DE LA COMPAÑÍA CORE ADVANCE GROUP SAS*. Abordado mediante un modelo cuantitativo, tuvo como objetivo el rediseño de la red LAN mediante el levantamiento de la información de la empresa, junto a su análisis y requerimiento para lograr el diseño de la red. El autor buscaba solucionar los aspectos e inconformidades de la empresa Core AdvanceGroup SAS mediante la distribución de sus equipos, el tipo de cableado, la velocidad de la red, la seguridad de la red, la calidad de salida de llamadas, y navegación de páginas web. Este trabajo logró poder identificar la parte estructural que conlleva la creación de una nueva red para dar solución a los problemas de administración de recursos, accesibilidad de la información, para futuros procesos de revisión.

Este trabajo presentaba como idea poder implementar una red más confortable para el acceso a internet, y los ajustes de comunicación para la salide de llamada, de tal manera que a futuro la empresa goce una estabilidad a nivel de infraestructura de red. Por otra parte, se busca analizar los equipos de trabajo que están presenten en el esquema de la red; generando un estudio interno de las necesidades de la compañía, y comparándolo que diseño actual de la red. Demostrando las debilidades que está sostiene. La base teórica relacionada con los equipos de trabajo a implementar, para el rediseño de la red LAN, servirán de base para la presente investigación.

Ledesma (2018), realizó un proyecto técnico para la obtención del título de Ingeniero de Sistemas, intitulado: *REESTRUCTURACIÓN DE LA INFRAESTRUCTURA DE RED LAN BASADO EN LAS NORMAS DE CABLEADO ESTRUCTURADO, Y LA APPLICACIÓN DE*

POLÍTICAS DE SEGURIDAD PARA EL CONTROL DE ACCESO MEDIANTE UN SERVIDOR PROXY LINUX EN LA UNIDAD EDUCATIVA HISPANOAMERICANO, realizado bajo el modelo cuantitativo, bajo el término de proyecto factible. Dicho trabajo tuvo como objetivo la reestructuración de la red LAN de la Unidad Educativa Hispanoamericano mediante la aplicación de las normas de cableado estructurado y aplicación de políticas de seguridad para el control de acceso de los usuarios. La autora identificó que la infraestructura de red representaba anomalías como: no etiquetación del cableado, el uso de cables en mal estado, y también la inexistencia de un punto de red.

Este proyecto logró solventar problemas de conexión a internet, detección de fallas mediante la identificación y etiquetado de cada punto de red y brindó una mejor administración al disponer de un diseño lógico de la red actual. Mediante este trabajo de investigación, se logró conocer los parámetros de seguridad necesarios a implementar en una red LAN, regulados por un servidor proxy. Otorgando así, relevancia para la presente investigación, ya que permite conocer las políticas de seguridad que pueden llegar a aplicarse.

Zheng (2017), realizó un trabajo grado para la obtención del título de Licenciado en Redes y Sistemas Operativos, intitulado: *DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN PARA LA EMPRESA PALINDA*. El mismo fue desarrollado bajo el modelo de investigación cuantitativo de tipo proyecto factible y teniendo como objetivo el diseñar e implementar una red LAN, para lograr abarcar la conexión de todos los equipos de la red y usuario final con una arquitectura Cliente-Servidor. Desde el punto de vista del autor, observó que se requiere un equipamiento informático, aplicaciones, cableado estructurado e infraestructura que se comuniquen entre sí para poder realizar las operaciones diarias de la empresa. En este proyecto, se tomó el Ethernet como la tecnología que fundamentó la administración e implementación de la red diseñada, logrando aprovechar el ancho de banda disponible mediante el enfoque de red jerárquicas, agrupando equipos funcionales y separándolos en 3 niveles de fácil abordaje.

El proyecto buscaba mejorar la integridad de los servicios de comunicación de la empresa PALINDA, mediante el análisis previo de los requerimientos de la infraestructura; lo que permitió plantear los diferentes parámetros a desarrollar, para garantizar el óptimo uso de la red. Por consiguiente, sirve como sustento para conocer la conformación lógica de una red LAN, juntoun proceso de transmisión de datos hacia un punto central que abarca toda el área de la empresa; por lo cual, se considera como base para la presente investigación.

2.2. Bases Teóricas

2.2.1. Infraestructura de red

En la presente investigación hace relevancia hacia los procesos de comunicación de la información, que representa un proceso fundamental para que una organización o empresa funcione de manera correcta mediante la implementación de un cableado estructurado, que permite intercomunicar a los equipos de trabajo que abarquen el espacio donde se encuentra la infraestructura de red.

Pastar, O. (2022). Menciona en un artículo de la Universidad de Carlemany que, la infraestructura de red:

Engloba todo el hardware y software necesario para la instalación y su uso. Por otra parte, hay que señalar que esto sirve para la comunicación ordinaria. Básicamente, la infraestructura engloba el cableado estructurado, la alimentación de los equipos, el SAI, los sistemas de seguridad, el cuarto de comunicaciones y la electrónica de red.

Haciendo énfasis el autor, en que la infraestructura de red está compuesta por una serie de elementos, que permiten coordinar los procesos que se ejecutan (subida y bajada) de dato, por lo cual se dispone a representar un procedimiento de cableado estructurado para obtener un desempeño predecible en la red. Además, asegura que los equipos que la conforman se conectan de manera eficiente siendo así fundamental para futuros procesos de actualizaciones, ya sea en la propia infraestructura de red o de algún dispositivo que la conforme.

Debido a esto, para la investigación se consideran los factores de beneficio que brindan la correcta implementación de una infraestructura de red, generando de esta manera mejora en algunos procesos de las organizaciones. Siendo uno de los principales la reducción de los costos de trabajo, junto a maximizar los procesos de ejecución. Reimann, R. (2021). Plantea que: “mediante la correcta implementación de infraestructura red, permite reducir los costos y mejorar al máximo los procesos dentro de una operación son, seguramente, dos de los principales objetivos de cualquier compañía o institución”. Entonces, poder contar una infraestructura de red que presenta un correcto cableado estructurado permite lograr obtener los objetivos deseados por la organización, viéndose mejoría en los procesos de trabajo. Siempre que se conozcan todos equipos elementos o equipos que la conforman.

2.2.2. La red y tipos de redes

Leyva, N. (2018) define a la red como:

Una serie de PC y otros dispositivos conectados por cables en forma alámbrica o inalámbrica entre sí.
Esta conexión permite comunicarse entre ellos y compartir información y recursos. Las redes varían en tamaño; pueden reducirse a una oficina o extenderse globalmente (...). Los dispositivos de una red se comunican entre sí, transmitiendo información en grupos de pequeños impulsos eléctricos (conocidos como paquetes). Cada paquete contiene la dirección del dispositivo transmisor (la dirección fuente) y la dirección del receptor (dirección de destino). Las PC y otros equipos de la red utilizan esta información para ayudar al paquete a llegar a su destino.

En este sentido, se expresa como red al conjunto de equipos que forman parte de un sistema, donde existe un flujo de información originado por impulso eléctrico, que permite transferir datos mediante un cable de red u ondas. Dependiendo del área que abarquen los equipos de red de la organización o empresa, se verá reflejado en tipo de estructura de red que deba implementarse.

Nuevamente, Leyva explica que:

Una red conectada en un área limitada se conoce como, Red de área local (LAN). Una LAN está contenida a menudo en una sola ubicación. Una Red de área extensa (MAN O WAN) es un grupo de dispositivos, o varias LAN, conectados en un área geográficamente mayor, a menudo por medio de líneas telefónicas, cables de fibra óptica, microondas vía satelital o terrestre u otro formato de cableado como puede ser una línea dedicada de alta velocidad. Uno de los mayores ejemplos de WAN es la propia Internet. Existen otras redes que son personales como PAN y SAN.

Por ello, determinar el nivel o alcance de la red es fundamental para lograr determinar el tipo de red de área que se necesita diseñar, abarcando de esta manera a todos los equipos que pueden llegar a conectarse a ella, ya sea mediante conexiones alámbricas (por cableado Ethernet) o inalámbricas (por ondas). Para motivos de esta investigación, se ve en la necesidad de enfatizar en las LAN. Para la investigación se resalta la infraestructura LAN como procesos de transmisión de datos.

2.2.3. Red de área local (LAN) y sus componentes

Páez, L. (2021: párr.4). Define a LAN como: “un conjunto de dispositivos electrónicos conectados entre sí que comparten una línea de comunicación común (...) con un servidor”. Entonces, una LAN es una red que abarca a diversos equipos, que solo pueden interconectarse

mediante un cableado de Ethernet; siempre enfocado hacia un punto de unión, conocido como servidor. Por otra parte, debido a los diversos elementos que pueden abarcar en esta red, primero es necesario conocer mecanismos solicitados para los procesos que se requieren dentro de esa infraestructura; siendo este un modo para poder determinar la topología o estructura de la red.

Las LAN están unidas por diversos equipos de trabajo, sin embargo, para su propio funcionamiento es indispensable contar con algunos componentes. Guzmán, D. (2018) establece que son: “(...) dispositivos, medios o servicios que en conjunto forman la infraestructura de red a través de la cual viaja la información y que respalda la comunicación (...) son dispositivos que se conectan de forma directa a un segmento de la red”. En este sentido las infraestructuras LAN, cuentan con ciertos elementos conectados directamente al cableado Ethernet, donde cada uno se encarga de realizar algún proceso dentro de ese entorno; dependiendo de las necesidades que se visualicen en los estudios previos. Nuevamente Guzmán, presenta, qué existen diversos componentes como:

- **Servidor.** Es la máquina encargada de ejecutar el OS de red que utilizan las estaciones de trabajo restantes.
- **Sistema de cableado.** Se refiere al cable coaxial, Ethernet o de fibra óptica que tiene la función de establecer los enlaces de datos entre las máquinas.
- **Tarjetas de interfaz de red.** Parte esencial de una conexión, es el esquema de red, que puede ser Arcnet, Ethernet o Token Ring. El cable va conectado a la tarjeta para interpretar los paquetes de datos.
- **Dispositivos periféricos y compartidos.** Aquí encontramos equipos como routers para distribuir la señal, bridges para conectar varias LAN y repetidores. También se incluye las impresoras, discos ópticos, HDD, trazadores y otro hardware.

Debido a esto, las LAN están formadas por diversos elementos que permiten su correcto funcionamiento, por otra parte, cada elemento que está conectado tiene tareas específicas a aplicarse en algún momento; siempre considerando aquellos beneficios de los equipos de trabajo que estén implementados en la infraestructura de red. Logrando concluir que los componentes de una red LAN son una subred segmentada y conectado mediante diversos equipos.

2.2.4. Configuración de las Redes LAN

Cuando se piensa en construir una Red LAN, esta engloba una diversidad de elementos, como los equipos de trabajo, los componentes de red, pero también entra en acción uno de los pilares de la infraestructura de una red, denominado la configuración de la misma, sabiendo que parte del sentido de dar una serie de permisos, restricciones, protocolos y controles que asignan

directamente en flujo de la red; siendo utilizado para configurar aquellos elementos inmersos dentro de toda la red.

Pardo, F. (2018) expresa que:

Es esencial elegir una configuración de red correcta para respaldar el flujo de tráfico a través de esta, así como respaldar y mejorar la seguridad y la estabilidad de la red. Además, utilizar herramientas de configuración o de gestión de la configuración de red puede conllevar distintas ventajas, como, por ejemplo:

- Automatización del seguimiento de datos y la generación de informes, que permite a los administradores detectar cualquier cambio de configuración y posibles amenazas o problemas.
- Una forma fácil de implementar cambios en bloque, como puede ser un cambio general de contraseñas si se da el caso de que estas se vean comprometidas.
- Los medios para restaurar rápidamente la configuración de red a una configuración anterior.
- Reducción del tiempo de inactividad gracias a una mayor visibilidad y a la capacidad de detectar cambios rápidamente.
- Optimización del mantenimiento y la reparación de los dispositivos de red (físicos o virtuales) y las conexiones.
- La posibilidad de reiniciar un dispositivo cuando falla, gracias a la gestión de almacenamiento centralizada de las configuraciones del dispositivo.

Dado lo planteado por el autor, contar con una configuración en nuestra Red es primordial para la funcionalidad de la misma. Sin embargo, dependiendo de la formación de la misma, es decir si es física o virtual, la configuración cambiará dísticamente. Pardo nuevamente explica que: “(...) en una red virtual es más fácil realizar cambios de configuración, porque los dispositivos de red física se reemplazan por software, eliminando la necesidad de configurarlos mediante un tedioso proceso manual. (...) caso contrario para una red física”. Por otra parte, un elemento principal para la configuración de una red, es lo denominado topologías de red.

Rouse, M. (2021: párr.2). Establece que:

Una topología de red es la disposición de una red, incluyendo sus nodos y líneas de conexión. Hay dos formas de definir la geometría de la red, la topología física y la topología lógica (o de señal). Debido a la disposición geométrica real de las estaciones de trabajo. Existen varias topologías físicas comunes, como:

- **Topología de la red de bus:** donde cada estación de trabajo está conectada a un cable principal llamado bus. Por lo tanto, en efecto, cada estación de trabajo está conectada directamente a cada otra estación de trabajo de la red.

- **Topología de red en estrella:** hay un ordenador central o servidor al que todas las estaciones de trabajo están conectadas directamente. Cada estación de trabajo está indirectamente conectada entre sí a través de la computadora central.
- **Topología de red en anillo:** las estaciones de trabajo están conectadas en una configuración de bucle cerrado.
- **Topología de red de malla (Mesh):** emplea cualquiera de los dos esquemas, llamados malla completa y malla parcial. En la topología de malla completa, cada estación de trabajo está conectada directamente a cada uno de los otros
- **Topología de red de árbol:** utiliza dos o más redes en estrella conectadas entre sí. Los ordenadores centrales de las redes en estrella están conectados a un bus principal. Así, una red de árboles es una red de buses de redes estrella.
- **Topología lógica (o de señal):** se refiere a la naturaleza de los caminos que siguen las señales de nodo a nodo. En muchos casos, la topología lógica es la misma que la topología física. Pero no siempre es así.

Por lo cual, considerando lo planteado por el autor, se lleva a destacar que la topología de red es una parte fundamental para el armado de la infraestructura de red. Debido a que permite definir la jerarquía de los equipos en la red. Donde se identifican los procesos lógicos o físicos; a su vez sirve guía de diseño para la implementación o armado completo de la red. Limones, E. (2021: párr.25) plantea que: “la topología de red más utilizada en la actualidad es la de estrella gracias a las ventajas que presenta como son; la alta escalabilidad (...) sin embargo, toda topología de red se definirá dependiendo de las necesidades del área”.

Considerando esto, el tipo de topología de red se verá reflejada dependiendo de las necesidades que representan los equipos de la red. Por otra parte, siempre se deben considerar los procedimientos más óptimos para el beneficio general de la infraestructura, entonces dependiendo del área, tamaño o beneficios, se logrará conocer el diseño a aplicar. Además, se debe reflejar que los factores externos pueden influir en la aplicación de alguna topología sobre la otra, como lo puede ser: la flexibilidad, el gasto económico, la viabilidad y la conectividad de los equipos.

Hertzog, R y Mas, R. (2015) hablan sobre la configuración de la red LAN, en el Manual de Administrador de Debian 10, donde establece que:

La red se configura de forma automática durante la instalación inicial. Si se instala Network Manager (que es generalmente el caso para instalaciones de escritorio completas), podría ocurrir que realmente no fuera necesaria ninguna configuración (...). Si se necesita una configuración (...) La mayoría de las redes modernas locales utilizan el protocolo Ethernet, en el que se dividen los

datos en pequeños bloques llamados tramas (...) y se transmite en el cable una trama a la vez. La velocidad de datos varía desde 10 Mb/s en tarjetas Ethernet antiguas hasta 10 Gb/s en las tarjetas más recientes (la tasa más común está creciendo actualmente de 100 Mb/s a 10 Gb/s). Los cables más utilizados son llamados 10BASE-T, 100BASE-T, 1000BASE-T, 10GBASE-T y 40GBASE-T, según el rendimiento que pueden proveer de forma confiable, estos cables finalizan en un conector RJ45.

Por otra parte, dentro de la configuración de la red encontramos una dirección IP, es un número utilizado para identificar una interfaz de red de un equipo en una red local o Internet. En la versión de IP más utilizada actualmente (IPv4) se codifica este número en 32 bits y generalmente se lo representa por 4 números separados por puntos (por ejemplo: 192.168.0.1), cada número entre 0 y 255 (inclusive, correspondiendo a 8 bits de datos). A su vez, cuentan con una máscara de subred (máscara de red) define en su código binario qué porción de una dirección IP corresponde a la red, el resto especifica el equipo. En el ejemplo de configuración de una dirección IPv4 estática dado, la máscara de red 255.255.255.0, indica que los primeros 24 bits de la dirección IP corresponden a la dirección de red y los otros 8 son específicos a la máquina.

Considerando lo planteado en el Manual, se refleja la aparición de 3 elementos principales dentro la configuración de una red LAN, cada uno encargado de controlar y regular la red dentro de sus propios parámetros. Pero, además existen otros elementos que conforman la configuración completada de una red que mediante la unión de los ya mencionado permiten formar una estabilidad en la configuración internet de la LAN. En el mismo manual, se estable también la existen de:

La dirección de red es una dirección IP en la que la parte que describe el número de equipo es 0. Generalmente se indica el rango de direcciones IPv4 en una red completa con la sintaxis “a.b.c.d/e” en el que “a.b.c.d” es la dirección de red y “e” es la cantidad de bits afectados por la parte de red en una dirección IP.

Un enrutador es una máquina que conecta varias redes entre sí. Se guía todo el tráfico a través de un enrutador a la red correcta. Para hacerlo, el enrutador analiza los paquetes entrantes y la redirección según su dirección IP de destino. Generalmente se conoce al enrutador como puerta de enlace, en esta configuración trabaja como una máquina que ayuda a alcanzar el exterior de la red local. Y, por último, la dirección especial de difusión conecta todas las estaciones en una red. Casi nunca es, sólo funciona en la red en cuestión. Específicamente, significa que un paquete de datos direccionado a difusión nunca pasará a través del enrutador.

Mediante estos elementos que conforman la configuración de una red, podemos llegar a asegurar de manera concreta el funcionamiento inicial de nuestra red LAN, donde cada proceso aginado y conectado a un cableado de red, logrará indicar los procesos o restricciones. Sin

embargo, dentro de las direcciones IP, existen dos elementos principales conocidos como protocolos que permiten conectar a los equipos a través del internet denominado TCP y UDP; cada una representa diversos servidores que permiten accesos dentro de la web.

2.2.5. Protocolos TCP y UDP

Martínez, A. (2021) menciona que:

Tanto TPC como UDP son protocolos utilizados para enviar bits de datos, conocidos como paquetes, a través de internet. Ambos construyen sobre el protocolo de internet (...), ya sea que esté enviando un paquete a través de TPC O UDP, ese paquete se envíe en una dirección IP. Estos paquetes se tratan de manera similar, ya que se reenvían desde su computadora a los enrutadores intermedios y al destino. Sin embargo, no son los únicos protocolos que funcionan sobre IP, aunque si son de los más utilizados. (...) sabiendo que la terminología correcta para cada protocolo es TCP / IP y UDP / IP.

- **TCP:** denominado como Protocolo de Control de Transmisión, es el protocolo más utilizado de internet (...) este garantiza que el destinario reciba los paquetes en orden numerándolos, mediante un remitente (...) si el remitente no recibe una respuesta correcta, reenvía los paquetes para asegurarse de que el destinario los haya recibido. Los paquetes también se comprueban a en buscar de errores.
- **UDP:**denominado como Protocolo de Datagramas de Usuario (...) permite que los paquetes se envíen al destinario (...) sin embargo, el destinario no espera asegurar que haya recibido el paquete; simplemente continuara enviando los siguientes paquetes (...) no hay garantía de que se estén recibiendo todos los paquetes y no hay manera de volver a pedir un paquete si lo pierde, pero perder todo este costo general significo que las computadoras se puedan comunicar más rápidamente.

Entonces, cada uno de estos protocolos brindará la labor de hacer llegar un paquete de datos en nuestra red, mediante la utilización del internet, por lo cual se debe considerar siempre tener estos elementos relacionados dentro de la infraestructura LAN. En pocas palabras, son los encargados de establecer estándares y políticas formales para ayudar al flujo de la información mediante los paquetes de datos.

2.2.6. La seguridad de datos en la red e implementación de servidores Proxy

Cuando se diseña una Red se debe tener en cuenta que mediante ella se origina un proceso de transmisión de información (datos), los cuales pueden llegar a representar una fuente de relevancia, para alguna organización; por esta razón, siempre se debe contar con una seguridad de datos dentro de nuestra Red, conocida como seguridad informática. Gómez, A. (2015: pág. 3) en su libro Seguridad Informática Básica, plantea que la seguridad de datos es:

Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema (...) para contemplar los procesos de seguridad informática se debe considerar los siguientes aspectos:

- Cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización.
- Control en el acceso a los servicios ofrecidos y a la información guardada por un sistema informático.
- Control en el acceso y utilización de ficheros protegidos por la ley.
- Identificación de los autores de la información o de los mensajes.
- Registro del uso de los servicios de un sistema informático.

Con lo cual, se sabe que fomentar una seguridad en la red permite lograr minimizar daños en un futuro en las organizaciones, ya sea mediante el resguardo de su información mediante políticas de seguridad, confidencialidad y resguardo físico de la red. Además, al aplicarse la seguridad informática dentro de una red LAN, se busca alcanzar los objetivos que logren beneficiar de manera directa a nuestra infraestructura de red. Gómez dictamina que los principales objetivos de la seguridad informática son:

- Mejorar la percepción y confianza de los clientes y usuarios en lo que respecta a la calidad del servicio.
- Cumplir la normativa sobre protección de datos.
- Preservar la confidencialidad de los datos y la privacidad de clientes y usuarios.
- Tener acceso a la información cuando se necesite y preservar la integridad de los datos.
- Minimizar el número de incidentes.
- Evitar interrupciones del servicio a causa de virus o ataques informáticos.

Contemplando lo planteado por el autor, dentro de la seguridad de información de una red, siempre se busca alcanzar una serie de procesos que brindarán un beneficio de control se seguridad dentro la red. Sin embargo, también se identifica la aparición de un elemento antes mencionado, el Servidor que en esta ocasión se presenta como fuente reguladora de la red; donde da asignaciones a los componentes de la misma, aplicando diversos parámetros de control y seguridad, explicados anteriormente en la configuración de las LAN. La Asociación Profesional de Ingenierías de Seguridad y Salud en las Obras de Construcción (ISSCO) explica que:

Un servidor de seguridad es un programa que protege tu computadora de intrusiones no deseadas. Si la computadora está conectada a una red o a Internet, es posible que alguien más (o que otra computadora) la “vea”, se

comunique con ella o incluso intente controlarla, por lo que los firewalls o servidores de seguridad funcionan como una especie de "pared" protectora entorno a la computadora.

Tomando en cuenta lo mencionado por ISSCO, este elemento se encarga de interactuar con otros equipos, componentes o redes externas. Entonces, la formación de este elemento (servidor), genera la clasificación de diversos tipos, conocidos como Servidores Proxy. Cada uno tendrá diferentes labores dentro de nuestra propia red, mediante necesidades que se encuentren al momento de gestionar la seguridad informática de la red, haciendo que se decante por algún tipo.

2.2.7. Servidores Proxy y Firewall Proxy

Borges, S. (2019) define que existen diversos tipos de servidores proxy, entre los cuales se encuentran:

- Servidor Proxy Web: se trata de un proxy basado en HTTP/HTTPS, donde el usuario accede a este servicio de la web, y desde allí puede usar el servidor proxy web intermediario para navegar por otras URLs. Así el usuario ingresa en el proxy web, indica la URL a donde quiere navegar, y el servidor proxy web devuelve el contenido.
- Servidor Proxy Transparente: un proxy transparente, también llamado proxy forzado, es un servidor que se encuentra como punto intermedio entre tu computadora en una red local, y el Internet. Lo que hace básicamente es tomar tu petición, y darle una redirección hacia el Internet sin modificar nada de ella. Por eso se le llama transparente, porque actúa como intermediario, pero no la modifica, es transparente.
- Servidor Proxy Cache: se trata de un servidor proxy que es utilizado como servidor intermedio entre una red y el Internet para cachear contenido, principalmente contenido de tipo estático como CSS, javascript, imágenes, vídeo o HTML. Esto permite acelerar el despacho de la información cuando los navegantes de la red acceden a Internet.
- Servidor Proxy Reverso o Reverse Proxy: un proxy reverso, o reverse proxy del inglés, es un tipo de servidor proxy que se usa para diferentes necesidades, entre las cuales se incluye: brindar acceso a Internet a usuarios de una red, balanceo de tráfico desde servidores web en el backend o proveer algún tipo de cache o despacho de ciertos archivos como lo son los estáticos.
- Servidor Proxy NAT: cuando hablamos de NAT proxy o proxy no-transparente, nos referimos a un servicio proxy que se usa principalmente para proteger la identidad de las verdaderas conexiones IP que acceden a Internet. Se usa de diferentes formas y con variadas configuraciones, pero la más típica y usada por los usuarios para tener anonimato es la llamada (...) es decir, realizar un enmascaramiento de las conexiones.

En estas circunstancias, para considerar un tipo de Servidor Proxy dentro de una LAN, dependerá de las necesidades internet que se vean reflejadas dentro de la misma, siempre entendiendo que su finalidad es ser una fuente de intercambio entre los equipos de trabajo y el servidor hacia el cual se desea entrar mediante el uso del internet, para así poder transferir información (datos), ya sea por la descarga o subido de archivos mediante los paquetes de datos. Pero, además, existe otro elemento que funciona como barrera física dentro de nuestra red, conocido como Firewall, empleado para diseño de redes privadas. CISCO define un firewall como:

Un dispositivo de seguridad de red que supervisa el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. (...) Los cortafuegos han sido la primera línea de defensa en la seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas seguras y controladas en las que se puede confiar y las redes externas que no son de confianza, como Internet. (...) Un firewall puede ser hardware, software o ambos.

Entonces, se dice que un Firewall funciona en teoría como una barrera física dentro de nuestra red, que permite intercomunicar al Servidor Proxy con los datos que desea buscar dentro de la Web, entonces dependiendo la formación podría llegar a clasificarse en un determinado tipo de Firewall, enfocados directamente para la infraestructura de red. Por este motivo, se dictaminan cinco (05) elementos. Pérez, A. (2022: párr.1) plantea en su blog que:

Hoy día existen muchos tipos de firewall diferentes entre los que elegir. Sin embargo, la mayoría de los responsables de seguridad de la información son conscientes de que proteger los datos simplemente construyendo un cortafuego alrededor de un sistema de información ya no es suficiente (...) se trata de un dispositivo que es capaz de permitir, limitar, cifrar y hasta decodificar el tráfico de comunicaciones entre un ordenador o red local e internet, impidiendo así que usuarios o sistemas no autorizados puedan tener acceso a ese ordenador o red local.

Por lo que se refiere a su funcionamiento, el cortafuego está programado para diferenciar entre las conexiones permitidas y las sospechosas, aplicando diferentes procedimientos en función de cómo califique a la conexión.

Los diferentes procedimientos pueden ser:

- **Políticas de cortafuegos:** suspendiendo las peticiones de comunicación que no provengan de la misma red o sistema, y disfrazando detrás de una IP los recursos internos.
- **Filtrado de contenido:** identifica los contenidos que pueden dar problemas, teniendo el usuario la última palabra sobre si se bloquea o no el acceso.
- **Servicios antimalware:** algunos cortafuegos pueden también detectar virus y evitar su expansión.

- **Servicios de DPI:** los procedimientos de Inspección Profunda de Paquetes añaden una segunda capa de seguridad al sistema, revisando en profundidad los paquetes de información que se reciben.

Entonces contar con un cortafuego dentro de nuestra Red va lograr permitir mantener una estabilidad a nivel seguridad, partiendo del hecho que necesita para generar una configuración estable dentro de la mismo. Además, se ve la necesidad que lograr definir la ubicación de cada equipo de trabajo dentro de Web, debido a que en ocasiones se necesita resguardar información suministrada, por lo cual el Firewall va a representen una barrera de enlace. Dependiendo del procedimiento a aplicarse de determinar un específico cortafuego para capa red. Otra vez Pérez plantea que:

Los firewalls de hoy necesitan tener una mayor visibilidad del tráfico que pasa por la red y permitir ver el flujo de contenido. En la actualidad, puede hablarse de cinco tipos de firewall, que son:

- **Cortafuegos de filtrado de paquetes:** se ocupa de tomar decisiones de procesamiento basadas en direcciones de red, puertos o protocolos. En general, son muy rápidos porque no hay mucha lógica detrás de las decisiones que toman. No hacen ninguna inspección interna del tráfico, ni tampoco almacenan ninguna información del estado.
- **Puerta de enlace a nivel de circuito:** (...) opera en la capa de transporte de los modelos de referencia de Internet u OSI y, como su nombre indica, implementa el filtrado a nivel de circuito en lugar del filtrado a nivel de paquete (...) comprueba la validez de las conexiones, es decir, circuitos, en la capa de transporte (generalmente conexiones TCP) contra una tabla de conexiones permitidas, antes de que se pueda abrir una sesión e intercambiar datos. Las reglas que definen una sesión válida prescriben y, una vez que se permite una sesión, no se realizan más verificaciones, ni siquiera a nivel de paquetes individuales.
- **Firewall de inspección con estado:** este es uno de los tipos de firewall capaces de realizar un seguimiento del estado de la conexión. Los puertos se pueden abrir y cerrar dinámicamente si es necesario para completar una transacción. Por ejemplo, cuando se realiza una conexión a un servidor utilizando HTTP, el servidor iniciará una nueva conexión al sistema en un puerto aleatorio. Un firewall de inspección con estado abrirá automáticamente un puerto para esta conexión de retorno. Habitualmente, se consideran más seguros que los de filtrado de paquetes, ya que procesan los datos de la capa de aplicación y, por ese motivo, pueden profundizar en la transacción para comprender lo que está sucediendo.
- **Puerta de enlace de nivel de aplicación (también conocido como firewall proxy):** Este tipo de firewalls operan en la capa de aplicación del modelo OSI, filtrando el acceso según las definiciones de la aplicación. Se considera como uno de los firewalls más seguros disponibles, debido a su capacidad para inspeccionar paquetes y garantizar que se ajusten a las especificaciones

de la aplicación. Dada la cantidad de información que se procesa, los firewalls de la puerta de enlace de aplicaciones pueden ser un poco más lentos.

- **Firewall de próxima generación:** Un cortafuego de próxima generación ofrece un filtrado de paquetes básico o una toma de decisiones basada en proxy dentro de las capas 3 y 4 del modelo OSI disponible dentro de los firewalls tradicionales y con estado. Sin embargo, amplía su protección al tomar también decisiones en la capa de aplicación (es decir, la capa 7). Las características que definen a este novedoso cortafuego son la identificación y control de aplicaciones, autenticación basada en el usuario, protección contra malware, protección contra exploits, filtrado de contenido (incluido el filtrado de URL) y control de acceso basado en la ubicación.

Contemplando la planteado por el autor, cada tipo de cortafuego se determinar dependiendo de los beneficios que busquen generarse mediante esta protección de datos dentro de red. Donde este proceso de lograría enfoca gracias a los objetivos que busquen lograrse dentro del organismo, ya sea para procesos de inspecciones o controles dentro del área de la infraestructura que conforma todos nuestros equipos de trabajo. Finalizando así, que la correcta configuración de una red está sustentada por diversos elementos que presenta relaciones entre sí, unidos mediante la conexión física dentro de la red o procesos lógicos programas dentro de la misma.

2.3. Bases Legales

2.3.1. Constitución De La República Bolivariana De Venezuela (publicada en Gaceta Oficial Extraordinaria N° 36.860, de fecha 30 de diciembre de 1999)

Art. 48.- Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso.

Analizando lo establecido en el artículo 48 de la Constitución De La República Bolivariana de Venezuela, se expresa primeramente que el Estado velará por la privacidad y seguridad de las comunicaciones privadas, las cuales no podrán ser interrumpidas bajo ningún aspecto por alguna persona o ente a excepción de un tribunal competente, el cual deberá cumplir con las disposiciones legales correspondientes para hacerlo y siempre manteniendo la confidencialidad.

Art. 110.- El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad

y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía.

Este artículo hace hincapié en el rol que tienen la ciencia, la tecnología y áreas afines en el desarrollo y avance del país en todos los aspectos, por lo tanto, el Estado proporcionara todos los recursos necesarios para seguir promoviendo estas actividades; así mismo, se resalta que el sector privado también debe aportar recursos para los mismos. Por último, es deber del Estado garantizar que se cumplan los principios éticos y legales que rigen este tipo de actividades, y es la Ley la que dicta como debe hacerse.

2.3.2. Ley Orgánica De Ciencia, Tecnología E Innovación (publicada en Gaceta Oficial Extraordinaria N° 37.291, de fecha 26de septiembre de 2001)

Art. 2.- Interés público. Las actividades científicas, tecnológicas, de innovación y sus aplicaciones son de interés público para el ejercicio de la soberanía nacional en todos los ámbitos de la sociedad y la cultura.

Dicho artículo hace referencia a todas aquellas actividades de índole científica, tecnológica y de innovación como piezas fundamentales para el buen desarrollo y ejecución de la soberanía en el país, dando a entender que, a través de su aplicación, los ciudadanos del territorio nacional serán capaces de lograr una mayor autoridad la cual es transferida a los gobernantes, quienes la ejercerán y harán del país un territorio independiente y rico en cuanto a avances tecnológicos.

Art. 19.- De la propiedad intelectual. La autoridad nacional con competencia en materia de ciencia, tecnología, innovación y sus aplicaciones, formulará las políticas y los programas donde se establecen las condiciones de la titularidad y la protección de los derechos de propiedad intelectual derivadas de las actividades científicas, tecnológicas y sus aplicaciones que se desarrolle con su recurso o los de sus órganos y entes adscritos conjuntamente con el Servicio Autónomo de Propiedad Intelectual (SAPI).

De acuerdo a lo señalado en el artículo 19, aquellos entes, organismos y demás autoridades relacionadas con el campo tecnológico y sus afines, están en su deber de establecer las normativas que amparen la titularidad de todos los documentos y/o proyectos que surjan de las

actividades tecnológicas, es decir, que dicha normativa le garantice a la persona que es el único autor de todas sus creaciones tecnológicas o innovadoras.

2.3.3. Ley Orgánica De Telecomunicaciones (publicada en Gaceta Oficial No. 36.920, de fecha 28 de marzo del año 2000)

Art. 1- Esta Ley tiene por objeto establecer el marco legal de regulación general de las telecomunicaciones, a fin de garantizar el derecho humano de las personas a la comunicación y a la realización de las actividades económicas de telecomunicaciones necesarias para lograrlo, sin más limitaciones que las derivadas de la Constitución y las leyes. Se excluye del objeto de esta Ley la regulación del contenido de las transmisiones y comunicaciones cursadas a través de los distintos medios de telecomunicaciones, la cual se regirá por las disposiciones constitucionales, legales y reglamentarias correspondientes.

Este artículo de la Ley Orgánica de Telecomunicaciones establece que dicha ley tiene como fin principal servir como un marco legal encargado de regular las actividades de telecomunicaciones, garantizando y asegurándose de que todos los ciudadanos gocen del derecho a la comunicación y de realizar las actividades económicas de telecomunicaciones que así requieran para tener acceso a la misma.

Art. 4.- Se entiende por telecomunicaciones toda transmisión, emisión o recepción de signo, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos, u otros medios electromagnéticos afines, inventados o por inventarse. Los reglamentos que desarrolle esta Ley podrán reconocer de manera específica otros medios o modalidades que pudiera surgir en el ámbito de las telecomunicaciones y que se encuadren en los parámetros de esta Ley.

Por otra parte, el artículo 4 de la misma ley da una breve definición de las telecomunicaciones, refiriéndose a esta como la transmisión de cualquier tipo de información a través de medios como hilos, radioelectricidad, medios ópticos y electromagnéticos afines. Igualmente, expresa que los reglamentos que conforman esta ley reconocerán cualquier otro medio que surja siempre y cuando cumplan con los parámetros de esta ley.

2.3.4. Ley Especial Sobre Delitos Informáticos (publicada en Gaceta Oficial No. 37.313, de fecha 30 de octubre del año 2001)

Art. 6.- Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

En cuanto a delitos informáticos se refiere, el artículo 6 deja en claro que todo aquel que, sin previa autorización o excediendo los límites que se le fueron establecidos, acceda o use indebidamente cualquier sistema que implemente tecnologías de información, será sancionado con una sentencia en prisión que oscila de uno a cinco años junto a una multa que puede ir de diez a cincuenta unidades tributarias.

Art. 7.- Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

En el mismo orden de ideas, el artículo 7 señala que todo aquel que cometa actos delictivos que arremetan con el normal funcionamiento de un sistema que utilice tecnologías de información o, lo use de manera indebida, será sancionado con una sentencia en prisión que puede ir de cuatro a ocho años junto a una multa que puede estar entre las cuatrocientas y ochocientas unidades tributarias.

Art. 11.- Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiera en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

Este artículo trata sobre el espionaje informático y establece que todo aquel que obtenga indebidamente información contenida en un sistema o difunda la misma, será sancionado con una

sentencia en prisión de cuatro a ochos años y una multa. Igualmente, aclara que dicha sentencia puede aumentar dependiendo de dos condiciones: si el delito cometido tiene como fin conseguir un beneficio, la sentencia aumentará de un tercio a la mitad; si la información filtrada atenta contra el Estado, las instituciones involucradas o las personas naturales o jurídicas, la sentencia aumentará de la mitad a dos tercios.

Art. 12.- Falsificación de documentos. El que, a través de cualquier medio, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad. El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

El artículo 12 manifiesta que todo aquel que altere o elimine un documento de un sistema o que gestione fraudulentamente los datos contenidos en el mismo, será sancionado con prisión de tres a seis años más una multa que puede ir de trescientas a seiscientas unidades tributarias. En caso de que la falta se haya cometido con el fin de obtener un beneficio, la sentencia aumentará entre un tercio y la mitad. Si la falta cometida arremete contra la integridad de alguien o algo, el aumento será de la mitad a dos tercios.

Art. 16.- Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. El que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penado con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias. En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Este artículo expresa que todo aquel que gestione fraudulentamente la información contenida en una tarjeta inteligente o en cualquier instrumento con los mismos fines; o quien de manera fraudulenta gestione la información de un sistema, será penado con prisión de cinco a diez años

junto a una multa de quinientas a mil unidades tributarias. Dicha sanción será aplicada para aquellos que actúen como intermediarios en actividades de comercialización de tarjetas inteligentes o de información contenida en ellas o en un sistema.

Art. 25.- Apropiación de propiedad intelectual. El que, sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

El artículo 25 contempla que, todo aquel que realice cualquier actividad con un software u obra sin la previa autorización de su autor original con el fin de obtener un beneficio económico, y que haya accedido fraudulentamente a cualquier sistema para la obtención del mismo, será sancionado con una sentencia en prisión de uno a cinco años más una multa de cien a quinientas unidades tributarias.

2.3.5. Ley de Infogobierno (publicada en Gaceta Oficial No. 40.274, de fecha 17 de octubre de 2013)

Art. 51.- El ente normalizador en materia de tecnologías de información y el órgano normalizador en seguridad de la información, ejercerán las funciones de unidades de apoyo especializadas de la Comisión Nacional de las Tecnologías de Información, en las materias de su competencia y de conformidad con las normas de funcionamiento dicte la Comisión.

El artículo 51 de la Ley de Infogobierno expresa que el o los entes con competencia en tecnológicas y seguridad de la información, servirán como organismos de apoyo para la Comisión Nacional de las Tecnologías de Información, trabajando en conjunto para llevar a cabo las actividades de su competencia y siempre siguiendo los lineamientos legales establecidos por la Comisión.

Art. 54.- La Superintendencia de Servicios de Certificación Electrónica, adscrita al Ministerio Del Poder Popular con competencia en materia en ciencia tecnologías e innovación, es el órgano competente en materia de seguridad informática, y es responsable del desarrollo, implementación, ejecución y seguimiento al Sistema Nacional de Seguridad Informática, a fin de resguardar la autenticidad, integridad, inviolabilidad y confiabilidad de los datos, información y documentos electrónicos obtenidos y generados por el Poder Público y por el Poder Popular, así como la generación de contenidos en la red.

El presente artículo manifiesta que, la Superintendencia de Servicios de Certificación Electrónica, órgano perteneciente al Ministerio del Poder Popular, es el ente con competencia en las actividades de seguridad informática y además, es el órgano rector del Sistema Nacional de Seguridad Informática, por lo tanto tiene la responsabilidad de gestionar los datos e información suministrados por dos poderes importantes: el Poder Público y el Poder Popular.

Art. 55.- La Superintendencia de Servicios de Certificación Electrónica tendrá, en el ámbito de aplicación de esta Ley, las siguientes competencias:

4. Articular e insertar en el Poder Público y en el Poder Popular las iniciativas que surjan inmateriales seguridad informática, dirigidas a la privacidad, protección de datos y de infraestructuras críticas, así como intervenir y dar respuesta ante los riesgos y amenazas que atenten contra la información que manejen.

9. Extraer, revisar y analizar las trazas y bitácoras de equipos y herramientas de redes.

Asimismo, el artículo 55 sigue haciendo referencia a la Superintendencia de Servicios de Certificación Electrónica, pero esta vez indicando las responsabilidades que se le atribuyen: en primer lugar, proponer iniciativas en relación a la seguridad informática en el Poder Público y Poder Popular, gestionar los riesgos y amenazas que atenten contra la información que manejan ambos poderes y, por último, gestionar la información de los equipos y herramientas de redes.

2.3.5. Ley Sobre el Derecho de Autor (publicada en Gaceta Oficial No. 4.638 Extraordinario, de fecha 1 de octubre de 1993)

Art. 2.- Se consideran comprendidas entre las obras del ingenio a que se refiere el artículo anterior, especialmente las siguientes: los libros, folletos y otros escritos literarios, artísticos y científicos, incluidos los programas de computación, así como su documentación técnica y manuales de uso; las conferencias , alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático -musicales, las obras coreográficas y pantomímicas cuyo movimiento escénico se haya fijado por escrito o en otra forma; las composiciones musicales con o sin palabras; las obras cinematográficas y demás obras audiovisuales expresadas por cualquier procedimiento; las obras de dibujo, pintura, arquitectura, grabado o litografía; las obras de arte aplicado, que no sean meros modelos y dibujos industriales; las ilustraciones y cartas geográficas; los planos, obras plásticas y croquis relativos a la geografía, a la topografía, a la arquitectura o a las ciencias; y, en fin, toda producción literaria, científica o artística susceptible de ser divulgada o publicada por cualquier medio o procedimiento.

Este artículo guarda estrecha relación con el artículo anterior, es decir, el artículo 25 ya que, en el presente artículo se presenta una lista detallada de todos los tipos de documentos, obras literarias y audiovisuales y demás proyectos que son susceptibles a ser damnificados bajo cualquiera de las actividades fraudulentas a las cuales se hacen referencia en el artículo 25.

Art. 67.- Salvo estipulación en contrario, la cesión del derecho de radiodifundir una obra o de comunicarla públicamente por cualquier otro medio de difusión inalámbrica de sonidos o imágenes, cubre la totalidad de las comunicaciones hechas por la empresa radiodifusora.

Por último, el artículo 67 da a entender que una vez que se le otorga o autoriza a cualquier empresa radiodifusora el derecho de difundir una obra, sea cualquiera de las mencionadas en el artículo 25, podrá publicarla a través de cualquier medio de difusión ya sea de audio, visual o ambos y de la manera que le resulte más oportuno; todo esto mientras no se estipule lo contrario y siempre que la empresa tenga la autorización del autor.

2.4.Definición de Términos

Ancho de Banda:

“Es la máxima cantidad de datos transmitidos a través de una conexión a Internet en cierta cantidad de tiempo”. (Verizon)

ARCNET:

Antigua red de área local para tener acceso a pasos de testigos. (Definición propia)

Base de datos:

“Es una recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema”. (Oracle Colombia)

Bits:

“Unidad de medida de información equivalente a la elección entre dos posibilidades igualmente probables”. (RAE)

Conector RJ45:

Conector físico de una red que permite unir equipos por protocolos de internet (Ethernet). (Definición propia)

Conectividad:

Capacidad de conectarse o hacer conexiones. (RAE)

Cisco:

“Empresa de origen estadounidense fabricante de dispositivos para redes locales y externa, también presta el servicio de soluciones de red”. (Netec Global Knowlegde)

Dato:

“Información dispuesta de manera adecuada para su tratamiento por una computadora”. (RAE)

Enrutador:

“Dispositivo que conecta dos o más redes o subredes de conmutación de paquetes. Cumple dos funciones principales: gestionar el tráfico entre estas redes mediante el reenvío de paquetes de datos a sus direcciones IP previstas”. (Cloudflare)

Ethernet:

“Modalidad de acceso al servicio de transmisión de datos a través de la cual se ofrece al usuario una capacidad de transmisión extremo a extremo entre dos puntos geográficos y que puede soportar cualquier protocolo mediante el empleo de los equipos terminales adecuados”. (Diccionario panhispánico del español jurídico)

Flujo de red:

Proceso de comunicación entre dos puntos de las redes contempladas por diversas limitaciones siempre que suceda un inicio y cierre de sesión dentro de la red. (Definición propia)

Hardware

“Conjunto de los componentes que integran la parte material de una computadora u ordenador”. (RAE)

Latencia:

“Tiempo que tarda un paquete en llegar del remitente al receptor. Por supuesto, cuanta más demora, más lenta “parece” la red. La latencia generalmente se mide en milisegundos (ms)”. (Cisco)

Telecomunicaciones:

“Transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos”. (RAE)

Token Ring:

“Topología de red de área local (LAN) que envía datos en una dirección a través de un número de ubicaciones especificado utilizando un testigo. El testigo es el símbolo de autorización para el control de la línea de transmisión”. (IBM)

Paquete de Datos:

“Conjunto mínimo de datos en que se divide la información para ser transmitida a través de internet”. (RAE)

Red:

“Es la interconexión física o inalámbrica que vincula varios dispositivos informáticos (servidores, computadoras, teléfonos móviles, periféricos, entre otros) para que se comuniquen entre sí, con la finalidad de compartir datos y ofrecer servicios”. (Cisco)

Software:

“Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora”. (RAE)

Web:

“Documento electrónico que puede contener cualquier tipo de contenido (texto, sonido, vídeo, programas, enlaces, imágenes, etc.), desarrollado mediante un lenguaje de programación, generalmente el HTML, y que puede ser interpretado por un navegador”. (RAE)

PARTE III

DESCRIPCIÓN METODOLÓGICA

Balestrini, M. (2006:126) define la descripción metodológica como: “(...) la instancia referida a los métodos, las diversas reglas, registros, técnicas y protocolos, con los cuales una teoría y su método calculan las magnitudes de lo real”. Este apartado tiene como finalidad describir metódicamente todos los procedimientos y técnicas que son empleados para el logro de los objetivos de la investigación.

3.1. Naturaleza de la investigación

En cuanto a la investigación cuantitativa, Raffino (2020: párr. 3), explica que “es aquella que emplea magnitudes numéricas para expresar su trabajo, mediante técnicas experimentales o estadísticas, cuyos resultados son representables luego matemáticamente. Su nombre proviene de cantidad o cuantificación, o sea, numeración”. Por lo cual, el presente trabajo de investigación está basado en el modelo cuantitativo, ya que se recopila datos para su posterior análisis permitiendo enfocar los conocimientos hacia los objetos de la investigación.

3.1.1. Tipo de investigación

El tipo de investigación está vinculado al nivel de profundidad de los objetivos, por lo que, el presente trabajo de investigación se enmarca como proyecto factible. Balestrini, M (2006:12) plantea que los proyectos factibles son: “aquellos proyectos o investigaciones que proponen la formulación de modelos, sistemas entre otros, que dan soluciones a una realidad o problemática real planteada, la cual fue sometida con anterioridad o estudios de las necesidades a satisfacer”. Por consiguiente, se busca analizar las variables presentes en el lugar de los hechos con el fin de alcanzar una solución idónea para el fenómeno estudiado; en este caso en concreto, un nuevo diseño de la red de área local de la Contraloría Municipal del Municipio Antolín del Campo.

3.1.2. Diseño de la investigación

El diseño de la investigación, según Hernández et al (2010) “se refiere a dónde y cuándo se recopila la información”. En este caso se utilizará la investigación de campo debido a que se investigará directamente en el lugar donde sucede el fenómeno. Arias, F. (2012:29), define la investigación de campo como: “(...) aquella que consiste en la recolección de todos directamente

de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variables algunas, es decir, el investigador obtiene la información, pero no altera los sus resultados”. De allí su carácter de investigación no experimental.

3.1.3. Población y Muestra

Arias, F. (2012:86) define población como aquel: “conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Esta queda delimitada por el problema y los objetivos del estudio”. Toda investigación requiere obtener y procesar datos aportados por: personas, objetos, empresas u otro elemento que estén involucrados en el objeto de estudio, para de esta manera se pueda dar veracidad al objetivo planteado o inferir un efecto sobre la totalidad del conjunto, éste debe estar definido, limitado y se conoce como la población del estudio, según su magnitud se define un subconjunto con las características propias de la población y se habla entonces de una muestra.

La población para efecto de esta investigación está representada por las personas que trabajan en la Contraloría Municipal de Antolín del Campo ubicado en la Isla de Margarita en el sector Loma de Guerra, Municipio Antolín del Campo, clasificadas por siete (07) direcciones de trabajos que determinan su desempeño en el organismo, donde en conjunto congregan una cantidad de veintitrés (23) personas. Para el estudio de esta problemática se consideran a aquellas personas que interactúen directamente con la red a diseñar, excluyendo intencionalmente al personal ambientalista. Por otra parte, debido a que la institución utiliza un personal de soporte técnico externo este será incluido dentro de la población, por lo cual; nuestra la población total es de veinticuatro (24) personas.

A pesar de que la población objetivo de la presente investigación es finita y conocida, se contempla el uso de una muestra, que, de acuerdo con Arias, F. (2006: 83), representa: “un subconjunto representativo y finito que se extrae de la población accesible”. Lo anterior debido a que permite agilizar el proceso investigativo, enfocándolo principalmente en el análisis de los datos obtenidos del personal anteriormente mencionado; además de reducir los gastos y agilizar el tiempo de implementación de las técnicas de recolección de datos.

Por este motivo de accesibilidad y facilidad, se enfoca en un modelo de muestreo no probabilístico que permita recopilar datos específicos de ciertos individuos del objeto de estudio, que guarde relación con los objetos de la investigación. Por consiguiente, se implementa un muestreo por conveniencia, el cual es definido por McMillan, J. y Schumacher, S. (2005), como:

“un método no probabilístico de seleccionar sujetos que están accesibles o disponibles”. Considerando lo citado, este tipo de muestreo va a permitir extraer información del fenómeno estudiado dependiendo de las necesidades que tenga el investigador. Para la presente investigación, se toma como muestra a los jefes de cada dirección, incluyendo a la Contralorajefa, dando un total inicial de siete (07) personas, además se anexa a la muestra al encargado del soporte técnico externo; representando así, un tamaño de muestra final de ocho (08) personas en total.

3.2. Técnica de recolección de datos

En relación a las técnicas de recolección de datos, Arias, F. (2006:146) expone que éstas son las “distintas formas o maneras de obtener la información”; siendo estas técnicas, mecanismos que van a permitir recopilar todos los datos del fenómeno a estudiar. De acuerdo a los objetivos del tema de investigación, se contempló implementar como técnicas de recolección de datos, en primer lugar, la observación participante, puesto que permite conocer de manera eficiente el manejo de la infraestructura de red de la Contraloría Municipal. En este sentido, Taylor, S y Bogdan, R. (2000:31) definen como observación participante a aquella que: “involucra la interacción social entre el investigador y los informantes en el ambiente (...) durante la cual se recogen datos de modo sistemático y no intrusivo.”. Por ende, este tipo de observación logra ampliar el conocimiento de los investigadores acerca de los hechos que podrían llegar a suceder dentro del campo de trabajo.

Asimismo, se tomaron en cuenta las entrevistas formales las cuales se realizarán a la muestra de ocho (08) personas que trabajan en la Contraloría Municipal de Antolín del Campo. Así pues, Rodríguez, D. (2019: párr.: 1) define la entrevista formal como: “una técnica cuyo objetivo es recolectar u obtener información (...) son estrategias utilizadas cuando la información debe obtenerse preferiblemente de la fuente directa (...) los entrevistados serán los protagonistas de la situación a estudiar”. Por este motivo, se utilizará este tipo de entrevista debido a que permite involucrar de manera directa al sujeto o persona que participa del fenómeno a estudiar.

En cada entrevista, las preguntas serán de forma abierta y cerrada con la intención de generar un ambiente de confianza y poder recopilar información relevante y necesaria para su posterior análisis; debido a que los entrevistados forman parte de las fuentes primarias de información para obtener los requisitos para el diseño de la LAN, complementando sus inquietudes y observaciones sobre las fallas que identifican en la organización referente a la temática de estudio.

Por último, a las demás técnicas de recolección se une la revisión documental. Hurtado, J. (2008) explica que ésta:

Es una técnica en donde se recolecta información escrita sobre un determinado tema, teniendo como fin proporcionar variables que se relacionan indirectamente o directamente con el tema establecido, vinculando esta relaciones, posturas o etapas, en donde se observe el estado actual de conocimiento sobre ese fenómeno o problemática existente

Por consiguiente, resulta de mucha ayuda al momento de investigar más a fondo sobre la problemática que se está estudiando. Como lo indica su nombre, mediante la revisión documental, los investigadores podrán revisar documentos de la empresa que les brinden datos relevantes que se complementen con la información obtenida a través de la observación y las entrevistas, así como bibliografía especializada en relación al objeto de estudiado.

3.3. Técnicas de análisis de datos

Arias, F.(2004)expresa que “en este punto se describen las distintas operaciones a las que serán sometidos los datos que se obtengan”. Esto quiere decir que las técnicas de análisis permitirán a los investigadores estudiar y descomponer la información obtenida a través de las técnicas de recolección seleccionadas anteriormente. Dicho esto, se escogieron como técnicas de análisis, primeramente, el cuadro descriptivo, el cual López, M. (s/f) lo define como: “herramientas gráficas que se usan para resumir la información y hacer que las personas puedan comprenderla de una manera mejor y más simple” siendo entonces una herramienta muy útil ya que permite a los investigadores organizar y resumir de manera práctica la información que se vaya recolectando, tomando nota de los puntos más relevantes y así facilitar su comprensión y posterior estudio.

También se consideró el análisisFODA,de manera que se pueda llevar a cabo un análisis de las condiciones actuales de trabajo y la red de la institución. Según Koontz, H. y Weichrich, H. (2004) la finalidad de la matriz FODA es “obligar a los líderes a analizar la situación de su organización y a plantear estrategias, tácticas y acciones, para el logro eficaz y eficiente de los objetivos organizacionales”. Por lo tanto, mediante esta técnica, una vez realizado el análisis por parte de los investigadores, se pondrá en marcha un plan para plantear posibles soluciones a la situación de la empresa que ayuden a optimizar su red local.

Asimismo, se incorpora a este grupo el croquis. Fernández, L. (s/f: párr. 1) se refiere al croquis como: “un boceto, diseño o dibujo simplificado que se hace con herramientas artísticas o

de diseño y que reproduce un modelo proveniente de la naturaleza, de la imaginación o de una perspectiva específica del mundo real”. Gracias a esta técnica, los investigadores podrán realizar un boceto del nuevo sistema de red para la Contraloría Municipal de Antolín del Campo, en el cual se detallará como irán ubicados los equipos que conformarán la nueva red LAN a proponer. En este mismo orden de ideas, se escoge el diagrama de red, que es definido por Lucidchart. (2022: 1) como “una representación visual de una red de computadoras o telecomunicaciones. Muestra los componentes que conforman una red y cómo interactúan, incluidos enrutadores, dispositivos, Hubs, cortafuegos, etc.”. A diferencia del croquis, el diagrama de red se implementará como un boceto en el cual se indicará gráficamente que equipos formarán parte de la red LAN, su conexión y configuración lógica.

Por último, se plantea el análisis de contenido, el cual Hernández, R, Fernández, C y Baptista, P. (2003) define como “es una técnica de procesamiento de cualquier tipo de información acumulada en categorías codificadas de variables que permitan el análisis del problema motivo de la investigación”. A través de esta técnica, los investigadores podrán realizar un análisis sistemático de la información recopilada.

PARTE IV

ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

El análisis y presentación de resultados según Hurtado, J (2008) “son técnicas e interpretación de los resultados según Hurtado (2010), “Son las técnicas de análisis que se ocupan de relacionar, interpretar y buscar significado a la información expresada en códigos verbales e icónicos”. Logrando así, adquirir un diagnóstico e interpretación de los resultados conseguidos mediante la implementación de las técnicas de recolección de datos. Ayudando al investigador comprender los procedimientos y actividades que permitan obtener la información necesaria para dar solución al fenómeno estudiado.

4.1. Estado actual de la infraestructura de red de la Contraloría del Municipio Antolín del Campo

Se realizó una visita a la Contraloría Municipal del Municipio Antolín del Campo, ubicada en la Calle Los Robles, de la población de Paraguachí, del mencionado municipio, donde se aplicó la técnica de observación para conocer la situación actual de la infraestructura de la red interna de la institución antes mencionada; con el fin de poder identificar de manera exhaustiva aquellos fenómenos que de alguna forma pudiesen estar causando fallas dentro de dicha red.

La Contraloría del Municipio Antolín del Campo es un organismo regulador conformado por diversos departamentos encargados de ejercer control administrativo-económico sobre la Alcaldía de dicho municipio; por lo que, maneja información relacionada con listados de controles de presupuestos anuales, así como normativas de regulaciones económicas para la aplicación de nuevos proyectos que garanticen la administración de manera segura y confiable de los presupuestos otorgados por el Estado.



Figura 1. Ubicación de la Contraloría Municipal de Antolín del Campo.

Fuente: Google Maps (2022).

Por otra parte, la Contraloría cumple funciones desligadas ala Alcaldía, puesto que se conforma en una institución autónoma e independiente dentro del sistema gubernamental del Estado venezolano. Por consiguiente, se encarga de aplicar medidas de control y auditoría para la ejecución de nuevos proyectos en su jornada anual de trabajo; determinando listados de nómina, pagos de transacciones bancarias, registro de los impuestos, regulación de medidas de control para gastos internos y, además, un proceso de autorización de presupuestos que deben regirse por los lineamientos emanados por las normativas estatales.

A nivel físico, la sede de la Contraloría está constituida por una casa de dos plantas, donde la planta baja posee un espacio físico con una medida de noventa y cinco con nueve (95,9) metros cuadrados y la planta alta cuenta con un espacio total de ochenta y cuatro con ciento veintiocho (84,128) metros cuadrados; ambas plantas alojan cuatro (4) departamentos administrativos, algunos en zonas cerradas e independientes para cada uno de ellos, mientras que otros comparten espacios.

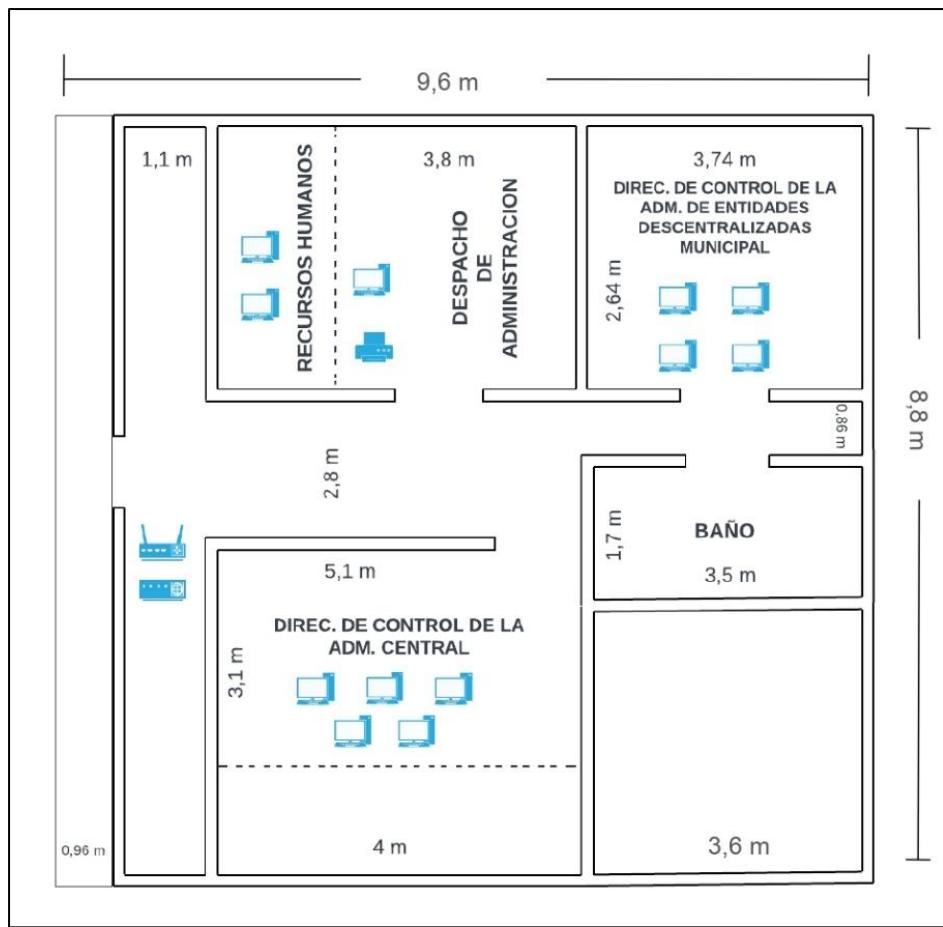


Figura 2. Planta Alta de la Contraloría del Municipio de Antolín del Campo.

Fuente: Elaboración Propia. (2022)

En referencia a la planta alta (ver **figura 2**), se aprecia que se constituyen en zonas cerradas e independientes las oficinas de Dirección de Control de la Administración de Entidades Descentralizadas Municipal y la de Dirección de Control de la Administración Central. Por su parte, los departamentos de Recursos Humanos y Despacho de Administración se encuentran unidos en un mismo espacio. Por último, en esta misma planta se encuentra un espacio sin resguardar donde están colocados los equipos de red destinados a suprir el servicio de internet para toda la institución.

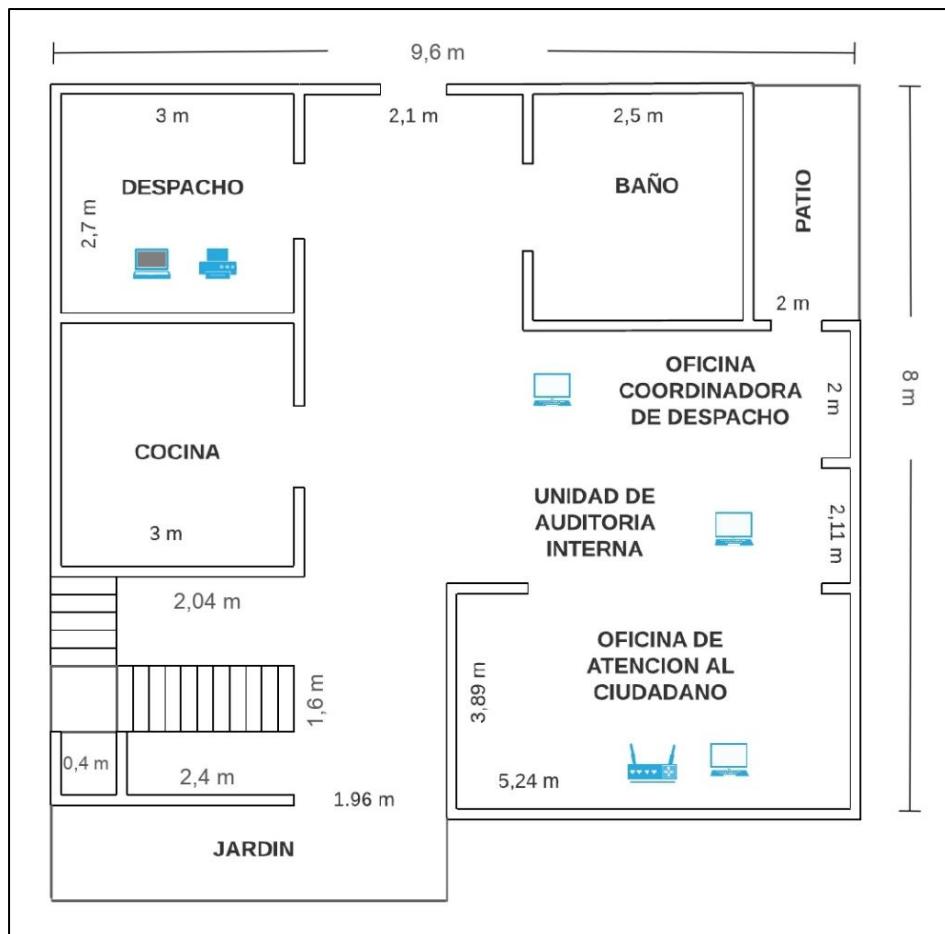


Figura 3. Planta Baja de la Contraloría del Municipio de Antolín del Campo.

Fuente: Elaboración Propia. (2022)

De la misma manera, la planta baja (ver **figura 3**) de la contraloría alberga otros cuatro (4) departamentos administrativos, distribuidos de la siguiente manera: tres (3) de ellos se encuentran en una sala compartida, estos son la Oficina Coordinadora de Despacho, la Unidad de Auditoría Interna y la Oficina de Atención al Ciudadano, y solo el despacho del Contralor/a del organismo se encuentra en un espacio cerrado. Además, esta planta también cuenta con un espacio desprotegido donde están ubicados los equipos de red que brindan conexión de internet a los departamentos mencionados con anterioridad.

En relación a los dispositivos informáticos empleados para llevar a cabo las actividades dentro de la contraloría, se constató que poseen quince (15) computadoras de escritorio y una (01) computadora portátil (tipo laptop) completamente funcionales. Estos equipos informáticos (computadoras/portátil) ubicados en los pisos de la Contraloría se les encuentran asignados una antena WiFi mediante un dispositivo USB TP-Link, que les permite captar la señal digital

proveniente de una red Wifi. Además, cuentan con dos (2) impresoras de red conectadas por cableado USB Hp de 1,5 metros de longitud unidas hacia un solo equipo, es decir, no hay disponibilidad para que otros equipos puedan llegar a acceder a sus funciones. Sin embargo, este dispositivo tiene una capacidad de concurrencia máxima de cinco (5) dispositivos.

En cuanto a la distribución física de la red, está representada por conexión inalámbrica (WiFi) por lo cual, no se posee directamente una segmentación física con cableado de la red, sino que está dividida y agrupada por zonas para establecer conectividad en todas las áreas que conforman la Contraloría. A nivel de conectividad, para que los equipos informáticos tengan acceso hacia internet, la Contraloría cuenta con un ISP que se encarga de proveer un servicio para la red actual mediante un cable dieléctrico.



Figura 4. Entrada del Cableado Coaxial por parte del ISP de la Contraloría.

Fuente: Elaboración Propia. (2022).

El proceso de traslado del cableado proveniente del ISP comienza desde un poste de electricidad ubicado al frente del organismo (ver **figura 4**), desde el cual sale una conexión por cable dieléctrico de cinco con treinta cinco (5,35) metros de longitud, por el cual se transmite la señal analógica proveniente del proveedor de internet hacia la Contraloría. Cabe destacar, que este cable pasa por el patio de la planta alta de la Contraloría entrando a la zona interna de la misma mediante una ventana.



Figura 5. Conexión del servicio del ISP a los equipos de red de la Planta Alta de la Contraloría.

Fuente: Elaboración Propia. (2022)

Una vez el cable dieléctrico entra a la planta alta de la Contraloría, se conecta a un módem Motorola por un único puerto de entrada físico, que permite convertir señal analógica a digital; este dispositivo tiene capacidades de trabajo elevadas, es decir, puede llegar a manejar velocidades entre los 10-100 Mbps. Luego de establecer esa primera conexión, se distribuye un cable de red Ethernet UTP de categoría 5 para interior de treinta (30) cm de longitud para servir de puente físico con el dispositivo router TP-Link (ver **figura 5**), que permite distribuir la señal WiFi hacia todos los equipos informáticos de la red ubicados en la planta alta de la Contraloría. Por otra parte, este router funciona como host debido a que representa un punto de acceso que permite establecer conexión a los servicios del ISP para los dispositivos informáticos de la planta baja.

Sin embargo, el estado actual de los cables (coaxial/ethernet) con los que cuenta la Contraloría no son los óptimos para los servicios que proporcionan los equipos de red que interconectan (ver **figura 5**), debido a que no se encuentran protegidos contra fenómenos o accidentes que puedan ocurrir en las jornadas de trabajo. Además, no cuentan con un sistema de aislamiento que evite el ruido que puedan llegar a causar ciertos equipos eléctricos mediante su vibración. De igual forma, debido a su mala ubicación dentro de la zona de trabajo, esto puede llegar a generar niveles de interferencia debido a que señales digitales transportadas por el aire pueden rebotar en algún metal pesado que se encuentra en el lugar. Así mismo, los equipos que conforman la red de la planta alta (modem/router) no cuentan con una zona segura para su resguardo (ver **figura 5**), sino

que están ubicados en zonas abiertas donde pueden llegar a ocurrir accidentes, lo que puede terminar deviniendo en desconexiones dentro del sistema de los equipos de red.

Además, el modelo del equipo (router) no es adecuado para las metodologías de trabajo que se cuenta actualmente en la Institución, debido que a pesar que puede llegar a manejar velocidad de 600 Mbps con frecuencia de 2,4 GHz, los estándares de servicio que abarca son de 802.11n conocido como Wifi 4, el cual no es acorde para la cantidad de equipos informáticos con los que cuenta actualmente la Contraloría y que acceden a los servicios que proporciona dicho dispositivo de red, puesto que el mismo solo puede garantizar la estabilidad en la red para un nivel máximo de concurrencia de ocho (8) equipos.

Como se dejó entrever en párrafos anteriores, el router de la planta alta de la Contraloría, sirve como host para conectar a la red al Router TP-Link ubicado en la planta baja, el cual funciona como un amplificador de señal para proporcionar una señal inalámbrica a la cual puedan conectarse los equipos informáticos de la planta; proporcionando de esta manera conectividad hacia el ISP. Sin embargo, este equipo presenta las mismas características de estándar que el modelo anterior, pero se destaca una discrepancia en la velocidad que puede llegar a manejar, debido a que existen un desnivel de características; dado que maneja velocidad de 350 Mbps con una frecuencia de 2,4 GH, impidiendo establecer un ancho de banda igual o similar al del equipo central.

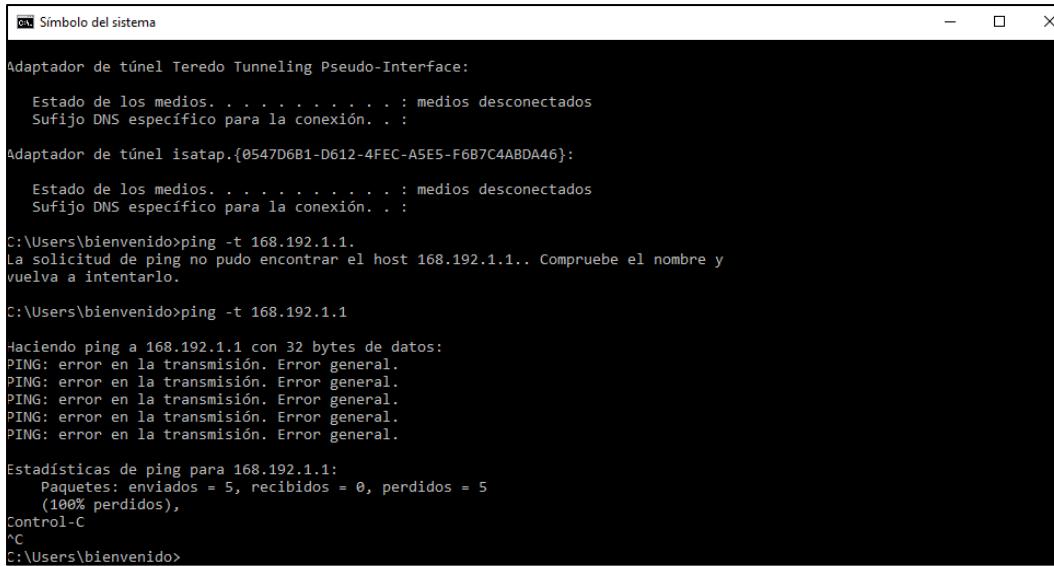


Figura 6. Router Amplificar de la plata baja.

Fuente: Elaboración Propio. (2022)

Además, este elemento (Router amplificador) tampoco cuenta con una zona segura para su protección e incluso se encuentra más expuesto que el host principal(**ver figura 5 y 6**), debido a que está ubicado al lado de una oficina de trabajo en una zona abierta al público. Además, se logra observar que no está ubicado en un estante o armariosólido para su estabilidad física, sino que está ubicado encima de una caja, siendo un peligro para el equipo ya que podría llegar a ocurrir algún tropiezo con algún personal de trabajo de la Contraloría, llegando así a ocasionar daños dentro del equipo.

Por estas razones, se realizaron en los equipos administrativos pruebas de testeo para establecer un diagnóstico de los estados de conexión dentro de la red (**ver figura 7**). Además, mediante estas pruebas se logró examinar los niveles de velocidad que maneja la red inalámbrica actual de la Contraloría en conjunto con las características del control de versión de direccionamiento IP que cuenta la red(**ver figura 8**).



The screenshot shows a Windows Command Prompt window titled "Símbolo del sistema". The command entered was "ping -t 168.192.1.1". The output indicates that the host could not be found, and the ping failed due to general errors. The statistics show 5 sent, 0 received, and 5 lost packets (100% loss).

```
Símbolo del sistema

Adaptador de túnel Teredo Tunneling Pseudo-Interface:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . .

Adaptador de túnel isatap.{0547D6B1-D612-4FEC-A5E5-F6B7C4ABDA46}:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . .

C:\Users\bienvenido>ping -t 168.192.1.1
La solicitud de ping no pudo encontrar el host 168.192.1.1.. Compruebe el nombre y vuelva a intentarlo.

C:\Users\bienvenido>ping -t 168.192.1.1

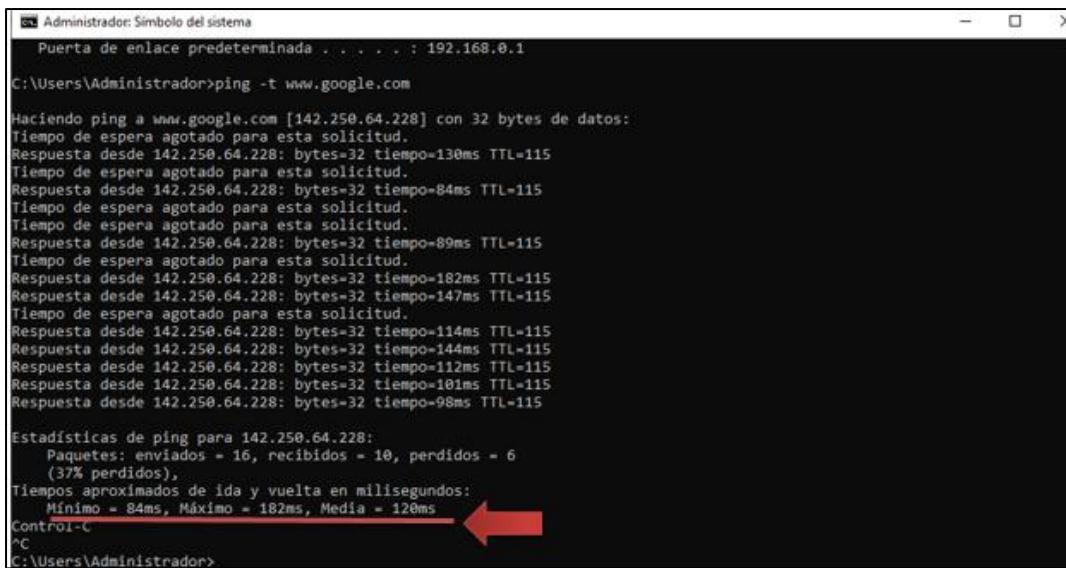
Haciendo ping a 168.192.1.1 con 32 bytes de datos:
PING: error en la transmisión. Error general.

Estadísticas de ping para 168.192.1.1:
  Paquetes: enviados = 5, recibidos = 0, perdidos = 5
              (100% perdidos),
Control-C
^C
C:\Users\bienvenido>
```

Figura 7. Diagnóstico al equipo informático (Laptop) de la Contraloría Municipal de Antolín del Campo.

Fuente: Elaboración Propia. (2022)

En relación con el estado de conexión entre equipos de la red (**ver figura 7**), se realizó un diagnóstico de prueba al equipo portátil ubicado en el despacho de la Contralora para corroborar la petición de paquetes hacia el Host principal (Router) de la planta alta de la Contraloría para determinar si existe conectividad con este elemento. El diagnóstico indicó que ocurre una falla para encontrar el servicio de direccionamiento, causando así una perdida en el envío de paquetes de un 100% debido a que no existen una conexión directa entre estos equipos, es decir, no hay registro de IP dentro host que permita el acceso del portátil hacia router de la planta alta. Además, la petición de servicio se realizó desde el equipo central del Contraloría el cual debería tener acceso directo hacia el Host.



```
Administrator: Símbolo del sistema
Puerta de enlace predeterminada . . . . : 192.168.0.1
C:\Users\Administrador>ping -t www.google.com

Haciendo ping a www.google.com [142.250.64.228] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Respueta desde 142.250.64.228: bytes=32 tiempo=130ms TTL=115
Tiempo de espera agotado para esta solicitud.
Respueta desde 142.250.64.228: bytes=32 tiempo=84ms TTL=115
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respueta desde 142.250.64.228: bytes=32 tiempo=89ms TTL=115
Tiempo de espera agotado para esta solicitud.
Respueta desde 142.250.64.228: bytes=32 tiempo=182ms TTL=115
Respueta desde 142.250.64.228: bytes=32 tiempo=147ms TTL=115
Tiempo de espera agotado para esta solicitud.
Respueta desde 142.250.64.228: bytes=32 tiempo=114ms TTL=115
Respueta desde 142.250.64.228: bytes=32 tiempo=144ms TTL=115
Respueta desde 142.250.64.228: bytes=32 tiempo=112ms TTL=115
Respueta desde 142.250.64.228: bytes=32 tiempo=101ms TTL=115
Respueta desde 142.250.64.228: bytes=32 tiempo=98ms TTL=115

Estadísticas de ping para 142.250.64.228:
Paquetes: enviados = 16, recibidos = 10, perdidos = 6
(37% perdidos).
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 84ms, Máximo = 182ms, Media = 120ms
Control-C
^C
C:\Users\Administrador>
```

Figura 8. Prueba de velocidad del equipo administrador de la Contraloría.

Fuente: Elaboración Propia. (2022)

De la misma manera para determinar las velocidades que maneja actualmente la red, se realizó unas pruebas de testeo del equipo administrativo (PC) (**ver figura 8**) ubicado en la oficina de Coordinación de Despacho, donde se implementó un ping de carga para enviar una solicitud de acceso hacia los servicios de google.com que logró determinar si velocidad promedios del equipo se mantiene en los estándares óptimos de una red WiFi al momento de estresas las salidas de peticiones.

Dando como resultado que el equipo presenta variaciones de velocidad (latencia) en milisegundos al momento de dirigirse al servicio antes mencionados presentando un registro mínimo de velocidad de ochenta y ocho (84) ms y un máximo de ciento ochenta y dos (182) ms para así generar un promedio final de ciento veinte (120) ms totales para una asignación de pedidos de dieciséis (16) ping (**ver figura 8**), lo que genera como resultado final que la velocidad que presenta la red no es adecuada debido que tiene picos muy variables en los tiempos de respuestas, siendo así una de las razones por las cuales existen diversas de latencias en cada departamento que conforma la actual red WiFi.

Por otra parte, estos diagnósticos realizados permitieron visualizar las versiones de direccionamiento IP de la actual red mediante la revisión del host central, lo que ayudó a verificar si existe algún procedimiento de configuración o control de tráfico de paquetes dentro de la red. Asimismo, se logró reflejar la ruta de enlace lógica del servicio brindado por el proveedor de internet para acceder a sus servicios.

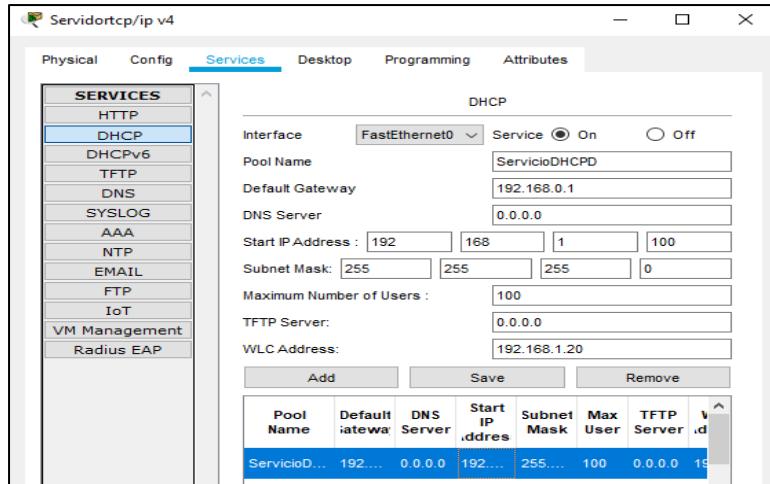


Figura 9. Configuración del host central (servicio DHCP) de la red actual.

Fuente: Elaboración Propia. (2022)

En la **figura 9**, se logra observar la configuración establecida del host central, el cual no presenta con servidores de control de IP (IPCP), sino que está conformada mediante un protocolo TCP/IP V4 mediante un servicio de dirección de asignación dinámica DHCP/V4 con un límite de cien (100) usuarios, regulada desde la dirección principal 198.168.0.0 y bajo una máscara de red de capa 24. Este host principal presenta una funcionalidad de controlador de la Red Inalámbrica (WLC) con dirección IP 192.168.1.20 lo que permite generar puntos de control de acceso que ayuden a establecer dirección de IP dinámicas a los equipos administrativos, estos servicios vienen iniciados por un Gateway único de IP 198.168.0.1/24 que permite enlazar los dispositivos hacia el ISP.

Sin embargo, a pesar de que cuenta con una configuración que se puede considerar estable, el no contar con control de IP pueda llegar a generar pérdidas con las asignaciones de direccionamiento dinámico en los equipos que generaría retraso en las peticiones de acceso. Además, debido a que todos los equipos administrativos presentan direcciones dinámicas no se logra establecer control de acceso dado a que no se ubicar de directa la IP en algún servicio en el interno o de la red, siendo así una de las desventajas de estas infraestructuras de redes.

Por otra parte, la Contraloría cuenta con servidor local de nómina ubicado en la planta alta de la Contraloría específicamente en el departamento de Administración Central, el cual cuenta con una capacidad cuatro (4) Gb memoria RAM con ocho (8) slots de memoria para una posible expansión, además tiene instalado un disco 500 SSD donde actualmente cuenta con una capacidad en uso de 49%.

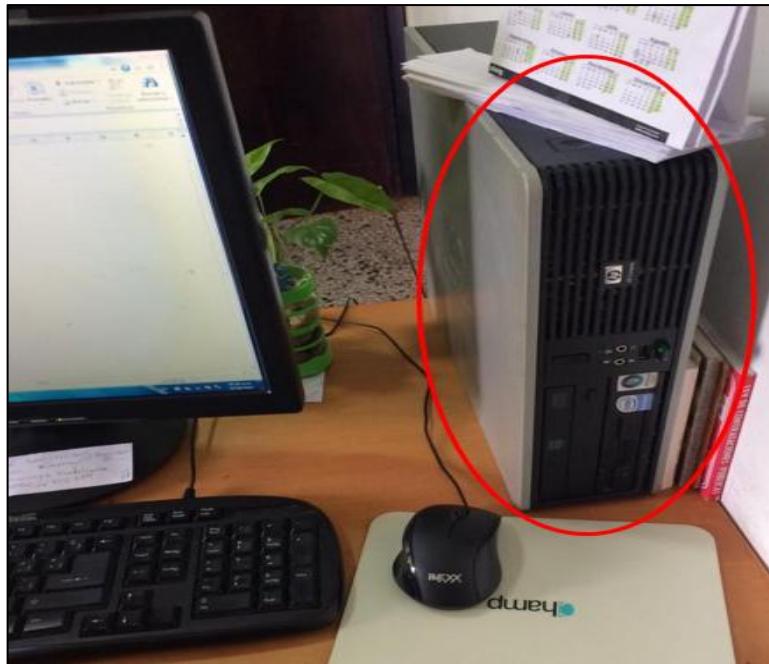


Figura 10. Servidor local de Nómina de la Contraloría.

Fuente: Elaboración Propia. (2022)

Este servidor sirve como herramienta para realizar labores de transacciones bancarias, llenado de nómina y registro de documentaciones legales previamente almacenadas, manejado mediante la funcionalidad de direccionamiento web en el servicio de internet mediante un servicio registro de dominio (DNS) que permite agilizar los procesos de conexiones hacia el mismo. Se logró determinar que este servidor (**ver figura 10**) no cuenta con un proceso de restricción de acceso para los usuarios, esto quiere decir, que todos equipos pueden tener conexión directa hacia el dominio del servidor lo que podría llegar a generar vulnerabilidades dentro de red.

Además, este elemento está direccionado con la ruta de enlace hacia el Gateway de la red actual de manera que le permita establecer proceso de conexión con el servicio de ISP, mediante el uso de una antena para captar señales WiFi, dado a que las funcionalidades de este servidor solo pueden ser utilizadas si se cuenta con el servicio de internet, por lo cual, si llegara a ocurrir fallas con el ISP este elemento quedaría inutilizado hasta que se pueda llegar resolver el problema.

Por otra parte, el servidor no cuenta con un espacio designado para su ubicación lo que podría generar malas prácticas con el equipo debido a que está a la disponibilidad del personal de trabajo de la Contraloría (**ver figura 10**). De la misma forma, no cuenta con equipo de protección que

sirva como elemento de control contra posibles amenazas dentro de servicio que puedan llevar a afectar a la red de la Contraloría.

Asimismo, la Contraloría cuenta con un documento donde se guarda la información de los equipos conectados a la red WiFi, establecido como un esquema de red (**ver cuadro 1**) en el cual se representan las direcciones IP que maneja cada máquina/equipo con acceso a la red en conjunto con la máscara de red. Además, se representa que tipo conexión por defecto existe para cada elemento de la infraestructura de red actual. Dicho esquema se refleja en el cuadro que se presenta a continuación:

Nombre	Interfaz	Modelo	IP	Sub Red	Gateway
RT1/	G0/0 Et1/0	Router Tp link 600 mbps Inalámbrico	198.168.1.1	255.255.255.0	198.168.0.1
RT2/)	G0/1	Router Tp link 450 mbps Inalámbrico	198.168.1.2	255.255.255.0	198.168.0.1
Modem	Et 0/1	Motorolasurfbo ard sb6121	198.168.0.1	255.255.255.0	Default
Laptop0	TPC/IP4	Windows 10 enterprise LTSC Intel ® core™ i5- 3570s 3.10 GHz, x64	Dinámica	255.255.255.0	198.168.0.1
Pc1	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Pc2	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Pc3	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Pc4	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Pc5	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Pc6	TPC/IP4	Windows 10 pro 1511. Inter ® core ™2,1.86 GHz X64	Dinámica	255.255.255.0	198.168.0.1
Pc7	TPC/IP4	benq Windows 7 professional Intel ® v Pentium ® dual cpu e2180, 2ghz	Dinámica	255.255.255.0	198.168.0.1
Pc8	TPC/IP4	Windows 7 ultimateService pack 1 Intel® Pentium ® dual	Dinámica	255.255.255.0	198.168.0.1

Nombre	Interfaz	Modelo	IP	Sub Red	Gateway
		Cpue2180 2 GHz x64			
Pc9	TPC/IP4	Windows 10 enterprise LTSC Intel ® core™ i5-3570s 3.10 GHz, x64	Dinámica	255.255.255.0	198.168.0.1
Pc10	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Pc11	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Pc12	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Pc13	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Pc14	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Pc15/	TPC/IP4		Dinámica	255.255.255.0	198.168.0.1
Imp1/	Fa0/1		10.50.28.110	255.255.255.0	N.D.
Imp2	Fa0/1	HP LaserJet 1000 series	15.20.28.108	255.255.255.0	N.D.
Servidor de Nómina	TPC/IP4	-	178.160.10.100	255.255.255.0	198.168.0.1

Cuadro 1. Esquema de la red actual de la Contraloría del Municipio de Antolín del Campo

Fuente: Elaboración Propia (2022)

En el **cuadro 1**, se identifica el esquema de red de la Contraloría, donde se identifican los nombres de los equipos que conforman la actual red junto a la puerta de enlace físico de los mismos, reflejándose procesos de conexión por protocolos TCP/IPV4 para las computadoras y portátiles, asimismo, se logra visualizar las entradas de conexión de los equipos de red (routers) e impresoras; donde todos los equipos del mencionado esquema manejan procesos de direccionamientos estáticos y dinámicos enmarcados en una sub red (255.255.255.0), es decir, de capa 24, unidas a una dirección de enlace lógico (Gateway).

. Sin embargo, cabe destacar que a pesar que cuenta con este esquema de red, este no es suficiente para lograr identificar de manera clara las zonas o subred de la red, generando así dificultades al momento de realizar algún cambio de direccionamiento, manteniendo o incluso modificación dentro de las rutas enlace hacia el servicio del proveedor de internet. Siendo esto una de las destajas de implementar direccionamiento dinámico en una red WiFi(**ver cuadro 1**).

Entrando a nivel de la seguridad física de la red, en la Contraloría no se cuenta con un espacio destinado para resguardar los equipos de red, tampoco se observa un gabinete o rack para la protección de los mismos. Por otro lado, no existen servicios de protección de vigilancia para los elementos que conforman la conectividad hacia el servicio del ISP ocasionando que el personal de trabajo pueda llegar a manipular los equipos de red generando algún problema interno dentro de la red. Además, no se cuenta con un personal directo dentro del Organismo encargado de brindar servicio de soporte a la red, sino que utilizan en personal externo para esas labores.

Por otra parte, se llevaron a cabo entrevistas estructuradas al personal de la Contraloría, dividido en las siguientes: un modelo de entrevista para el personal administrativo donde se tomó a un integrante de cada departamento, generando así un total de siete (7) personas, y otro modelo de entrevista para el personal externo encargado del soporte técnico. Dichos formatos se implementaron para recopilar información relevante acerca de la temática de la infraestructura de la red actual del organismo, junto a los procesos de trabajo dentro de la red de manera que permita reforzar la información obtenida mediante el proceso de observación. Además, se buscó conocer los motivos generales por los cuales existen las caídas y retrasos de la red; así como también para conocer el uso de algún otro tipo de servicio que sea necesario para el funcionamiento de los departamentos que conforman la Contraloría. Por último, lograr identificar todos los procesos de seguridad lógica y física de la red que toman dentro del grupo de trabajo de Contraloría.

En cuanto a la actividad y servicio necesarios para el trabajo dentro de la Contraloría, se identifica el uso frecuente de la red para conocer los cambios leyes gubernamental del País que puedan influir dentro de la metodología de trabajo de la Institución. Además, de hacer uso de servicio de internet para conocer actualizaciones referentes a los cambios monetarios del Banco Centro de Venezuela (BCV). Por otra parte, utilizan los servicios HTTP de Google para conectarse al dominio de email para enviar información del Organismo hacia otros entes gubernamentales o hacia alguna empresa que brinde algún servicio directo a la Contraloría.

Asimismo, hacen uso de este servicio para revisar las redes sociales de la Organismo dado a que el nuevo plan estratégico Estatal necesita el flujo constante de la información que esté sucediendo en las jornadas laborales. Por otra parte, lo logró identificar que el personal de trabajo utiliza el servicio del ISP para realizar actividades fuera de labores de trabajo diarias, es decir, hacen uso del internet para acceder a cuentas bancarias privadas o para realizar consultas

personales consultas dentro de la web. A su vez, se logró identificar que se necesita el flujo constante y óptimo de la red para lograr llenar los listados de nómina al momento realizar transacciones bancarias, dado que en ocasiones al momento que ocurrir grandes itinerarios de trabajo existen perdidas de conexiones aleatorias en los equipos administrativos. Lo que ha generado que se tenga que desconectar algunos equipos dentro de la red para evitar este tipo inconveniente cuando se esté realizando pagos de nómina.

Además, se logró conocer que los servicios del ISP no cuentan con ninguna restricción hacia el personal administrativo de la Contraloría, es decir, que todos pueden tener acceso a cualquier dominio en la web, cosa que no debería suceder según lo explicado por la contralora del organismo, donde resaltó que solo los departamentos de Despacho Central, Administración Central y Coordinación de Despacho deberían tener libre acceso en la red, debido a que se cuenta con una red inalámbrica la cual no presentan un proceso de regulación de IP o MAC para los equipos, generando de esta manera que un tercero pueda conectarse al servicio de enlace inalámbrico (WLC) ocasionando inestabilidad o posibles vulnerabilidades internas en la red.

Por otra parte, se identificó la inconformidad de los servicios de la actual red dado que los equipos informáticos presentan una inefficiencia en el proceso óptimo de conectividad hacia los equipos de red que genera caídas de conexión constante durante todo el día de trabajo, llegando a tomar un tiempo máximo de desconexión de tres (3) horas en promedios, aunque en algunas ocasiones puedan llegar a pasar varios días sin conexión a los servicios de ISP.

Por otra parte, mediante la información recopilada por la entrevista realizada a la administradora central, se logra determinar que los procedimientos de transacciones bancarias pasan con un verificado de doble confirmación enlazadas hacia los departamentos de Administración Central y Despacho, donde cada jefe encargado debe confirmar la transacción para que pueda ser ejecutada, lo cual en ocasiones existen retraso en pago de servicios debido que en algunos momentos cualquier de los dos departamentos mencionados no cuenta con el servicio de internet.

Por estas razones mencionadas, se ha visto afectada la Contraloría debido a que en ocasiones no han logran cumplir con las metas pactadas en sus cronogramas de planificación, generando entonces que durante el transcurso de año 2022 hayan existido perdidas de un aproximado de cincuenta (50) documentos debido a desconexiones de la red. Y, además de generarse retrasos en pago de nómina hacia personal de trabajo donde en ocasiones existe pago de nómina incompleto,

es decir, que no todos los trabajadores se les paga el mismo día. Debido a estas circunstancias el personal administrativo implementa dispositivos de almacenamientos (pendrive) para resguardar la información necesaria para cumplir con las labores correspondientes, pero este elemento es de muy peligroso dado a que puede llegar a infectar a algún equipo dentro de la red si no existe un proveo control o chequeo del mismo mediante el antivirus.

En relación con la seguridad lógica de la red, no presenta un esquema de control y regularización, es decir todas las maquinas del personal administrativo tiene acceso directo a las políticas del servidor DHCP/V4 debido a que se sustentan como usuarios administradores dentro del sistema. Además, no cuenta con proceso de segmentación o túnel de control de acceso interno, por lo que todos equipos utilizan la misma vía de enrutamiento con Host central. Por otra parte, no se tiene una licencia verificada de cortafuegos para los servidores HTTP y DHCP de la infraestructura de red actual, caso contrario a los equipos informáticos que si presenta una licencia activa para su seguridad. Sin embargo, dentro de la red no se tiene con un cortafuego interno para proteger los niveles de seguridad de cada ruta o envío/consulta de información hacia la web, como tampoco para la red privada de la Institución. Por otra parte, los niveles de control de información de los servidores están configurador de fabrica, es decir viene destinado con los protocolos, usuarios y claves de defecto.

De la misma forma, se no cuenta con dispositivos de red encargados de regular las direcciones de su capacidad de ancho de banda, por consiguiente, todos sus máquinas y equipos intentan utilizar el máximo de su capacidad, ocasionando pérdidas de conexión por zonas de trabajo, ya que no se tiene una segmentación lógica previamente configurada, por lo cual cada equipo lucha internamente para poder mantener conexión establece. Además, por el hecho de no contar con una segmentación esto ocasiona que red sea altamente vulnerable por infecciones internas. Por otra parte, debido a que se utiliza una red WiFi donde solo se aplica un servicio de acceso hacia los equipos, esto puede ocasionar infiltraciones en la red mediante el robo de la contraseña, de la misma manera, debido utilizar el pendrive para compartir o enviar información de un departamento este elemento puede llegar a generar puntos de infección en la red que puedan llegar a vulnerar la integridad de la misma.

Dentro de la seguridad física de la red se logró identificar que los equipos están ubicados en zonas cercanas a los equipos administrabas lo que generado en los lapsos de marzo-abril de 2022 tropiezos con los equipos de red generando daños a la integridad física del elemento, causando

por ello perdida de conexión a un sector de la planta baja de la Contraloría. Además, no se aprovecha el máximo potencial de los equipos de red debido a que no se han realizado estudios previos de las zonas de la Contraloría que permitan determinar la disponibilidad de conexión de la red dentro de los espacios requeridos.

Del mismo modo, debido a que los equipos de red se encuentran distribuidos en diversas áreas abiertas, estos no tienen un sistema de refrigeración adecuado provocando sobrecalentamiento del equipo de red lo que ha ocasionado en los meses de septiembre y octubre del año 2022 daños de Hardware y software en los equipos en específico daño de la tarjeta lógica y falla en sistema de auto ventilación del Router.

Asimismo, se reflejan fallas eléctricas dentro de la Institución donde se logró obtener identificar caída constante de servicio eléctrico durante los períodos de trabajo. Donde no se contempla un plan o esquema de horas de servicio del corte eléctrico, sino que se ocurre de forma inesperada e independiente, sin margen de hora de llegada, es decir, no se sabe la duración de cortes. Al suceder este fenómeno, los procesos de trabajo se retrasan debido a que no se cuentan con un sistema de alimentación interrumpida dentro de Organismo que permita dar estabilidad y conexión eléctrica a los equipos red e informáticos generando pérdida de tiempo durante las horas sin el servicio anteriormente mencionado ocasionando que se tenga que cumplir labores administrativas en tiempo de descanso.

Por otra parte, los equipos de red no cuentan con regulador y protector de voltaje que sirva como barrera si sucede alguna baja o caída de corriente. En igual forma, los equipos informáticos solo presentan un protector de voltaje, el cual no es suficiente para la protección de las máquinas debido a que no regula el suministro eléctrico, lo que ha generado daños en algunos equipos informáticos.

En cuanto a las infecciones dentro de la red o a los equipos de trabajo, se logró obtener que durante los meses enero-abril del año 2022 se han visto afectado la mayoría de los equipos informáticos de la red, representando una infección en cadena proveniente del máquina ubicada en el departamento de Recursos Humanos generando pérdidas de archivos del personal de Administración Central, así como también bloqueos de información debido a la infección de un ransomware de bloqueo en la máquina de la oficina de Despacho que perduró durante una (1) semana, ocasionando pérdida total en el área de Coordinación de Despacho.

Por otra parte, a nivel de la infraestructura de red esta no ha sufrido daños de infecciones de terceros durante todo su periodo de implementación, pero si ha ocurrido vulnerabilidades en el acceso de terceros a red WiFi, reflejando que durante los periodos de abril-junio del mismo año se han detectado elementos no pertenecientes no forman parte de grupo de equipos de la Contraloría.

En relacion al proceso de solución de fallas dentro de la infraestructura de red, el Organismo presenta un personal de soporte tecnico externo el cual no cumple una labor fija dentro de la Institucion, sino que es solicitado al momento de suceder algun fenomeno fisico-logico que efecto a los equipos de la red, donde se establecio un tiempo de respuesta de una (1) a dos (2) días luego de averse solicitado su servicio. Este personal de soporte realiza su proceso de trabajo dentro de la misma Contraloria en la cual no cuenta un espacio establecido para ejercicio sus habilidades y no tampoco establece un control de accion que registro los labores realizadas en ese lapso solicitado.

En cuanto al tiempo de respuesta para la solucion del problema todo viene a depender del tipo de circunstancia que se presente al momento de revisión, sin embargo, se sustenta que suele tardar dentro de una (1) a tres (3) horas de trabajo. El mismo personal de soporte técnico destaca que el personal administrativo en ocasiones vulnera los equipos de red ocasionando que algunas circunciona los tiempo se resolucion del problemas puedan llegar a tarda mas dias.

Para facilitar el análisis de los datos anteriormente mencionados se desarrolló un análisis FODA, que permitió reflejar de manera mas sencilla toda la información obtenida mediante la aplicación de las técnicas de recolección de datos, de tal manera que ayude a identificar aquellos elementos que puedan estar efecto directe al fenómeno estudiado dentro de la Contraloría del Municipio de Antolón del Campo.

Nivel	Puntaje
Bajo	1
Medio	2
Alto	3

Cuadro 2. Nivel de proceso para el Análisis FODA.

Fuente: Elaboración Propia. (2022)

De esta forma, se establece un cuadro que en el cual se establece el nivel de impacto de cada elemento reflejado en el análisis FODA (**ver cuadro 2**) que logra brindar de manera práctica aquellos elementos que puedan estar ocasionando la problemática en la infraestructura actual de

red inalámbrica de la Institución, logrando así comprender de manera clara las posibles soluciones que puedan llegar a brindarse.

FORTALEZAS	DEBILIDADES
Disponibilidad económica para reformación de red. (2) Buen ambiente de trabajo.(3) Sirve cualquier ordenador conectado a internet. (2) Equipos informáticos óptimos. (2)	No conocen en funcionamientos interno de la red. (3) No presentan con personal de soporte interno. (2) No existen un lugar destinado a resguardar los equipos de red. (3) Equipos de red ineficientes para los requerimientos básicos. (3)
OPORTUNIDADES	AMENAZAS
Disponibilidad de contratar a personal calificado. (3) Potencia de difundir conocimientos de la seguridad de la red.(2) Alta compatibilidad de los equipos informáticos. (1) Posibilidad de contar con zona de resguardo.(2)	Vulnerabilidad de la red a manos de terceros.(2) Perdidas de información por fallas eléctricas. (3) Cracking de las contraseñas de red.(3) Colocación de malware a equipos de los usuarios de la red.(3) Hurto de información mediante Phishing.(2)

Cuadro 3.Puntación de los elementos del análisis FODA.

Fuente: Elaboración Propia. (2022)

Mediante el análisis del **cuadro 3**, se puede decir que la contraloría del Municipio Antolín del Campo presenta diversas de fallas en relación a la infraestructura de red, sin embargo, debemos constatar que tiene posibilidades de mejorar estas circunstancias gracias a las fortalecer y oportunidades que presenta que permitan garantizar la estabilidad a futuro de su red. Posteriormente se hizo el conteo de los puntos, sumado por cada cuadrante de la matriz FODA y se vaciaron los datos en el **cuadro 4**.

Fortalezas	Debilidades	Oportunidades	Amenazas	Total
9	11	8	13	41
22%	27%	20%	32%	100%

Cuadro 4. Ponderación general de cuadrantes de la Matriz FODA.

Fuente: Elaboración Propia. (2022)

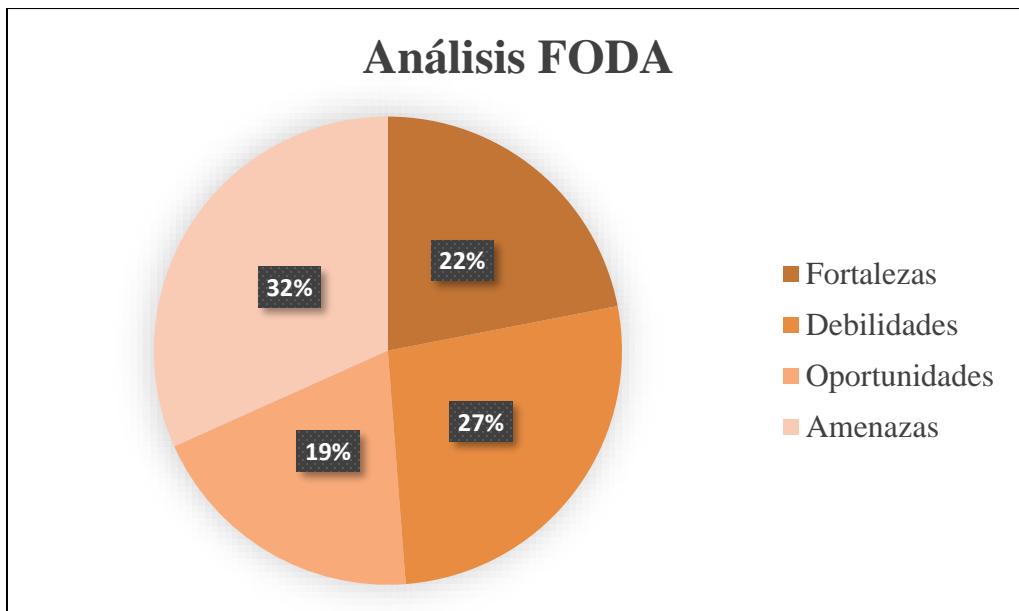


Figura 11. Análisis FODA de la infraestructura de red de la Contraloría del Municipio de Antolín del Campo.

Fuente: Elaboración Propia. (2022)

En la **figura 11**, se puede visualizar los porcentajes, basados en la puntuación que obtuvo cada cuadrante de la matriz FODA. Se expone que la Contraloría del Municipio de Antolín del Campo cuenta con un veintidós (22) porciento de fortalecer, por otra parte, un veintisiete (27) porciento de debilidades, luego un veinte (20) porciento de oportunidades y por ultimas encontramos que cuenta con un treinta y dos (32) porciento de amenazas. Posteriormente, se determina la ponderación de los dos factores que presenta la matriz FODA, siendo estos el factor de oportunidad y el factor de riesgo.

Factor de Oportunidad	Factor de Riesgo	Total
17	24	41
41%	59%	100

Cuadro 5. Factores del análisis FODA.

Fuente: Elaboración Propia. (2022)

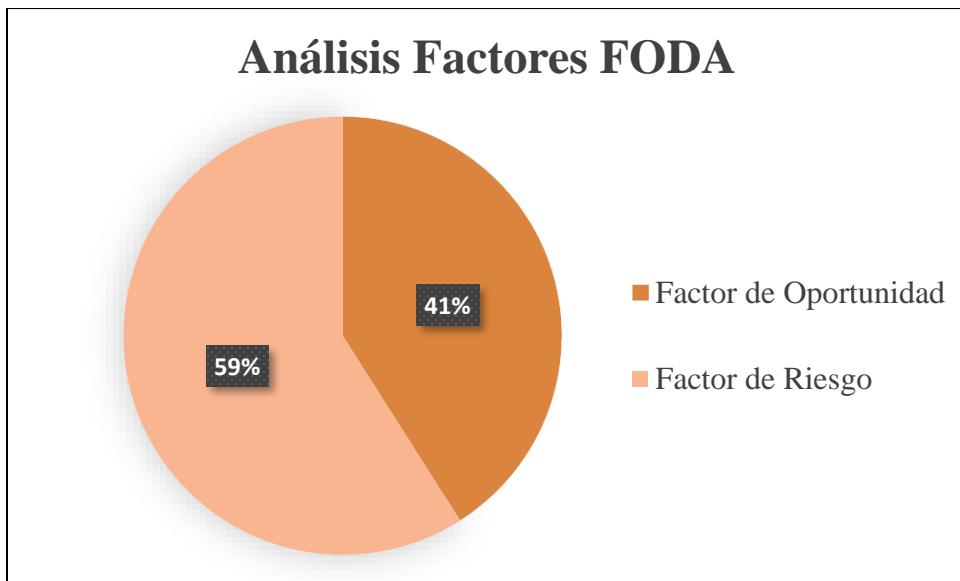


Figura 12. Análisis de factores de oportunidad y riesgo.

Fuente: Elaboración Propia. (2022)

En la **figura 12**, se identifica los porcentajes, basados en la puntuación que obtuvo los factores anteriormente mencionados dentro de la matriz FODA. Se presenta entonces que la Contraloría del Municipio de Antolín del Campo, tiene un cuarenta y un (41) porciento de factor de oportunidad, caso contraloría para el factor de riesgo que presenta un cincuenta y nueve (59) porciento. Resaltando por ello, que actualmente el Organismo presenta una deficiencia en su infraestructura de red lo cual puede causar pérdidas significativas para la Contraloría. Por consiguiente, se plantea en el **cuadro 5** las estrategias DOFA de la matriz FODA.

ESTRATEGIAS FO	ESTRATEGIAS DO
1) Contratar personal de soporte técnico interno. 2) Realizar foros y tallares de instrucción sobre la seguridad de las redes al personal administrativo. 3) Generar manuales estratégicos para usuarios con sus respectivos equipos informáticos. 4) Ubicar una sede DMZ para los equipos de red y servidores.	1) Hacer manuales usuarios de red y documentación de la misma. 2) Reforzar los conocimientos del personal de soporte mediante la realización de cursos sobre seguridad y administración de redes. 3) Establecer medidas y equipos de control y seguridad en caso de suceder algún suceso físico. 4) Adquirir otro servicio de internet.
ESTRATEGIAS FA	ESTRATEGIAS DA
1) Invertir en cortafuegos (firewalls) para los equipos red y equipos administrativos. 2) Asignar servidores de respaldo para el manejo de información. 3) Configurar los equipos de red mediante asignaciones de usuarios, con un control de acceso de dos medidas. 4) Invertir en un servicio de protección (antivirus) óptimo en contra de infecciones por malware. 5) Asignar planes estratégicos mediante protocolos de seguridad web para la detección de Phishing.	1) Establecer medidas de control de acceso a los equipos administrativos y de red. 2) Asignar equipos de protección y regulación de voltaje, junto a un personal encargado de llevar control de los mismos. 3) Establecer rack para los equipos de red. 4) Implementar nuevos equipos de red con niveles de seguridad avanzados. 5) Regular el acceso a plataformas web mediante controles de reloj en los equipos informáticos.

Cuadro 6. Análisis DOFA de la Matriz FODA.

Fuente: Elaboración Propia. (2022)

En el **cuadro 6**, se establecen las estrategias FODA para aplicar dentro de la Contraloría del Municipio Antolín del Campo. Encontrando entonces las estrategias FO donde se determina la contratación de personal especializado que ayude a solucionar fallas que puedan llegar a ocurrir en la red; además se plantea la realización de foros y talleres para instruir al personal de trabajo a tomar conciencia de las consecuencias que puedan llegar a ocasionar las malas prácticas dentro de la red. Así mismo, se plantea la elaboración de documentos que permitan registrar la información de los equipos del personal administrativo de manera que se faciliten las actividades

al personal de soporte en caso de llegar a realizar algún proceso de mantenimiento de la red. Por otra parte, se buscar implementar una zona desmilitarizada (DMZ) que logre brindar protección dentro de la red al momento de realizar peticiones hacia los servicios del ISP.

Seguidamente, encontramos las estrategias DO que buscan subsanar las debilidades que presentan actualmente la organización mediante el uso de las oportunidades que estén presentes, remarcando implementar manuales que faciliten al usuario el manejo del equipo administrativo que le corresponde. Asimismo, impulsar los conocimientos del personal de la contraloría en relación a los procesos de seguridad que conlleva una red. De la misma manera, se propone instaurar elementos que sirvan de apoyo para la protección física de los equipos de red. También, se plantea adquirir los servicios de otro proveedor de internet que permita aumentar la capacidad de ancho de banda de la red.

Luego, encontramos las estrategias FA, donde se establecen medidas para mitigar las amenazas mediante el aprovechamiento de las fortalezas que presenta la Contraloría, donde se propone invertir en un equipo de red (cortafuegos) que permita mantener control de seguridad en la red, junto a servicio de antivirus que permita mantener seguros los equipos administrativos (computadoras, impresoras y portátiles). Del mismo modo, asignar equipos para el resguardo de la información que se maneje dentro de la Contraloría de manera que se puedan establecer medidas de preventivas y correctivas en caso de extraviarse algún dato de importancia. Además, se plantea establecer asignaciones de usuarios de manera que logre mejorar la seguridad de la red. También, surge la necesidad de implementar protocolos de servicios dentro de la red que logren proteger a los equipos en caso de ser expuesto a software malicioso.

Por último, se exponen las estrategias DA, las cuales se establecen para buscar neutralizar los puntos críticos de las debilidades y amenazas identificadas; por lo cual, se plantea implementar estrategias de control para el acceso del personal administrativo a los equipos informáticos mediante un registro físico. De igual manera, se plantea invertir en elementos que permitan mantener estabilidad del servicio de electricidad que presenta la Contraloría, de forma que coadyuve a mejorar los niveles de seguridad física de los equipos de la red. Además, se refleja la implementación de rack para establecer los equipos de red que generar conectividad dentro de la infraestructura. (ver **cuadro 6**).

De la misma forma, dentro de las estrategias DA se buscar establecer en los equipos de red medidas de seguridad para el acceso lógico, permitiendo solo acceso a aquellos equipos que

lo requieran y estén habilitados para llevar a cabo tal acción. También, se plantea regular el acceso de los equipos administrativos a los servicios proporcionados por la web, de manera que se puedan prevenir posibles fallas a nivel de seguridad. Es así como, todas las estrategias expuestas en los párrafos que preceden, se realizaron con el fin de usar el análisis realizado mediante la matriz FODA como punto de inicio para mejorar la red de área local de la Contraloría del Municipio Antolín del Campo.

4.2 Componentes necesarios para el diseño de la nueva Red de Área Local alámbrica para la Contraloría del Municipio Antolín del Campo.

Para determinar todos componentes necesarios para el diseño de la nueva Red Alámbrica, se realizan procesos de revisión documental para análisis que factores serían conveniente aplicar para cada nuevo elemento vinculado a la red, para así garantizar su implementación dentro del nuevo diseño, brindando de esta manera satisfacer las necesidades identificadas, por lo cual, se basó en las normativas establecidas por la Asociación de Industrias Electrónicas (EIA), que permitan garantizar la estabilidad en la conexiones de los equipos administrativos (pc, portátiles, impresoras) de la Contraloría.

En cuanto a los componentes para el cableado de red encargados de interconectar los equipos, se optó por elementos capaces de proporcionar velocidades de hasta 1000 Mbps y frecuencias que van desde 100 a 300 MHz, siendo las opciones ideales para manejar el flujo de información de la Contraloría; además de brindarle al cableado la protección que necesita. En tal sentido, se consideran los siguientes elementos:

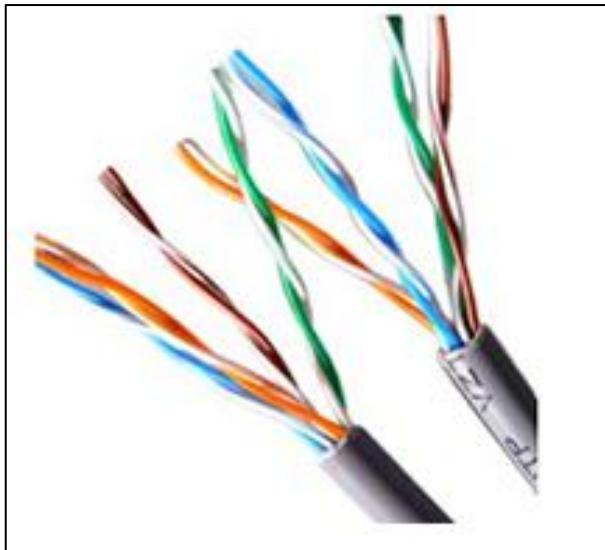


Figura 13. Cable Ethernet UTP Cat. 5e para interior

Fuente: Black Box. (2022)

Así pues, para establecer conexión física en la red se hará uso de un cableado de modelo Ethernet UTP para interior de categoría 5e (**ver figura 13**), para establecer interconectividad entre todos los equipos aginados dentro de la nueva red, que maneja velocidad de 10-100 Mbps mediante el enlace de conexión por señal digital para permita el transporte de la Data dentro de todos el Organismo, además de proporcionar de conexión constante, ya que se establece un proceso servicio por cable.



Figura 14. Conectores Rj45 Cat. 5e

Fuente: Mercado Libre. (2022)

Para conectar el cableado hacia los equipos de red y maquinas administrativas es necesario contar con dispositivos que manejen las mismas características del cableado, por lo cual, se considera implementar conector de enlace de modelo Rj45 para categorías de cableado 5e (**ver figura 14**), ya que presentan las mismas características y estándares establecidos para el cableado de red anteriormente mencionado.



Figura 15. Canaleta para cableado de red.

Fuente: Amazon. (2022)

De la misma forma, se necesita de un elemento que permita transportar el cableado Ethernet desde los dispositivos de salida del servicio de internet hacia los dispositivos o máquinas de la red de manera que asegurar su traslado dentro de la Contraloría, siendo entonces utilizado una canaleta de red de 3 segmentos (**ver figura 15**), con sistema de conductor cubierta por metal de color blanco, resistente a impacto.



Figura 16.Jack Coupler Cat5e
Fuente: Mercado Libre. (2022)

Por otra parte, para establecer la conexión del cableado hacia los conectores mencionados anteriormente, se ve la necesidad de implementar un Jack CouplerCat5e (**ver figura 16**) que maneje los mismos estándares de red de manera que permita conectar de forma física el cableado de red hacia todos los equipos administrativos que se determinen en la nueva red alámbrica para la Contraloría.

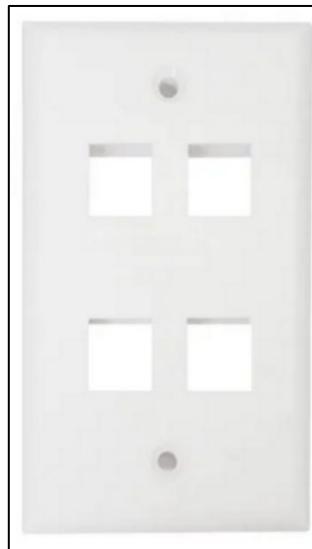


Figura 17. Tomas para cableado de red.
Fuente: Mercado Libre. (2022)

Ahora, para poder establecer conexiones a todas las máquinas de la Contraloría se ve la necesidad de implementar tomas para cableado Ethernet de 4 entrada que permitirán facilitar los procesos de conexión física en la red hacia los equipos informáticos de los departamentos de cada zona de trabajo, generando mayor seguridad cableado mencionado anteriormente (**ver figura 17**) dado a permite ocultar dicho elemento.



Figura 18. Botas de red CAT/5e.

Fuente: Amazon. (2022)

En relación con la protección de los elementos que conformaran la nueva infraestructura de red, se visualiza la implementación de botas de red para resguardar el cableado, junto a los conectores Rj45 que se insertarán en cada dispositivo que se encuentre en la infraestructura de la red, funcional para cables con niveles de CAT5/5E/6 Ethernet LAN (**ver figura 18**), con una cubierta del conector de color azul, compatible para cualquier equipo personal.

En cuanto a los equipos de red, estos serán los encargados de dotar de internet a la nueva red, así como permitirán segmentar la misma en redes más pequeñas para cada departamento. Igualmente, tendrán la tarea de crear controles de acceso como medida de protección para la información que viaja por la red; además de hacer posible la distribución del ancho de banda para cada subred. Dicho esto, se consideraron los siguientes equipos:



Figura 19. Modem Motorola.

Fuente: Amazon. (2022)

Por otra parte, para captar el servicio proveniente del ISP es necesario implementar un equipo de red que permite transformar esa señal analógica a digital mediante cableado coaxial, por ello se hace uso del Modem Motorola sb6121 Soundfreaks Inter de color negro (**ver figura 19**), debido a que cumple con las características necesarias para satisfacer los nuevos componentes de la red alámbrica.



Figura 20. Router Neutro.

Fuente: Amazon. (2022)

También, se utilizará un dispositivo de enrutamiento neutro por conexión Ethernet que permita convertir la señal analógica a digital y la propague hacia todos los equipos pertenecientes

a la nueva infraestructura de red. Para esto se hará uso de un Router TRENDnet modelo TW100-S4W1CA negro de 4 puertos LAN y 1 puerto WAN con capacidad de acceso de hasta 253 usuarios (**ver figura 20**).



Figura 21. Switch TP-Link color negro de 24 puertos Gigabit Ethernet
Fuente: Amazon. (2022)

Por otra parte, para lograr intercomunicar a todos los equipos de red mediante procesos de enrutamiento para los departamentos que conforman la Contraloría es necesario aplicar un dispositivo Switch TP-Link negro de 24 puertos (**ver figura 21**), ya que permitirá establecer conectividad a todos los nuevos equipos junto con los que se cuenta actualmente, pero también permitirá establecer conexión a futuros elementos que puedan llegar a establecer en la red.

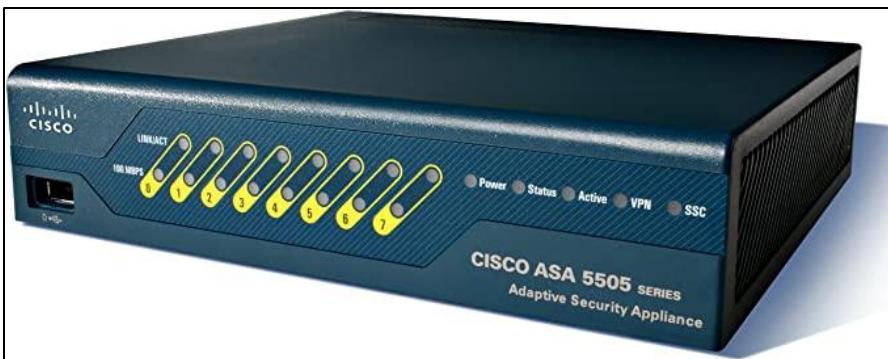


Figura 22. ASA 5505 para seguridad web.
Fuente: Amazon. (2022)

Para poder controlar los accesos a las segmentaciones de la red se ve la necesidad de implementar un equipo informático Cortafuegos (Firewalls) ASA 5005 (**ver figura 22**) que permite crear túneles para distribución general de la infraestructura mediante uso de VLANS para garantizar la seguridad lógica de cada zona que conforma la Contraloría, pero además para poder

administrar la capacidad de velocidad que maneje para área en relación que las necesidades que se permiten para ese equipo o elemento de la red. Además, este dispositivo se puede establecer mediante una configuración interna para medidas de control acceso a nivel de seguridad para cada elemento que este unido al mismo.

El siguiente grupo corresponde a los equipos de cómputo, entre los cuales se encuentra el servidor proxy, encargado principalmente de recibir peticiones de acceso de otros equipos de la red, asignar permisos a los mismos y controlar los protocolos de red. Del mismo modo, se necesitará un servidor de nómina que sea capaz de satisfacer los requerimientos de la red y que se pueda optimizar aún más su funcionamiento. Por lo cual, se consideraron los siguientes elementos:



Figura 23. Máquina HP Z640.
Fuente: Amazon. (2022). (2022)

Dicho esto, para establecer el nuevo servidor Proxy se ve la necesidad de implementar una máquina de modelo HP Z640 para controlar el tráfico de información y registrar la seguridad para asignar permisos dentro de los servicios del Servidor. Por otro lado, este elemento cuenta con la capacidad de 32 GB DDR, con límite de 8 slot de RAM, con capacidad de disco SSD de 1 Terabit (**ver figura 23**). También, dicho equipo maneja las mismas frecuencias que los dispositivos anteriormente explicados.



Figura 24. Máquina HP.

Fuente: Contraloría Antolín del Campo. (2022)

Del mismo modo, para implementar el servidor local de nómina de la Contraloría se hará uso de una máquina HP debido a que posee compatibilidad con los nuevos equipos y además permite la posibilidad de poder expandir su capacidad debido a presenta 4 slot para memoria RAM (**ver figura 24**). Además, para no perjudicar los sistemas configurados, no se establecerán cambios a nivel de interno del software.



Figura 25. Monitor HP full HD.

Fuente: Amazon. (2022)

Por otra parte, para poder visualizar las grabaciones de los cámaras de seguridad antes mencionadas se necesita un dispositivo que puede tener conexión directa mediante cableado para poder obtener los registros de las grabaciones realizar, por este motivo se hace uso de un monitor

HP full HD (**ver figura 25**) de manera tal que no presente inconveniente de resolución al momento de identificar algún momento específico dentro de la grabación.

Por último, se necesitarán de ciertos elementos para la protección de los equipos de la red. Este grupo es quizá de los más importantes, ya que algunos de ellos permitirán atender cualquier eventualidad y así evitar el daño de los equipos. Gracias a ellos también se podrá monitorear quienes acceden a la zona de resguardo y tienen contacto con los equipos. Igualmente, se usarán equipos encargados de la parte del flujo eléctrico y, otros como armario para guardar los aparatos. Dentro de este grupo se encuentran:



Figura 26. Fuente de alimentación ininterrumpida (UPS) APC.

Fuente: Amazon. (2022)

En relación con las problemáticas de origen físico en específico los cortes eléctricos, se ve con ello la implementación de una fuente de alimentación ininterrumpida de línea modelo un APC USP inteligente de 1500 VA (**ver figura 26**), con batería de reserva. Para de esta manera garantizar la conectividad hacia internet de los equipos central encargado de enrutar conexión hacia el servicio de internet, generando así estabilidad para en la red utilizada por el personal de trabajo de la Contraloría.



Figura 27. Detector de humo y monóxido de carbono. Kidde.

Fuente: Amazon. (2022)

Por otra parte, a nivel de seguridad de la red se implementa un equipo que funcione de alarma contra incendios internos en la ubicación generar de los equipos de red, tomando como modelo el Kidde – Detector de monóxido de carbono y humo de color blanco funcional con baterías recargables (**ver figura 27**), el cual brindará la función de alertar si existe algún problema con el centro de control de la red, es decir, si está ocurriendo incendios eléctricos de manera de poder llegar a prevenir un daño mayor en los equipos cables del nuevo diseño del a red.



Figura 28. Extintor de incendios

Fuente: Amazon. (2022)

Por otra parte, si llega a ocurrir un incendio eléctrico en algún dispositivo o servidores de la nueva red, se ve la necesidad de implementar un equipo extintor de incendios especializados para este tipo de labor para no comprometer al equipo de red, ya que si se implemente un elemento incorrecto podría llegar a afectar el funcionamiento la red. Por la cual, se implementa un extintor de incendios AnsulCleanGuard modelo FE-36 (**ver figura 28**) a base de hidroflourocabono el cual es biodegradable por lo que genera una estabilidad luego de ser aplicado a los equipos afectados, es decir, no sufren daños colaterales por su uso.



Figura 29. Desagüe de aguas para baños.

Fuente: Amazon. (2022)

Asimismo, para prevenir daños con respecto a inundaciones en el área de resguardo de los equipos de red se ve la necesidad de implementar un desagüe para baños (**ver figura 29**) de manera que brinde apoyo con estos posibles eventos que puedan afectar la integridad física de los equipos, garantizando de esta manera mayor seguridad de la zona de resguardo y además permitiendo poder mantener una estabilidad de la infraestructura de la red LAN en caso de presentarse el fenómeno mencionado.



Figura 30. Aire acondicionado para refrigeración.

Fuente: Mercado Libre. (2022)

De la misma forma, para garantizar una adecuada refrigeración de los equipos de red ubicados en la zona de resguardo, se ve la necesidad de implementar un aire acondicionado (**ver figura 30**) capaz de mantener refrigerado el área mencionada, pero a su vez permitir prevenir niveles altos de humedad ya que esto puede llegar a afectar la integridad física de los equipos generando así posibles fallos en la red.



Figura 31. Regleta protectora/reguladora CRST.

Fuente: Amazon. (2022)

Para poder conectar a los equipos de red hacia una fuente de energía se ve la necesidad de implementar una regleta CRST de color negro protectora (**ver figura 31**), como fuente reguladora de poder para establecer conexión hacia cada dispositivo conectados a la misma,

debido a que permite controlar mediante regulación de voltaje de los equipos implementado en el diseño de la nueva red. Por otra parte, este elemento tiene la disponibilidad de acceso para conectar futuros equipos lo que permite poder ampliar la red si lo es necesario.



Figura 32. Cámara de seguridad Swann.

Fuente: Amazon. (2022).

De la misma forma, se implementa dispositivos de seguridad que registren mediante grabaciones el control de acceso a los dispositivos de la red, que permita tener un control del acceso hacia y manejo de los equipos. Por la cual, se ve la necesidad de implementar una Cámara de seguridad inteligente Swann de color blanco con características con resolución 1082 Full HD (**ver figura 32**), con capacidad de conectividad alámbrica/inalámbrica con detector verdadera PIR de color/movimientos, visión nocturna y radio.



Figura 33. Protector de voltaje 220 V.
Fuente:Amazon. (2022)

Por otra parte, se implemente un elemento para controlar las caídas de voltaje debido por las bajas de tensión de corriente eléctrica para prevenir el daño en los equipos y dispositivos de red que se implementan en el nuevo diseño, por lo cual se determinar usar protector de sobretensiones eléctricas (**ver figura 33**) para electrodomésticos y equipos de red con salidas de voltaje de 220, permitiendo establecer protecciones a los equipos de la red.



Figura 34. Rack StarTech.
Fuente: Amazon.(2022)

Para finalizar, para lograr resguardar los equipos de red es necesario contar un almacén o armario para rack que permita establecer a los equipos de manera segura, donde además brindara una disposición física especial para cada equipo perteneciente, dependiendo de la utilidad del mismo. Por esta razón se ve la necesidad de implementar elemento StarTech Armario-rack (**ver imagen 34**), con profundidad ajustable y color negro con funcionalidad compartidas para dispositivos de red, con protección por fijado de metal. Este elemento cuenta con la suficiente capacidad para establecer los nuevos equipos para el diseño de la red, pero también para futuros elementos que puedan llenar aginarse

4.3 Configuración óptima para garantizar la seguridad y conectividad de la nueva Red de Área Local alámbrica de la Contraloría del Municipio Antolín del Campo.

Para establecer la configuración óptima de la nueva red alámbrica para la Contraloría, se hace medida de los estándares de conexión de cableado estructurado establecidos por la EIA para cableado cruzado de modelo UTP recomendadas para el diseño e instalaciones de los equipos, donde se determinan los parámetros de la normativa, como: la topología, la distancia de los cables, el rendimiento de los componentes, las tomas de los conectores permitan intercomunicar procesos de telecomunicaciones.

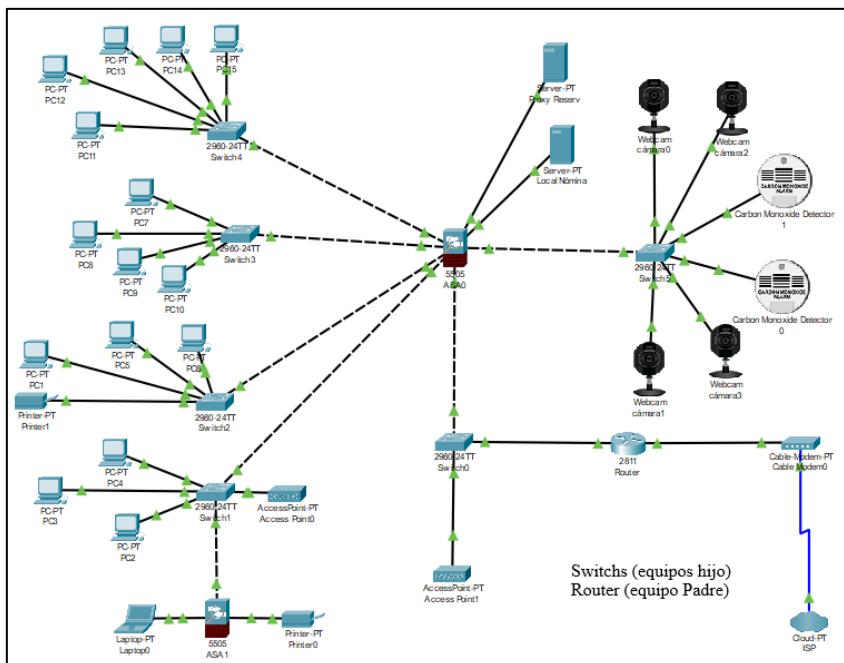


Figura 35. Topología de la nueva red.

Fuente: Elaboración Propia. (2022)

Entrando con la topología asignada para la nueva red alámbrica para la Contraloría del Municipio de Antolín del Campo (**ver figura 35**), se designan mediante conexiones de cableado UTP, divididas por zonas de trabajo mediante commutadores(switches), que permitan generar conectividad en la red, por tal motivo, cada representación de estas zonas se establece como una topología de estrella dado que depende únicamente de un elemento de red, es decir, da una conexión hija. Sin embargo, para generar las segmentaciones de la red se implementa un equipo de seguridad principal (cortafuego “ASA0”), mediante el cual se distribuye de manera controlada la nueva red. Debido a que cada una de estas zonas tienen dependencia del cortafuego, se representan una topología final de árbol, ya que ahora se visualiza un equipo padre desde el cual se subdividen ramificaciones para lograr establecer conectividad.

Por otra parte, debido a que se debe mantener un control dentro de la red para que el transporte de la información (datos) de manera que brinde una estabilidad, se determinan niveles de capas dentro de la nueva red alámbrica guiadas bajo la normativa OSI de manera que brindar una armonía en los procesos de transferencia, protección y control ayudando de esta manera a generar una confiabilidad dentro de la red. (**Ver figura 36**)

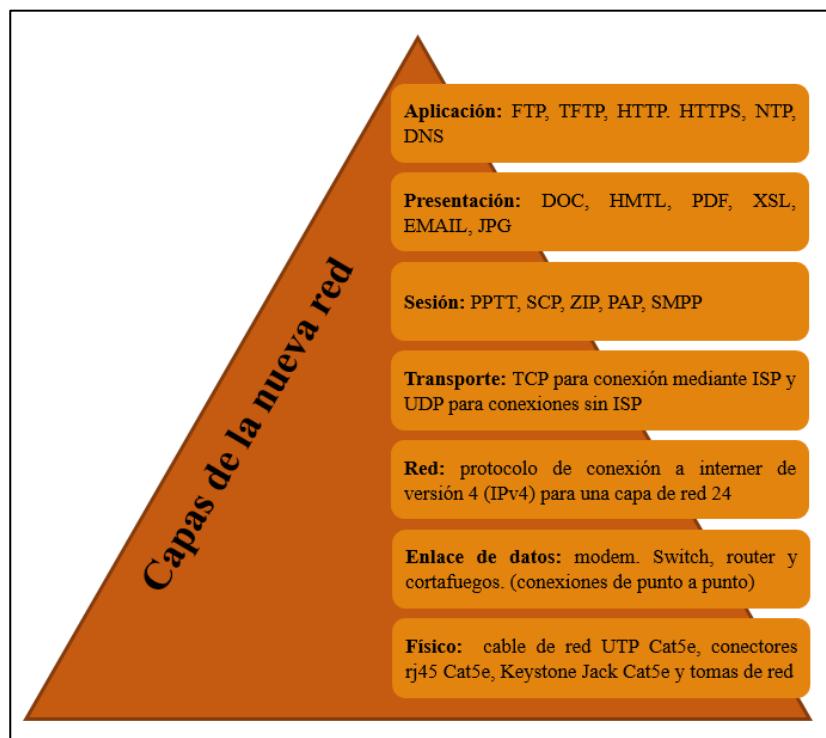


Figura 36. Capas para la nueva red.

Fuente: Elaboración Propia. (2022)

Para iniciar, se representa la capa física de la nueva red donde se determina las especificaciones eléctricas y mecánicas mediante las cuales va a funcionar la infraestructura de red. Teniendo de esta forma una transmisión mediante cableado de cobre, denominado cable de red UTP categoría 5e para interior con capacidad de manejar velocidades de transmisión de datagramas de 10-100 Mbps. Además, para la conexión física del cableado hacia los equipos de red y administrativos se determina conectores rj45 categoría 5e capaz de manejar estas señales transmitidas por cable cobre, asimismo, para facilitar los puntos de acceso se representa tomas de red en las cuales se asignan Jack Coupler de categoría 5e que ayuden a establecer las conexiones del cableado de red hacia las tomas (**ver figura 36**).

Enseguida, encontramos la capa de enlace de datos donde se representa el transporte confiable de los datos mediante un enlace físico, es decir, conforman a los equipos de red encargados de transmitir los datos dentro la red (**ver figura 36**). Debido a ello, encontramos el modem encargado de captar la señal analógica proveniente del servicio del ISP para luego transportarla hacia el router en forma digital. De allí, el enrutador se encarga de distribuir los paquetes de entrada en la red, donde se le asigna un equipo de protección (cortafuego) que se encarga de suministrar de forma regulada el acceso a estos paquetes. Por último, se ubican los switches que tendrán la tarea de controlar las conexiones de punto a punto mediante procesos half-dúplex y full-dúplex, es decir, controlar el flujo de ancho de banda para cada equipo conectado en él. Cabe destacar que el enrutador y los cortafuegos se les determina velocidad automática (100 Mbps).

En relación a los cortafuegos, se establecen redes de área local virtuales (VLANS) donde la configuración óptima del mismo va a depender de las necesidades que abarque los departamentos a los cuales se direcciona este equipo de red. Debido a ello, se llegan a considerar 2 niveles de conexión establecidas por defecto, encontramos entonces una conexión de entrada a la red junto a una conexión de salida de la misma.

Tipo de protección (VLAN)	Nivel	Conexión
Baja	0	Salida
Media	50	Entrada
Alta	100	

Cuadro 7. Configuración del nivel de seguridad de los cortafuegos.

Fuente: Elaboración Propia. (2022)

De esta forma, en el **cuadro 7** se visualizan la configuración lógica de los cortafuegos, donde dependiendo del tipo de conexión se establecen parámetros de seguridad estandarizados por CISCO de manera permiten tener niveles de control de las segmentaciones, estipuladas por 3 tipos de protección en donde las que presenten mayor nivel de protección serán capaces de acceder a cualquier zona enlaza hacia el cortafuego, caso contrario a los niveles bajos los cuales no van a tener acceso hacia una zona con mayor protección. Por esta razón, las conexiones que se establecen desde ASA0 hasta los switches (**ver figura 36**) abarcan un direccionamiento IP con una segmentación establecida, donde el comutador establecerá este círculo virtual proporcionado a cada host conectado en él.

En otra medida, se determinó configurar dentro de los switches 0 y 1, puertas de enlace físico que permitan llegar a establecer conexión mediante puntos de acceso, dado si existe la necesidad en el futuro de implementar esto tipo de conexiones. Asimismo, para mantener control de seguridad a posibles elementos se ubica un punto de acceso fuera de la zona de segura dentro de la nueva red (Switch 0) para establecer servicio al público que se presente dentro de la Contraloría y otro inmerso dentro de la protección establecida por el cortafuego principal (Switch 1) de manera que pueda proporcionar servicio a personal de trabajo del Organismo.

Seguidamente, encontramos la capa de red (**ver figura 36**) que nos permitirán mantener conectividad dentro de la red, donde se implementa en la nueva red protocolo de internet de versión 4 basado en notación de treinta y dos (32) bit capaz de manejar con un grande número de direccionamientos IP, donde a su vez es capaz de dar rutas más rápida y dinámicas dentro de la red, mediante un proceso de encapsulamiento mediante una dirección de origen y destino dentro de la nueva red para luego proceder con el desencapsulamiento que permita leer el encabezado a los paquetes. De la misma manera, para controlar la cantidad de asignaciones de IPv4 se establece un modelo de mascara de cada 24 para todos los equipos de red y administrativos, siendo este modelo de capa capaz de lograr abarcar futuras asignaciones dentro de la nueva red en tal caso que existe un aumento de los equipos.

Por otra parte, encontramos la capa de transportese establecen el protocolo TCP/IP que permitan controlar de manera segura la red de manera que permitan acceder a círculos virtuales (segmentaciones), que garantice la comunicación entre hosts mediante un servicio de conexión que genere fidelidad de los datos, debido a que se implementa una secuencia para la entregada de los mismo, aunque este protocolo sea algo lento permite poder mantener un control de la

información garantizando que los paquetes llegan de manera completa y no existan perdidas mediante la transmisión del mismo dentro de la nueva red mediante el proceso TCP/IP, siempre y cuando exista conectividad hacia los servicio del ISP. (**Ver figura 36**)

Asimismo, en esta capa se presenta el protocolo de datagramas de usuarios (UDP) que permita establecer comunicación entre equipos, sin necesidad que existen conexión con internet, donde busca la velocidad absoluta del paquete mediante a red, donde no examina que existe perdida de los mismo, pero garantiza la estabilidad interna de la red al momento de presentar fallas con el protocolo TCP. Cabe destacar, que debido a que consideran protocolos TCP/UDP para la nueva red está siempre mantendrá conectividad, sin importar que exista fallos el proveedor de internet. (**Ver figura 36**)

Luego, encontramos la capa de sesión donde se establecen mecanismo para abrir, cerrar y administrar una sesión dentro de un equipo de red o administrativo. Donde se determinó que los protocolos necesarios para la nueva red, encontramos primero el protocolo de túnel de punto a punto que permitirá establecer túles de conexión segura entre dos hosts, donde dependiendo de las asignaciones de IPv4 aginadas podre consignar respuesta entre ellos. Asimismo, este modelo de protocolo es recomendado para sistemas operativos Windows, donde a pesar que actualmente no es tan implemento, este permite poder mantener una línea segura dentro de la red.

Equipo	Servicio	Departamento	IP	
Laptop0	Admin	Despacho	Estática	
Pc2		Coordinadora de Despacho		
Pc1		Administración Central		
Pc3	No-Administrador	Auditoría Interna	Dinámica	
Pc4		Atención al Cliente		
Pc5		Recursos Humanos		
Pc6		Dirección de Control de la Administración de entidades descentralizadas	Estática	
Pc7			Dinámica	
Pc8				
Pc9				
Pc10			Estática	
Pc11				
Pc12		Dirección de Control de la Administración Central		
Pc13				
Pc14				
Pc15		Dinámica		
Imp0	-	Despacho	Estática	
Imp1		Administración Central		

Cuadro 8. Configuración de las direcciones y servicios de los equipos administrativos de la nueva red.

Fuente: Elaboración Propia. (2022)

De esta manera, en el **cuadro 8** se visualiza el control acceso en los equipos informáticos de la nueva red, donde se determinan parámetros de administrados y usuarios, normalizado bajo un sistema operativo de Windows 10 PRO para todos los equipos. El usuario Admin tendrá disposición total a la red interna, donde se establecen protocolo de control de sesiones (SCP) de manera que determine si el equipo puede acceder a la información almacenada en los servidores, logrando así solicitar acceso mediante el envío de paquetes hacia otro dispositivo que no tenga su mismo nivel o rango, por otra parte, el usuario no-administrador solo podrá acceder a información relevante para su cargo. Además, para determinar acceso a los servicios de la red, se determinó un protocolo de autentificación de contraseña (PAP) que permite proteger la nueva red contra posibles amenazas.

Asimismo, cada dispositivo dependiendo de la función de acceso de tenga se le establece una dirección estática (administrador) o dinámica (no-administrador). Sin embargo, para máquinas

reguladoras de cada departamento se establece a un equipo con dirección IP estática que permiten ser polito de control para cada segmentación de la red mediante un protocolo de información de zona (ZIP). De la misma forma, para la configuración de las maquinas auxiliares (impresoras) se le considera administrar un servicio de dirección IP estáticas para los equipos de manera permitan identificar el acceso de los usuarios a sus servicios mediante el mismo protocolo ZIP.

Por otra parte, para garantizar la comunicación entre los equipos de la nueva alámbrica se determina un protocolo de mensaje de corta de igual a igual (SMPP) que permite poder comunicar a equipos (PCs) entre si de una manera rápida y segura, debido a que va a permitir gestionar a la información enviada mediante el control del Gateway de la red, es decir, el direccionamiento IP de router que brinda servicio hacia el ISP.

Dentro de esta capa (sesión), se establece la configuración interna dentro del servidor Proxy para el cual se determina como sistema operativo a Linux en el entorno Ubuntu, administrado mediante el servicio Ubuntu Server 20.04.1 LTS, con capacidad una capacidad de 4 GB de RAM, que a su vez se proporciona 500 GB de disco SSD. Así mismo, se sustentan una línea de enrute hacia el Gateway (router) de manera de proporcionarle conectividad con internet.

En otro orden, encontramos la capa de presentación la cual se determina como va a poder reflejarse la información transportada en la nueva red. Debido a ello, se consideran las metodologías de trabajo de la Contraloría, concluyendo entonces que se necesita manjar modelo de archivos de Documento (DOC), ya que constantemente implemente este modelo para el llenado de nuevo informes, así mismo, se determina el modelo de formato portátil de documento (PDF) dado a que los informaciones, registros o leyes que se utilizan en el Organismo viene basados en dicho formato.

Por otra parte, de establecen extensiones de archivos de Email debido a que es la principal herramienta para él envío de información fuera de la Contraloría. Además, se establecen los formatos de imagen (JPG) debido a existen documentos o leyes que contiene este tipo de documentación. Asimismo, se considera un lenguaje de hojas de estilo extensible (XSL) debido a que procesos de llenado de nómina establecido por el servidor local de la Contraloría contiene este modelado. Y, por último, se establece el lenguaje de marcado de hipertexto (HTML) dado a que los equipos deben acceder la información web dentro de la red.

Para finalizar con las capas de la red, encontramos la cada de aplicación donde se consignan los protocolos de servicios que ayudaran a la nueva red a cumplir con los niveles de seguridad y

control para las transferencias de los datos. Donde se determinó que la configuración óptima para el nivel se necesita la implementación de los protocolos de servicios de transferencia de hipertexto (HTTP/HTTPS) de manera que permitan la negación web de los equipos. Así mismo, se establecerá un protocolo para la trasferencia de archivos de versión 4 (FTP) de manera que se permita compartir paquetes desde un equipo hacia otro.

De la misma manera, en este nivel de aplicación se establece un protocolo de transferencia de archivos trivial de manera que permita guarda una petición establecida por el (FTP) ayudando transportar los datagramas desde un punto lejano de la red hacia otro, mediante el analizar previo del equipo de red. Por otra parte, para poder establecer niveles de direccionamiento dinámicos se determina el uso de un protocolo de configuración dinámica de host.

Protocolo	Ubicación	Límite	Gateway
DHCPv4	Servidor Proxy	100 host	Router

Cuadro 9. Protocolo DHCP de la nueva red.

Fuente: Elaboración Propia. (2022)

En el **cuadro 9**, se visualiza la configuración inicial del protocolo DHCP. Donde se determinó que necesaria una ruta de enlace directo hacia el router de manera que permita establece conectividad hacia internet a aquellos equipos administrativos que presenten un direccionamiento dinámico, por otra parte, se considera un límite máximo del servicio de cien (100) host, dando cabida a que, si en el futuro existe una expansión de la red, este protocolo puede soportar dicho crecimiento. Y, además, se distingue que este servicio debe estar ubicado dentro del servicio proxy para su control.

Por parte, dentro de esta misma cada de aplicación estima la necesidad de implementar un protocolo de tiempo de red (NTP) que permita medir la sincronización de los equipos host (PCs) dentro de la red, mediante el mapeo de su direccionamiento IP para aquellos dispositivos que presenta dirección estáticos y por mapeo de la MAC del equipo para equilos que se les administre direcciones dinámicas, basados en el protocolo UDP. Y, por último, se considera la implementación de un protocolo de sistema de nombres de dominios (DNS) de manera que proporcionar una dirección de enlace directa hacia cualquier servicios o equipo dentro de la red el cual presente un direccionamiento estático, garantizando de esta manera aumentar las velocidades de respuesta dentro de la nueva red.

Dentro de esta capa (aplicación), se determinan las configuraciones finales del servidor proxy, en donde se desactiva el sistema de protocolo SMB para evitar vulnerabilidad externa hacia el servidor, por lo cual se establecen interfaces de acceso para el puerto 19 para conexión IPv4 TCP/UDP, en conjunto con la configuración del puerto 21 para la inicialización del servicio FTP. Además, se administrar de forma abierta el puerto 80 para peticiones HTTP/HTTPS en la web mediante el transporte o cola del servidor. De la misma manera, se establece un método manual para el control de acceso al servicio DHCP. En este mismo sentido, para generar los niveles de acceso dentro de la capa de sesión, se considera las direcciones IP del conjunto de servicios que conforman la nueva manera de que están proporcionados dentro de almacenamiento del mismo servidor.

Particiones	Disponibilidad	Formato
BIOS	1 GB	Disco Local
Root	50 GB	Ext4
Memoria I.	30 GB	Swap
Destino	-	Home

Cuadro 10. Configuración del CPU para la implementación del servidor Proxy.

Fuente: Elaboración Propia. (2022)

Para dirección de acceso hacia el servidor proxy se establece la dinámica inicial <http://mx.archive.ubuntu.com/ubuntu>, actuando como Host central de los servicios en función de encaminar las peticiones aceptadas para cada dispositivo administrativo o equipo de red perteneciente a la infraestructura. Además, se determinan las particiones necesarias del servidor con su disponibilidad para reguardo de información y ejecución de procesos dentro de la nueva red. **Ver cuadro 10.**

Por otra parte, para finalizar con la configuración del Servidor Proxy se establecen las asignaciones finales del perfil para el acceso al sistema Ubuntu Server, mediante un acceso SSD para proporcionar comunicación interna dentro de la nueva red alámbrica dentro de la Contraloría Municipal de Antolín, estableciéndose: nombre, nombre del servidor, nombre de usuario con su respectiva contraseña para luego poder acceder al sistema del servicio, que permitan poder control de manera física al servidor Proxy en caso tal de ser necesarios para establecer nuevo protocolos o procesos en la red.

En otro orden de ideas, para la configuración física de la red se determina establecer direcciones de acceso para la red local de la nueva infraestructura trabajo bajo una subred de capa

24 para dar posibilidad a futuros accesos. La red estará establecida 3 zonas de control para regular y configurar la entrada de peticiones hacia la red. Teniendo así la zona de desmilitarizada denominada (DMZ) que funciona de receptor entre la nueva red alámbrica y la red proveniente del ISP.

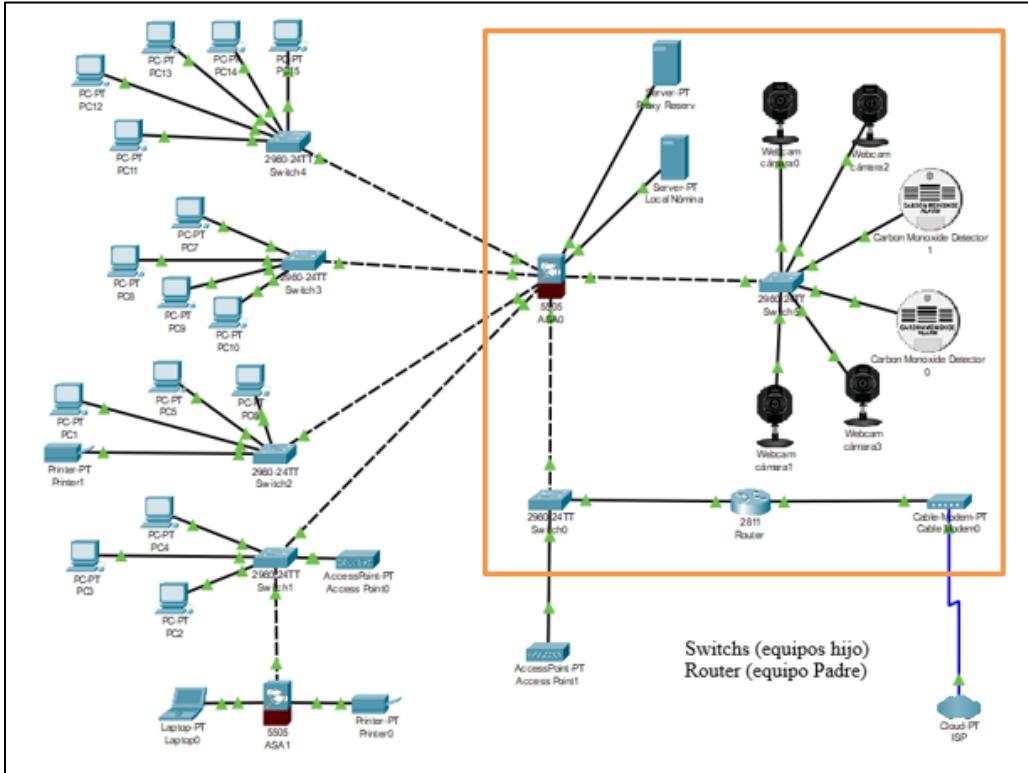


Figura 37. Zona DMZ de la nueva red.

Fuente: Elaboración Propia. (2022)

Por ello en la figura 37, se observa la zona desmilitarizada (DMZ) que mantendrá los Servicio HTTPS del servidor local de la Contraloría (Servidor de Nómina), además de implementar una dirección de enlace hacia el Gateway en conjunto con la conexión directa hacia el servicio Proxy mediante la puerta de enlace 21. Luego, encontramos la nueva red alámbrica la cual abarca dentro de su mismo espacio a la zona DMZ, sin llegar a interponerse los equipos que la conforman dentro de la zona desmilitarizada. Y, por último, tenemos a la red proveniente del proveedor de internet lo cual brindara conectividad de internet a la nueva red LAN.

En relación a los niveles de la seguridad física de la nueva red alámbrica, se determina una zona de control para el resguardo de todos los dispositivos de red y los servidores del sistema el cual contendrá los equipos necesarios para la protección física en caso de suceder algún evento

que pueda llegar a comprometer la vida útil de los equipos. Dentro de esta zona, se establecen equipo de vigilancia para llegar registro de las actividades realizadas dentro y fuera del lugar.

Cámara	IP	Mascara de red
0-3	Estáticas	24

Cuadro 11. Configuración cámaras de seguridad de la nueva red.

Fuente: Elaboración Propia. (2022)

Estos equipos de seguridad se determinan trabajar bajo los modelos de servicio de IPv4 dado que van a lograr establecerse direccionamiento de IP estáticos junto a una máscara 24 de red, de manera que se puedan identificar de forma rápida dentro de la nueva red. Sin embargo, estos elementos estarán conectados mediante una ruta enlace hacia la zona DMZ de manera que capaz de reflejar su contenido almacenado en un monitor(ver cuadro 11).

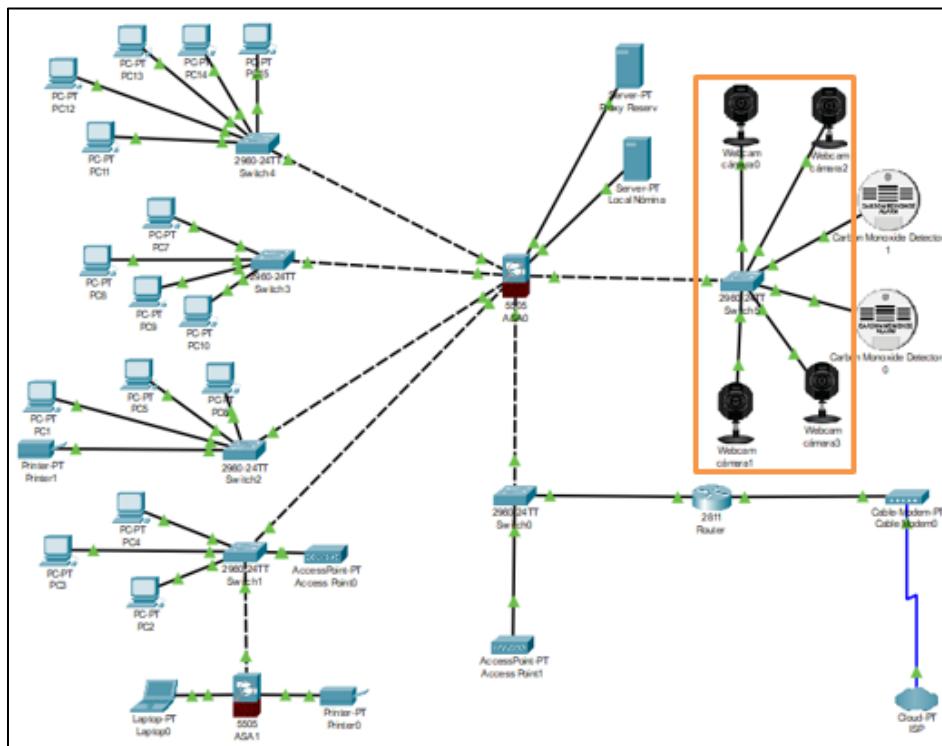


Figura 38. Adaptación de las cámaras de seguridad en la topología de la nueva red.

Fuente: Elaboración Propria. (2022)

Además, para establecer conexión global de acceso se configurada mediante la puerta de enlace hacia el Router permitida mediante la interconexión de un conmutador configurado para designar direccionamiento del equipo. Por otra parte, por medidas de seguridad lógica no se le

establece dirección directa hacia el servicio de dominio (DNS), de manera de prevenir vulnerabilidad en la nueva infraestructura de red. (**Ver imagen 38**)

Para culminar con la configuración optima de la nueva red, se designa un equipo especial para la detección de humo o monóxido de carbono en la zona de resguardo para así evitar incendios en el lugar(**ver imagen 38**). En caso de suceder el fenómeno mencionado se implementa equipos especializado control incendios eléctricos (extintores) que permitan control del mismo para evitar daño a los equipos de red de la Institución. De la misma manera, considerando que existen problemas eléctricos se establecen protectores de voltaje para todos equipos de la nueva red alámbrica de manera que logre brindar conectividad en momentos donde se cuenta el dicho servicio. Así mismo, para evitar sobrecalentamientos de los equipos se diseña dentro de la zona de resguardo con la implementación de un aire acondicionados especial para los equipos de red para generar un entorno idóneo para sus funcionamientos. Finalmente, se determina implementar dentro de esta zona desagües para evitar daños por inundaciones en los equipos de red.

PARTE V

LA PROPUESTA

5.1. Importancia de la aplicación de la propuesta

En la actualidad las redes de área local alámbrica representan un gran parte de las infraestructuras de red de una Instituciones debido a que permite comunicar de manera directa y rápido dispositivos dentro un entorno determinar, donde además se logra establecer puentes de acceso físicos para poder intercomunicar nuevos equipos dependiendo de las necesidad que se tengas, por otra parte este tipo de redes logran mantener una estabilidad de transporte de información (datos) mediante el uso de un determinado tipo cableado donde dependiendo de la marca, modelo y estándares que se manejen, pueden llegar a ofrecer grandes niveles de velocidad para subida y descarga de paquetes de archivo.

Así como también, este tipo de infraestructuras alámbricas logran ser de mayor confianza en relación a protección de sus datos, ya que se puede manejar de manera física la configuración de segmento que se quiere establecer en una sede permitiendo poder ser administrada por un Host (servidor) que cumpla con las capacidades que requiere el diseño de la red, este servidor va a permitir controlar mediante el uso protocolos de servicios a aquellos elementos, equipos o maquinas que requieran un sistema monitorio para seguridad.

Por lo cual, la importancia de la aplicación del diseño de la Red de Área Local Alámbrica para la optimización de la conectividad y seguridad de datos mediante un servidor Proxy para la Contraloría del Municipio Antolín del Campo recae, que principalmente va a mejorar su proceso de conexión de todos sus equipos permitiendo mantener relación de acceso directo hacia el servicio de internet, pero además va a lograr establecer conexiones directas para cada departamento que conforma el Organismo de manera que ayude a optimizar la mecánica de trabajo. Por otra parte, debido a la implementa de una red por cableado los niveles de velocidad establecidos van a ser compatibles con las necesidades de los dispositivos logrando de esta manera aprovechar toda la capacidad de ancho de bando que puede llegar a ser suministrada.

De la misma manera, este diseño va a garantizar poder mantener un proceso de confiabilidad en el manejo de la información que se tenga dentro de la red debido a que contara con protocolo de servicio de seguridad que permitan establece niveles de acceso hacia los elementos almacenadas en los servidores, donde además mediante las segmentaciones antes mencionadas lograran

brindar niveles de seguridad establecidas a cada espacio determinado permitiendo de esta manera poder manejar en un ambiente estable para los empleados de la Contraloría.

De la misma forma, se logra brindar soluciones de control de acceso directo a la red debido a que no diseñan conexiones abiertas en el nuevo diseño de red Alámbrica, generando de esta manera que no puedan ocurrir vulnerabilidad de terceros mediante conexión establecido por puntos de acceso, sino que tendrá que establecerse de manera física en la red, para lo cual se plantean niveles de seguridad lógica en equipos donde asignan niveles de servicio en relación con los tipos de usuarios que se establezcan.

Además, con respecto a problemáticas de fenómenos físicos como incendios o inundaciones que puedan llegar a ocurrir en la Contraloría, este diseño de red va resguardada y protegida en caso de esos sucesos donde se administra sistema de control y monitorio para los mismo, además de contar con equipo especializado para esos casos de manera de tal que permita garantizar el estados de los equipos de red logrando de esta manera resguarda la información vital de la Contraloría de forma que no existen perdidas de documentos, y retrasos de la operaciones que se manejen durante esos procesos.

Para finalizar con la importancia de la implementación de red para la Instituciones, se resalta que además de poder brindar los beneficios antes mencionados este diseño va a lograr poder establecer parámetros guías para que futuras Organizaciones Gubernamentales toman este modelo como ejemplo para su aplicación, generando así poder establecer a la Contraloría como potencia en relación al nivel infraestructura de red alámbrica en conjunto con los procesos de seguridad que conlleva la misma.

5.2. Viabilidad de la propuesta

5.2.1. Viabilidad Técnica

Para poder implementar el diseño de la red alámbrica se consideró diversos equipos que contiene ciertos requisitos para poder establecer una correlación con las maquinas actuales de la contraloría, junto a las necesidades que requiere el Organismo para su funcionamiento adecuado, permitiendo de esta manera poder mantener un control mediante configuraciones lógicas más sencillas para dispositivo o equipo a implementar.

Planta	Nombre	Modelo	Características
Interna	Cableado de Red	UTP Categoría 5e	Cableado de par trenzado UTP ethernet de color azul categoría 5e para interior con capacidad de transporte de data de 10-1000 Mbps.
	Conector Interfaz física	Rj-45 Categoría 5e	Conectores para equipos de red para modelo de cableado ethernet Cate 5e/6 de color blanco para rutas de enlace físico con capacidades de 10-1000 Mbps.
	Botas de Red	Categoría 5e/6	Elemento de red para protección de los conectores de entrada del cableado Ethernet, con capacidad para modelo de Categoría 5e en adelante con cubierta resistente de color azul.
	Tomas de red	X20TT	Toma de red para 4 set de color blanco con tapa De Red 1-2-4 puertos para Jack.
	Modem	sb6121 Soundfreadks	Equipo Surfboard de Cable de extremo modelo sb6121 Soundfreaks Inter con capacidad de descarga de hasta 50-100 megas, no presenta adaptador a red Wireless, ni puerta de entrada para telefonía VoIP, cuando solo con un puerto de entrada Gigabit Ethernet para conexión directa por ordenador o Router
	Router	TW100-S4W1CA	Enrutador neutro de color negro, con cuatro (4) puertos de entrada ethernet, con capacidad de manejo de velocidad de 10-100 Mbps mediante procesos de full-dúplex y half-dúplex, con asignación de protocolo TCP para versiones de direccionamiento de tipo 4
	Cortafuegos	ASA 5005	Dispositivo CISCO de seguridad de red manejado mediante control remoto, con dimensiones 12,25 x 9,8 x 6 de ancho, modelo 6 x 10/100Base-TX LAN, 2 x 10/100Base-TX - 1 x SSC / ASA5505-50-BUN-K8, con 8 puertos de entrada Gigabit Ethernet.
	Comutador	Switch TP- TS-SG1024S	Equipo para administración de tráfico de red Switch d de color negro, sin ventilación y de material resistente. Con capacidad de conector de 25 Gigabit Ethernet.

	Máquina	HP Z640	Equipo con servicio de torre de servidor - Intel, Xeon E5-2690 V3, con una frecuencia de 2.6GHz, con procesador 12 Core, con capacidad de 32GB DDR y 8 RAM. Presenta un controlador de discos LSI 9217 4i4e SAS SATA, con disco sólido Enterprise de capacidad de un 1TB - NVS 310 512MB - 925W PSU.
	Máquina	HP LTSC	Con Sistema operativo Windows 10 Enterprise, además cuenta con un Procesador Intel Core i5-3570s, con manejo de frecuencia de 3.10 GHz, x64 bits. Por otra parte, tiene capacidad de 500 Mb de almacenamiento.
	Fuente de alimentación ininterrumpida	USP APC	USP inteligente de 1500 VA con SmartConnect, modelo SMC1500C Sinemawe, con batería de reserva, AVR de 120V.
	Cámara de seguridad	Swann	Cámara de seguridad inteligente de color blanco con capacidad de resolución 1082 Full HD de conectividad alámbrica/inalámbrica con detector verdadera PIR de color/movimientos, visión nocturna y radio.
	Lámpara de emergencia	GEL	Lámpara de Emergencia Led MARCA: GEL 110v-277V, Luz Blanca 6500K Duración de Iluminación encendida de 90 Minutos encendido Somos Tienda Física De Iluminación Led
	Armario	RK4242BK24	Armario para Rack de servidor / equipos de red de 42U, con profundidad ajustable de 4 postes (5,2" a 35"). Con un espacio compartido que funciona como caja de rack (4) para equipos de red de TI con ruedas, con un peso de total 3315 libras, con disponibilidad para conexiones de voltaje directo.
	Monitor	1D0J9AA #ABA	HP Monitor FHD de 24 mh - Monitor de computadora con pantalla IPS de 23,8 pulgadas (1080p) - Altavoces incorporados y montaje VESA - Ajuste de altura / inclinación para visualización ergonómica - HDMI y DisplayPort -

			I24.
	Detector de Humo y Monóxido de Carbono	Kidde 21026043	Kidde - Detector de monóxido de carbono y humo, funciona con pilas, alarma combinada de humo y monóxido de carbono con alerta de voz. De medida 1.8 x 5.6 x 5.6 pulgadas.
	Extintor de fuego	FE-36	Ansul CleanGuard modelo FE-36 a base de hidroflourocabono, sin ODP. Preventivo contra daños a los equipos de red, con una eficacia de extensión superior, además de ser mejores para el ambiente. De clase B para líquidos inflamables y clase C para equipos eléctricos. Marca Amerex B386T de 5 libras, con soporte incluido.
	Protectores de voltaje	BSEED	Protector de sobretensiones electrónico para electrodomésticos, protector de voltaje para refrigeradores, congeladores, aires acondicionados y equipos de red, salida de voltaje de 220 V, 20 A, 4400 vatios.
	Desagüe	GP-6839	Desagüe Anti-olor de color gris para Baño Centrales, formado por una aleación de Acero y cobre con medidas 4x4.
	Aire Acondicionado	S-120 UM	Aire Acondicionado Split 12000 Btu 110v, para funciona de refrigeración de zonas cerrado, con controlador de humedad.
Externa	Canaletas	StarTech	Canaletas para tomas de corriente de color negro de capacidad de 110v, con regular interno de voltaje para medidas de control.
	Cableado de red	UTP Cat5e	Cableado de par trenzado UTP ethernet de color azul categoría 5e para interior con capacidad de transporte de data de 10-100 Mbps.
	Conector Interfaz física	Rj-45 Categoría 5e	Conectores para equipos de red para modelo de cableado ethernet Cate 5e/6 de color blanco para rutas de enlace físico con capacidades de 10-100 Mbps.
	Jack Coupler	Categoría 5e	Conector físico Jack coupler inserto de color blanco para cableado de red
	Lámpara de emergencia	GEL	Lámpara de Emergencia Led MARCA: GEL 110v-277V, Luz Blanca 6500K Duración de Iluminación encendida de

			90 Minutos encendido Somos Tienda Física De Iluminación Led
	Router	Tplink TI-we	Router de color negro con entrada de acceso WiFi y de red, con capacidad de descarga de 600 Mbps. Implementado con dos antenas para señal, con un estándar de Wifi 4
	Router	Tplink Tl-wdr3500	Router de color negro con entrada de acceso WiFi y de red, con capacidad de descarga de 450 Mbps. Implementado con dos antenas para señal, con un estándar de Wifi 4

Cuadro 12. Equipos de planta interna y externa de la nueva red.

Fuente: Elaboración Propia. (2022)

Asimismo, en el **cuadro 12** se indican los equipos necesarios para el funcionamiento óptimo de la nueva propuesta de red alámbrica. Del mismo modo, dichos equipos estarán distribuidos de la siguiente manera: una planta interna en la cual se encontrarán aquellos elementos que no serán manipulables al exterior, sino que estarán resguardados en una zona de seguridad bajo vigilancia; y, una planta externa donde estarán todos aquellos equipos o elementos que si permanecerán expuestos al exterior y al personal de trabajo.

Entre los elementos mencionados se encuentra en primer lugar los cables de red, encargados de conectar todos los equipos de la red proporcionándoles velocidades de 10 a 1000 Mbps, y sirviendo como medio físico de transporte de la información. También, se hará uso de conectores físicos Rj45, los cuales irán en un extremo de los cables de red y serán los encargados de surtirles la conexión a los equipos. Dichos conectores tienen compatibilidad con cableado de categoría 5e en adelante, lo que evita pérdida de velocidad al momento de enviar los datos por el cableado.

Igualmente, se usarán botas de red para proteger los conectores Rj45 y fijar aún más el cable al equipo. Siguen las canaletas, las cuales tendrán 3 compartimientos, una cubierta de metal y permitirán, en primer lugar, proteger el cableado y segundo, dividir las conexiones a cada departamento. De la misma forma, para conectar de manera sencilla el cableado UTP antes mencionado, es necesario implementar tomas de red de manera que el proceso de conexión sea más eficiente, permitiendo ahorrar en material a nivel cableado y mejorar la protección del mismo.

Ahora bien, para recibir la señal internet proporcionada por el ISP, se utilizará el mismo Módem Motorola de la Contraloría, el cual a pesar de su antigüedad es de los dispositivos más actualizados dentro del Organismo, con velocidades de 50 a 100 Mbps; además de ser uno de los equipos de mayor durabilidad ya que sus procesos de trabajo no son de alta intensidades. Para poder convertir dicha señal de internet captada por el Módem se usará un Router Tp-link con Wifi 5, capaz de recibir solicitudes de servicio provenientes de 40 dispositivos o más simultáneamente.

Por otra parte, se implementará un Switch Tp-link de 24 puertos de entrada para distribuir las conexiones hacia cada departamento y permitiendo establecer futuras conexiones en caso de ser necesario. Del mismo modo, se necesitará un cortafuego ASA 5005 responsable de establecer niveles de segmentación del ancho de banda del internet, así como también permite establecer niveles de entrada y salida, reforzando la seguridad interna de la red. Por otro lado, debido a los constantes cortes de luz, será necesaria una fuente de alimentación ininterrumpida o UPS capaz de suministrarle electricidad a los equipos durante 4 horas y media aproximadamente; además de contar con baterías recargables en tal caso que se necesite un mayor uso del mismo.

Igualmente, se hará uso de un armario para Rack para resguardar los equipos de red y que se ajusta a medida que se vayan ubicando los equipos en él; cuenta además con material libre de electromagnetismo para evitar inestabilidades en la red. También se usará un CPU que se configurará para funcionar como servidor Proxy. Asimismo, se mantendrá el CPU de servidor de nómina de la Contraloría, ya que tiene la capacidad de soportar mayores cargas de datos sin verse reflejado en su rendimiento.

En cuanto a la zona de resguardo, se instalarán cámaras de seguridad marca Swann y resolución Full HD 1080 integradas con detector de rostro y movimiento, para así mantener un control de acceso a la misma. Para visualizar las grabaciones y monitorear al personal, se usará un Monitor HD con la misma resolución de las cámaras.

Por otro lado, se implementará un detector de humo y monóxido de carbono que alerte en caso de un incidente y mida los niveles de temperatura en la zona de resguardo. Ahora bien, en caso de incendio se usarán extintores especiales de clase B:C, cuyo diseño permite apagar el fuego sin dañar los equipos. También, se colocarán desagües para casos de inundaciones en la zona. Cabe resaltar, que se instalará un aire acondicionado que funcionará como elemento de

refrigeración y evitará niveles de humedad elevados, además de mantener una temperatura adecuada.

Luego, se hará uso de regletas con múltiples tomas para conectar varios equipos de red y así facilitar el mantenimiento de los mismos, además de servir como reguladores de voltaje, es decir, proporcionarán niveles de voltaje adecuados para cada equipo protegiendo la integridad de cada uno. Finalmente, se implementarán protectores de voltaje que protejan a los equipos ante subidas de tensión que atenten contra su funcionamiento.

5.2.2. Viabilidad operativa

Para el nuevo diseño de la red alámbrica de la Contraloría, se toman en consideración diversos factores que le permitan poder establecer un óptimo funcionamiento en relación con su viabilidad operativa, por lo cual esta red cuanta con procesos y servicios internos que permiten mantener conectividad completa en todas las áreas, junto con la protección adecuado de cada proceso que se genere al momento de iniciar algún transporte de data por la nueva infraestructura.

Dado a la designación del servicio de direcciónamiento de versión 4 establecido en la configuración óptima de la red, estos estándares de trabajo deben contar con un sistema de vigilancia lógica de manera que se puede llegar a visualizar las direcciones de los hosts (PCs) dentro de la red, dado caso se necesite cambiar el IP de este equipo. Por esta razón, para garantizar el funcionamiento de diseño de la nueva red LAN es necesario contar con personal capacitado para su resguardo a nivel de procesos internos.

Cantidad Personal	Cargo	Trabajo
1	Soporte Técnico	Resolver problemas de origen físico dentro de la red
1	Ing. en Telecomunicaciones/ Sistemas	Resolver inconveniente de origen lógico en la red
1	Administrador de redes	Llevar control de los servicios de la red, junto a los mantenimientos (servidores/equipos de red)

Cuadro 13. Personal necesario para la viabilidad operativa de la nueva red.

Fuente: Elaboración Propia. (2022)

Para ello en el **cuadro 13**, se determina la necesidad de contar equipo de soporte técnico que será capaz de resolver conflicto por origen físicos debido a que pueden ocurrir daños con el cableado asignado en los equipos y maquinas, además se debe contar con un ingeniero de

telecomunicación o de sistemas con experiencia en el área de redes alámbricas para poder asegurar resguardo de los datos lógicos de la infraestructura de red y por ultimo contar con un administrador de redes con capacidad para llevar control los servicios actuales de red, junto a los nuevos que se puedan ir asignando a manera que sea capaz de proporcionar direcciones IP, cambios o configuraciones de acceso dentro de los servidores o asignar nuevas mecánicas de trabajos para los usuarios en la red.

Equipo	Duración entre mantenimientos	Personal encargado
Equipo de red	3 meses	Ing. Telecomunicaciones/Sistemas
Equipos administrativos	3 meses	Técnico en Computación
Servidor Local de Nómina	6 meses	Administrador de redes
Servidor Proxy	5 meses	
Cableado	4 meses	Soporte Técnico

Cuadro 14. Guía para los mantenimientos de la nueva red.

Fuente: Elaboración Propia. (2022)

Para finalizar con el óptimo manejo de la red, se establecen los procesos de mantenimiento (**ver cuadro 14**), debido a que se establecen conexiones por cableado ethernet es necesario establecer pruebas de testeo cada cuatro (4) meses para determinar si existen pérdidas de velocidad o bajas de latencias en algún sector de la red cuando hay un tráfico elevado de paquetes, permitiendo verificar si existen cortes de cable. Además, se debe hacer mantenimiento cada tres (3) meses de los puertos de entrada de los equipos debido a que pueden ocurrir cortes superficiales de los conectores Rj45 hacia el cable de red. Por otra parte, se deben realizar pruebas cuatrimestralmente dentro de los equipos de la red mediante ping de alta frecuencia para intentar colapsar la red a manera de determinar las fallas que puedan estar ocurriendo.

De la misma forma, para mantener control a nivel de mantenimientos del servidor local de nómina se recomienda realizar análisis interno cada 6 meses de manera de evitar desconfiguraciones de los servicios internos, y además de mantener registro de todos los procesos que se han realizados de forma que permita detectar si existen infecciones de agentes maliciosos dentro del servidor. (**Ver cuadro 14**)

Por otra parte, para el mantenimiento del servidor proxy se determinó un periodo entre mantenimiento de cinco (5) meses (**ver cuadro 14**), mediante el comando “*apt update*” para

determinar si existen actualizaciones de paquetes para permitir proporcionar los mejores servicios a la red sin, sin embargo, se debe mantener sumo cuidado con este proceso, ya que puede generar un descontrol interno en la red como desconfiguraciones de servicios y direccionamientos IP.

5.2.3. Viabilidad económica

Para hacer posible la implementación de la nueva red, se necesitarán una serie de equipos y materiales los cuales se presentarán en la tabla a continuación. Igualmente, al final de dicha tabla se encuentra el total de la inversión en cuanto a materiales, esto sin agregar los honorarios de los profesionales. Asimismo, se menciona la importancia de implementar esta propuesta en la Contraloría, los beneficios económicos y el cambio que significará en su día a día y, además, posibles casos de cómo podrían sacarle el máximo provecho a la nueva red.

Nombre	Descripción	Cantidad	Precio Unitario	Total
Cable de Red	Cableado Ethernet Cat5e UTP interior bobina de 100 metros	3	\$39,00	\$117,00
Botas de Red	Color azul para cableado 5e. Paquete de 100 unidades	1	\$8,00	\$8,00
Conectores de Cableado	Conektor Rj-45 Cat5e. Paquete de 100 unidades	1	\$6,00	\$6,00
Canaletas de Red	Canaleta para cableado de red de 2 compartimentos de color blanca de 3 metros	79	\$3,00	\$237,00
Switch TP-Link	Switch 24 Puertos 10/100 Mbps Tplink Desktop Switched Red Rj45	6	\$137,50	\$825,00
Cortafuegos	Cisco Firewall de seguridad de 8 puertos Gigabit Ethernet (GbE).	2	\$1.250,00	\$2.500,00
CPU	HP Z640 Tower Server - Intel Xeon E5-2690 V3 2.6GHz 12 Core - 32GB DDR, con 8 RAM	1	\$750,00	\$750,00
UPS	UPS APC color negro de 1500VA	1	\$354,89	\$354,89
Monitor	HP Monitor FHD de 24 mh - Monitor de computadora con pantalla IPS de 23,8 pulgadas (1080p)	1	\$80,00	\$80,00
Detector de Humo y Monóxido	Kidde - Detector de monóxido de carbono y humo. Kit de 2 unidades	1	\$44,99	\$44,99
Extintor de incendios	Extintor recargable estándar para el hogar, clasificación UL 1-A:10-B:C. Kit de 4 unidades	1	\$484,00	\$484,00

Nombre	Descripción	Cantidad	Precio Unitario	Total
Regleta	Crst Regleta Protectora Contra Sobretensión 12 Toma 4050	4	\$135,00	\$540,00
Cámara de seguridad	Swann - Cámara de seguridad de interiores. Pack de 4 unidades	1	\$539,00	\$555,17
Armario	StarTech Armario para rack de servidor 20U. Caja de rack para equipos de red de TI con ruedas. Con ventilador para cada rack	1	\$249,99	\$257,49
Tomas de Red	Toma de red para 2 set de color blanco con tapa De Red 1-2-4 Puerto	24	\$6,50	\$156,00
Protector de Voltaje	BSEED Protector de sobretensiones electrónico para electrodomésticos, salida de voltaje de 220 V, 20 A, 4400 vatios (1 paquete)	4	\$12,99	\$51,96
Aire Acondicionado	Aire Acondicionado Split 12000 Btu 110v	1	\$463,90	\$463,90
Jack Coupler	Conector físico Jack Coupler in-serto de color blanco para cableado de red Categoría 5e. Paquete de 10 Unidades	10	\$19,99	\$199,90
Lámpara de Emergencia	Lámpara Led de emergencia contra	2	\$30,00	\$60,00
TOTAL				\$7.191,3

Cuadro 15.Presupuesto para la compra de los equipos y elementos de la nueva red.

Fuente: Elaboración Propia. (2022)

Nombre	Valor
Costo del traslado de la compra de los equipos/elementos de la red	\$150,26
Costo por el personal capacitado	\$1.500
Costo para el mantenimiento de la red	\$1.200
Costo para la construcción de la zona de resguardo y taladrar el cableado	\$1.200
TOTAL	\$4.050,26

Cuadro 16. Presupuesto para el contrato del personal, mantenimientos y traslado de compra.

Fuente: Elaboración Propia. (2022)

Nombre	Valor
Presupuestos de contrato, manteamientos y traslado	\$4.050,26
Presupuestos de compra	\$7.191,3
Total Inversión	\$11.241,56

Cuadro 17.Costo total de la inversión.

Fuente: Elaboración Propia. (2022)

En el **cuadro 15**, se observa la inversión de compra de los equipos necesarios para el diseño de la nueva red, además se determinan los precios necesarios para el traslado de los equipos y elementos que se implementarán en la nueva red, dado a que algunos de ellos se ven la necesidad de traerlos fuera del Estado Nueva Esparta. Así como también, el costo para la contratación del personal capacitado para el manejo óptimo de la nueva red alámbrica y juntos a los costos necesarios para su mantenimiento, tomando como estándar un valor de 10% de la inversión inicial(**ver cuadro 16**). Por otra parte, se determina el valor total de inversión generada mediante la suma de todos los factores. un valor de inversión total para el diseño de la nueva red de cien mil ochocientos catorce con cincuenta y tres (\$10.814,53) dólares estadounidenses (**ver cuadro 17**).

Tomando en cuenta tanto la situación económica actual que se vive en el país como las necesidades de los trabajadores de la Contraloría, la implementación de una red alámbrica en lugar de una inalámbrica representa la mejor opción para la Institución, puesto que la red cableada conlleva un costo mucho menor. Así pues, se procedió a diseñar una propuesta cuyo presupuesto estuviera dentro del alcance de la Contraloría y, que, al mismo tiempo, les permitiera a los empleados trabajar más cómodamente y de manera más eficiente, satisfaciendo sus necesidades y atacando los fenómenos observados. Cabe resaltar que la Contraloría al ser un órgano estatal, es el Estado el encargado de suministrarle a la Institución el capital necesario para llevar a cabo dicha inversión, la cual a su vez se refleja en el presupuesto inicial de cada año gubernamental.

Otro punto importante a tener en consideración con este tipo de red alámbrica es que, siempre y cuando se les den a los equipos el cuidado que ameritan, pueden llegar a durar varios años; por lo tanto, esto se traduce en un ahorro de capital a largo plazo ya que no será necesario invertir en hardware constantemente. En relación a la idea anterior, se decidió facilitar un espacio dentro de la Institución para resguardar los servidores; con esto se procurará que dichos equipos estén

expuestos y se dañen ante cualquier eventualidad y deban ser reemplazados por otros nuevos, generando un gasto extra. Igualmente, tanto los costos de instalación como de mantenimiento de una red alámbrica son menos elevados que los de una red inalámbrica, lo que también es otro gran beneficio.

También, la implementación de esta nueva estructura de red le brindará a la Contraloría diversas ventajas como un notable aumento en su productividad, pues gracias al cableado de red la información podrá viajar por los equipos mucho más rápido y de manera más segura, evitando la pérdida de paquetes y permitiendo que todas las máquinas cuenten con acceso a internet. Al mismo tiempo, los empleados podrán ahorrar horas de trabajo, ya que con la nueva propuesta se configurarán los equipos de tal manera que permitan conectar muchos más dispositivos a la red de los que existen actualmente en la Contraloría. Con esta nueva configuración ya no será necesario que deban desconectarse varios computadores para que otros puedan funcionar, logrando así agilizar el flujo de trabajo y evitando que los empleados deban quedarse horas extras para poder cumplir con sus labores.

Igualmente, otra gran ventaja dentro de esta propuesta es que se reutilizarán varios recursos que ya tiene la Contraloría, tal es el caso de un Router Tp-Link de 600 Mbps, un Modem Motorola Surfboard sb6121, un Servidor Local de Nómina y un Router (amplificador) Tp-Link de 450 Mbps; debido a que dichos elementos cumplen con los estándares necesarios establecidos en el nuevo diseño, lo que representa un ahorro monetario.

Ahora bien, con esta nueva propuesta la Contraloría podrá aprovechar mucho más la red implementando nuevos servicios a largo plazo, lo que permitiría la automatización de los procesos y facilitaría un poco más el manejo de la información, además de aportarle al lugar un sistema de trabajo más novedoso. De igual forma, el diseño propuesto también permite administrar los recursos de la Contraloría, ya que en caso de que los trabajadores necesiten agregar más periféricos a la red, como una impresora, por ejemplo, se puede configurar la misma para que varios departamentos hagan uso de la misma impresora y así evitar un gasto mayor en varios de estos equipos.

5.3. Objetivos de la propuesta

5.3.1. Objetivo General

Diseñar una Red de Área Local Alámbrica para la optimización de la conectividad y seguridad de datos mediante un servidor Proxy en la Contraloría del Municipio Antolín del Campo.

5.3.2. Objetivos Específicos

1. Establecer niveles de direccionamiento IP a los equipos claves dentro de la nueva red.
2. Construir segmentaciones mediante VLANS para mejorar el flujo de paquetes en la nueva red alámbrica.
3. Lograr establecer conexiones de punto a punto, y de punto a multipunto para el control de las velocidades de los equipos administrativos.
4. Especificar un nivel de control-petición de servicios para mejorar la seguridad interna de la red alámbrica.
5. Incorporar un servidor proxy como regulador de protocolos de servicios de la nueva red alámbrica.
6. Mejorar la conectividad de los equipos administrativos y de red de la contraloría.

5.4. Estructura y representación gráfica de la propuesta

Para la estructura del nuevo diseño de la red alámbrica se consideraron diversos factores que permiten determinar las zonas y áreas de servicio que brindan conectividad a los equipos de red junto a las máquinas administrativas de cada departamento, por lo cual se configuran direccionamientos IP desde el cortafuego (ASA0) con diferentes destinos del Gateway (Router) para lograr tener independencia de acciones dentro de la red.

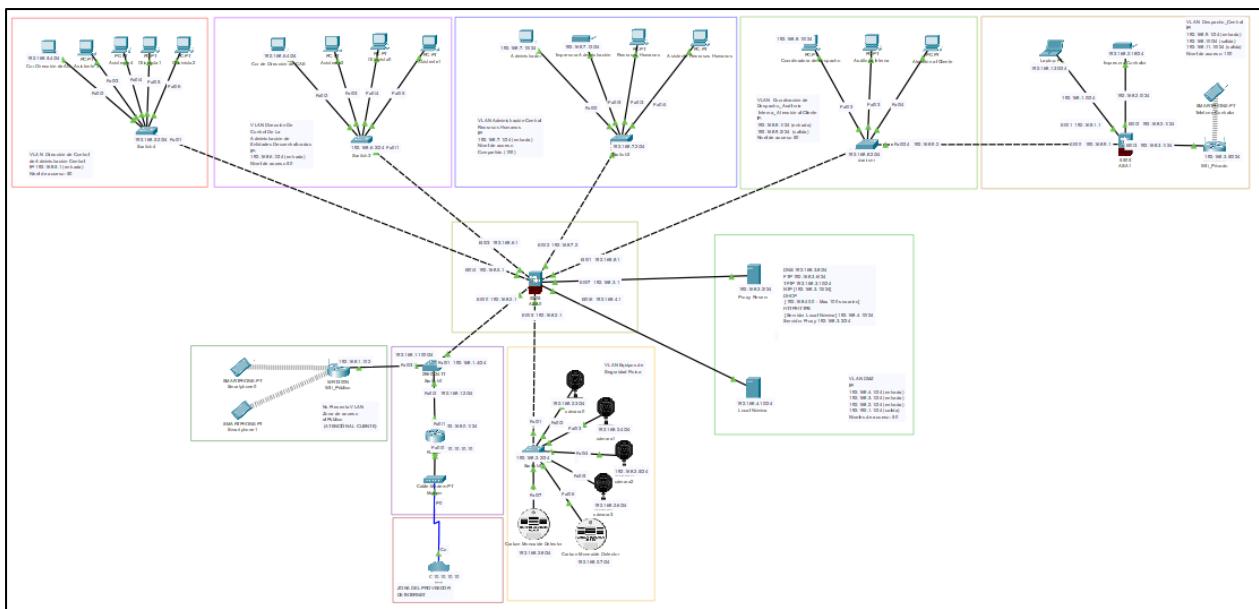


Figura 39. Topología de red detallada con las segmentaciones de red.

Fuente: Elaboración Propia. (2022)

En la **figura 39**, se identifican la estructuración representación lógica de la nueva red, donde se establecieron puertos de conexión física para los equipos de red y máquinas administrativas basadas en un direccionamiento inicial de la red de 192.168.0.0/24. Por otra parte, se estableció la dirección (10.10.10.10) proveniente del servicio de ISP mediante el cual los equipos administrativos (pc) usaran para acceder a los servicios de internet.

Luego de esto, se establece un equipo principal dentro de la red (cortafuego) el cual trabaja bajo el de dirección de la red, brindando de esta forma segmentaciones a través de círculos virtuales para cada zona identificada en la figura 40, mediante la asignación de sus puertos de conexión ethernet que abarcan desde la 0/0 hasta 0/7, donde cada uno de ellos se le proporciona un puente de manejo para direcciones IP.

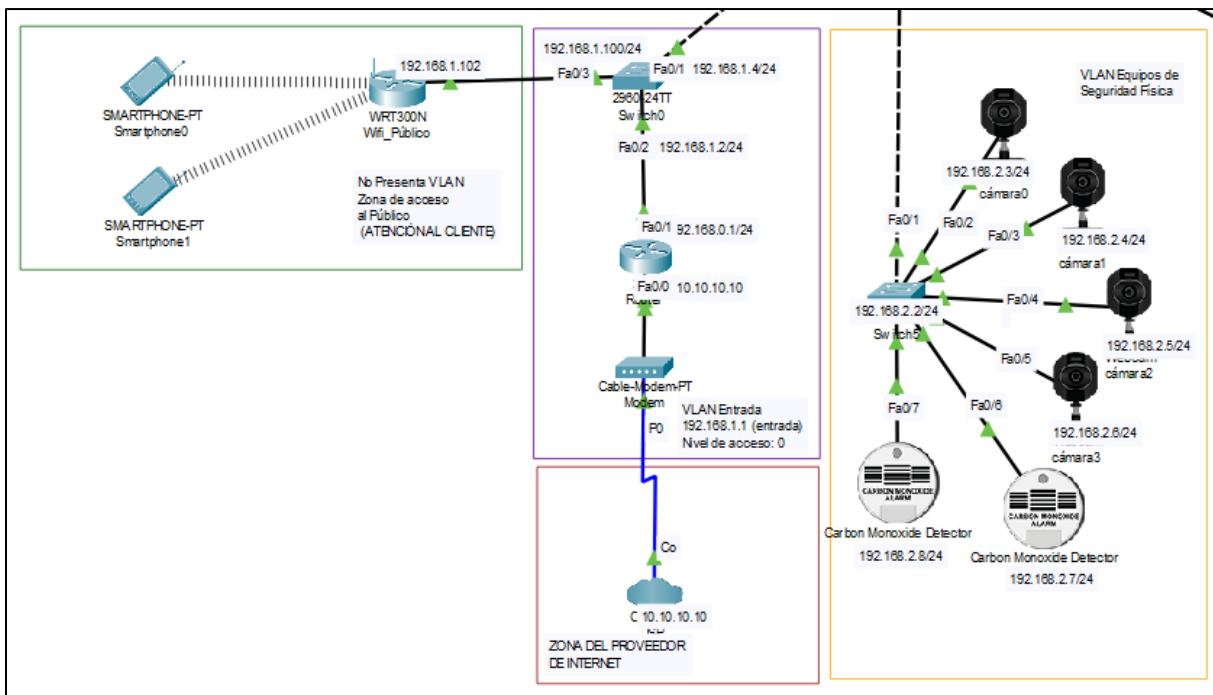


Figura 40. VLAN de Entrada a la red, punto de acceso WiFi al público.

Fuente: Elaboración Propia. (2022)

Por lo cual, ya establecida la conexión proveniente del ISP mediante un cable coaxial se direcciona una ruta de enlace por cableado de red UTP hacia el Router, donde se le asigna el direccionamiento 192.168.0.1/24 el cual funcionara como Gateway de la red (ver figura 40), desde este Router se transporte una conexión hacia el switch 0 con dirección IP 19.168.1.2/24 mediante un puerto de entrada Fast-Ethernet 0/2. Desde este switch se dictaminan dos rutas, una designada para establecer una zona de acceso wifi para el público que presenta un IP enlazada de 192.168.1.102 a través del puerto de entrada 0/3 y otra ruta que se conecta directamente desde el puerto 0/1 con el equipo protector de la red, es decir el cortafuego mediante su puerto físico Ethernet 0/0.

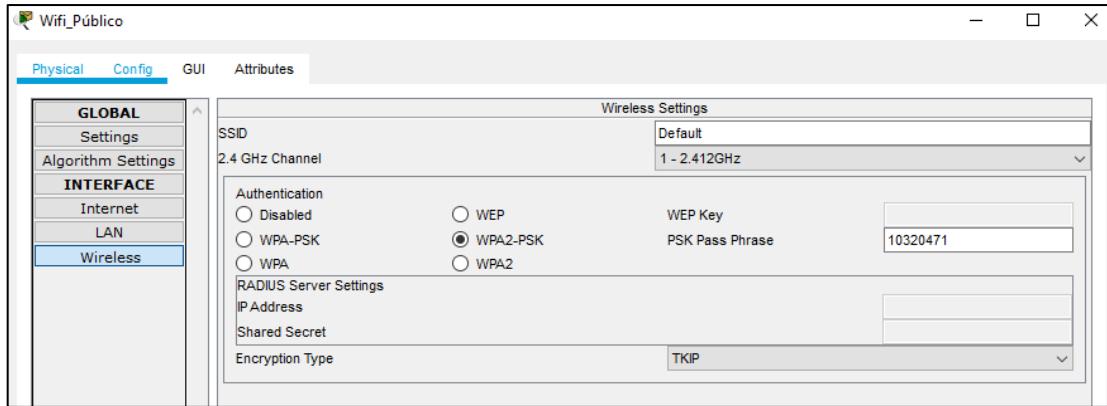


Figura 41. Configuración Wireless del Router para acceso público.

Fuente: Elaboración propia.

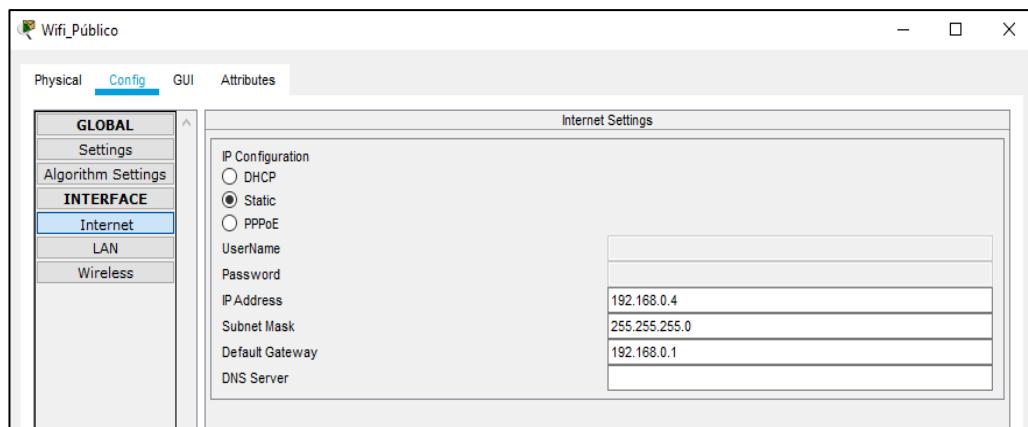


Figura 42. Configuración Network del Router para acceso público.

Fuente: Elaboración propia.

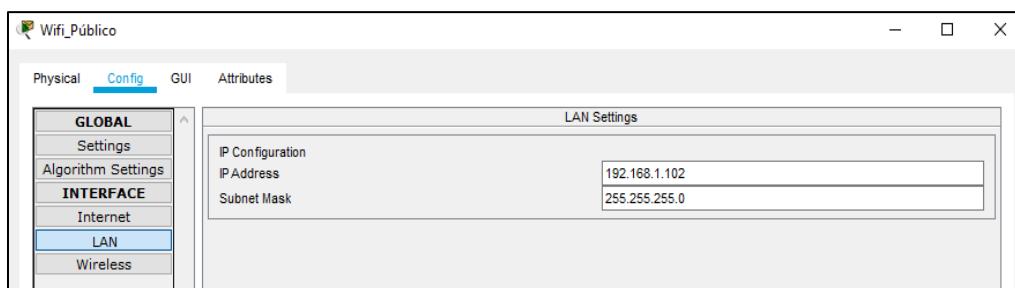


Figura 43. Configuración LAN del Router para acceso público.

Fuente: Elaboración propia.

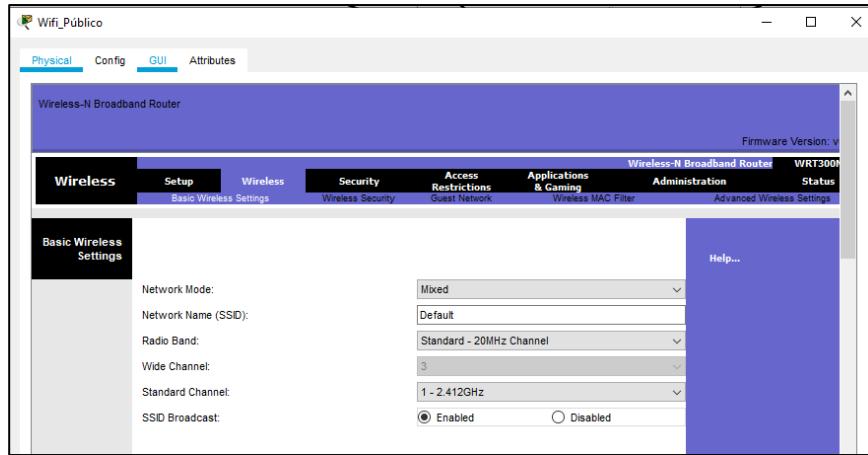


Figura 44. Configuración básica del Wireless.
Fuente: Elaboración propia.

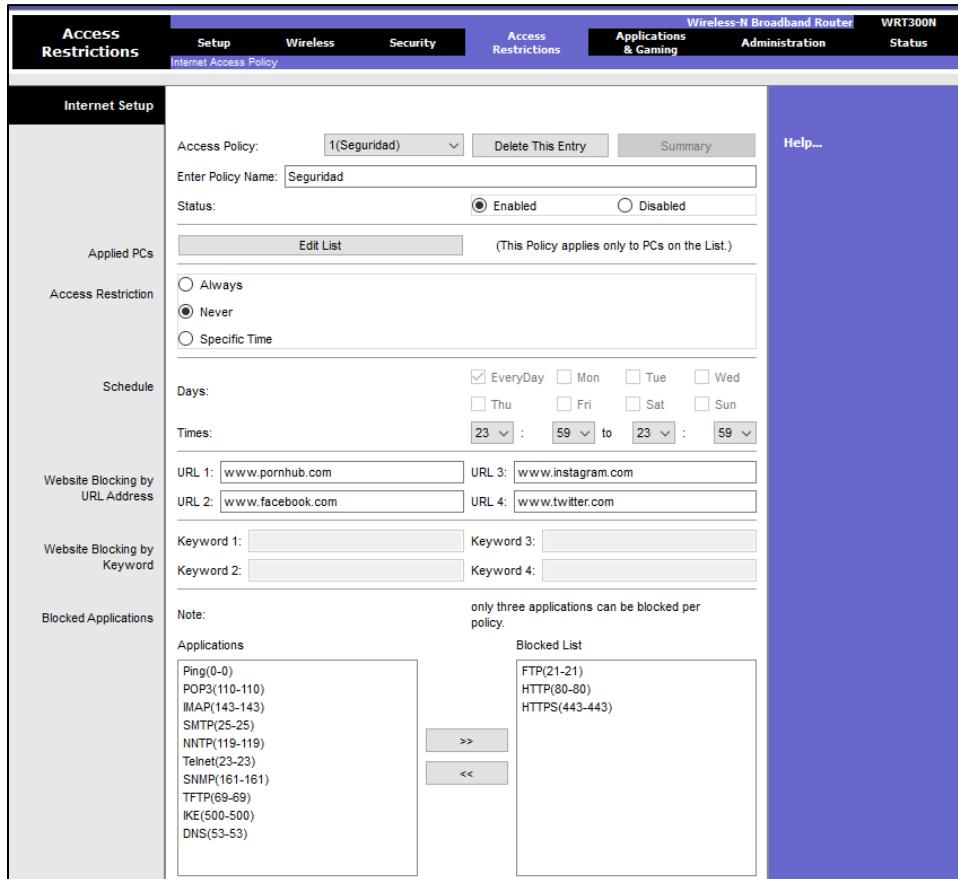


Figura 45. Restricciones de seguridad para Router público.
Fuente: Elaboración propia.

Access Restrictions		Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Wireless-N Broadband Router	WRT300N Status
Internet Access Policy								
<p>Internet Setup</p> <p>Access Policy: <input type="text" value="2(Seguridad2)"/> <input type="button" value="Delete This Entry"/> <input type="button" value="Summary"/></p> <p>Enter Policy Name: <input type="text" value="Seguridad2"/></p> <p>Status: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</p> <p><input type="button" value="Edit List"/> (This Policy applies only to PCs on the List.)</p> <p><input type="radio"/> Always <input checked="" type="radio"/> Never <input type="radio"/> Specific Time</p> <p>Days: <input checked="" type="checkbox"/> EveryDay <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun</p> <p>Times: <input type="text" value="23 : 59 : 23 : 59"/></p> <p>Website Blocking by URL Address</p> <p>URL 1: <input type="text" value="www.snapchat.com"/> URL 3: <input type="text" value="www.MySpace.com"/> URL 2: <input type="text" value="www.mercadolibre.com"/> URL 4: <input type="text" value="www.Ad.Doubleclick.net"/></p> <p>Website Blocking by Keyword</p> <p>Keyword 1: <input type="text"/> Keyword 3: <input type="text"/> Keyword 2: <input type="text"/> Keyword 4: <input type="text"/></p> <p>Note: only three applications can be blocked per policy.</p> <p>Applications</p> <div style="border: 1px solid black; padding: 5px;"> Ping(0-0) FTP(21-21) POP3(110-110) IMAP(143-143) SMTP(25-25) NNTP(119-119) Telnet(23-23) SNMP(161-161) IKE(500-500) DNS(53-53) </div> <p><input type="button" value=">>"/> <input type="button" value="<<"/></p> <p>Blocked List</p> <div style="border: 1px solid black; padding: 5px;"> HTTPS(443-443) HTTP(80-80) TFTP(69-69) </div>								

Figura 46. Restricciones de seguridad 2 para Router público.
Fuente: Elaboración propia.

Access Restrictions		Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Wireless-N Broadband Router	WRT300N Status
Internet Access Policy								
<p>Internet Setup</p> <p>Access Policy: <input type="text" value="3(Seguridad3)"/> <input type="button" value="Delete This Entry"/> <input type="button" value="Summary"/></p> <p>Enter Policy Name: <input type="text" value="Seguridad3"/></p> <p>Status: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</p> <p><input type="button" value="Edit List"/> (This Policy applies only to PCs on the List.)</p> <p><input type="radio"/> Always <input checked="" type="radio"/> Never <input type="radio"/> Specific Time</p> <p>Days: <input checked="" type="checkbox"/> EveryDay <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun</p> <p>Times: <input type="text" value="23 : 59 : 23 : 59"/></p> <p>Website Blocking by URL Address</p> <p>URL 1: <input type="text" value="www.eBay.com"/> URL 3: <input type="text" value="www.hotmail.com"/> URL 2: <input type="text" value="www.Meebo.com"/> URL 4: <input type="text" value="www.Orkut.com"/></p> <p>Website Blocking by Keyword</p> <p>Keyword 1: <input type="text"/> Keyword 3: <input type="text"/> Keyword 2: <input type="text"/> Keyword 4: <input type="text"/></p> <p>Note: only three applications can be blocked per policy.</p> <p>Applications</p> <div style="border: 1px solid black; padding: 5px;"> Ping(0-0) FTP(21-21) POP3(110-110) IMAP(143-143) SMTP(25-25) NNTP(119-119) Telnet(23-23) SNMP(161-161) TFTP(69-69) </div> <p><input type="button" value=">>"/> <input type="button" value="<<"/></p> <p>Blocked List</p> <div style="border: 1px solid black; padding: 5px;"> HTTPS(443-443) HTTP(80-80) </div>								

Figura 47. Restricciones de seguridad 3 para Router público.
Fuente: Elaboración propia.

En relación con la zona de acceso al público, esta no cuenta con una segmentación establecida debido a que no representa un nivel de interés dentro de la Contraloría. Sin embargo, se le asignada un cable de acceso (WPA2-PSK), **ver figura 41**, para impedir que extender intenten vulnerar la red, además para no limitar a la distribución de ancho de banda dentro de la nueva infraestructura se le asigna una conexión de punto a punto con capacidad de transporte de data de 10 Mbps. Así mismo, se determinó las configuraciones necesarias para los accesos Network, Wireless y LAN del dispositivo, estableciéndose IPS correspondiente a la dirección principal del Switch 0. (**ver figura 43 y 44**). Además, para garantizar la establece de este punto de acceso, se configuraron restricciones de acceso permanente para las páginas de acceso con mayor índice de malware. (**ver figura 45, 46 y 47**).

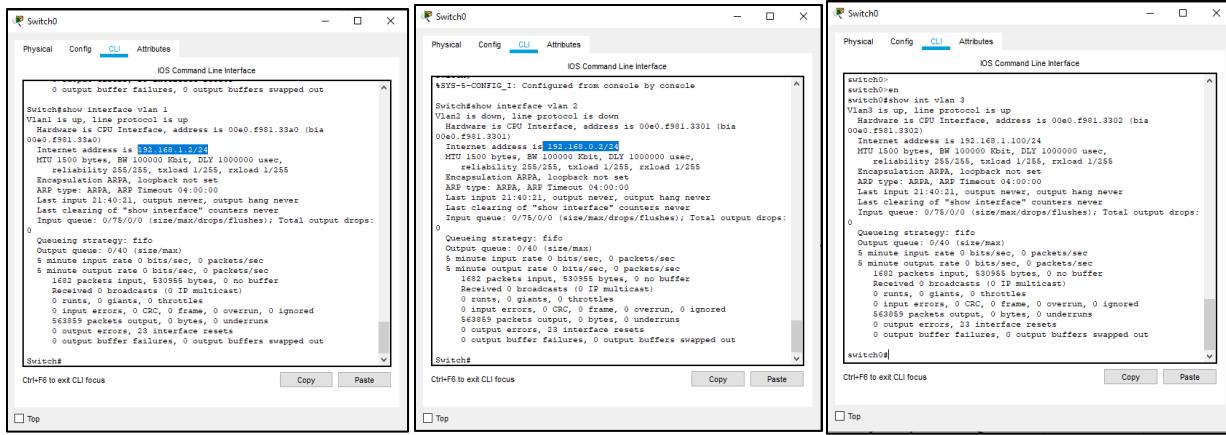


Figura 48. Activación del Switch nº0.

Fuente: Elaboración Propia. (2022)

Asimismo, entrando con la activación del servicio del Switch 0 dado a que presenta 3 niveles de conexión se procesa entonces tres (3) VLAN. Teniendo entonces la VLAN 1 con una interface de entrada desde el Router de direccionamiento de 192.168.1.2/24, una VLAN 2 con un direccionamiento 192.168.0.2/24 de salida hacia el cortafuego (ASA0). Y, por último, una VLAN 3 de salida hacia la zona al público con una IP de 192.168.1.100/20. Luego de determinar los direccionamientos de entrada hacia el cortafuego, este mismo funciona como gestor de direcciones IP para la conformación de círculos virtuales por zonas de trabajo. Donde cada una de estas VLANS cuenta con una ruta de enlace directa hacia el cortafuego, y además se le asignó un servicio para cada puerto de entrada Ethernet. (**Ver figura 48**).

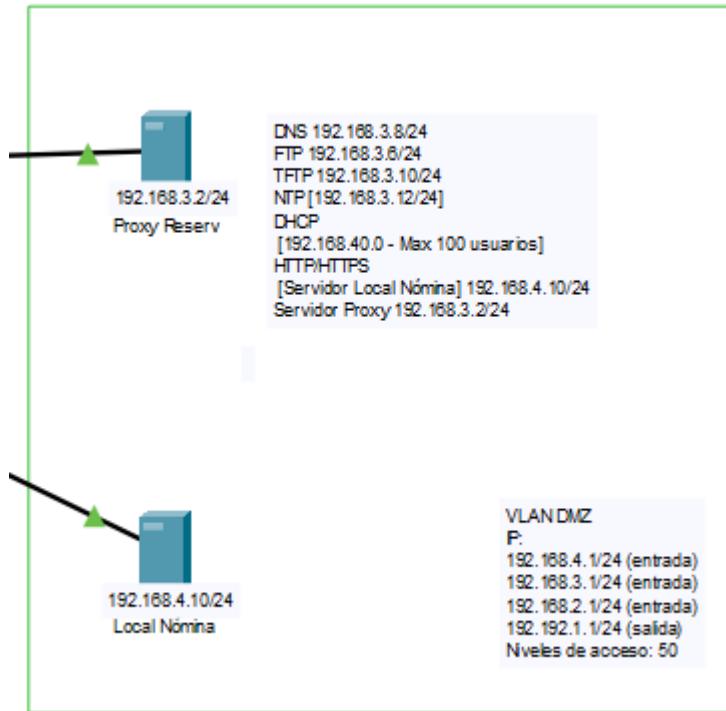


Figura 49. VLAN 5 de la nueva red.

Fuente: Elaboración Propia. (2022)

En este sentido, encontramos la zona DMZ de la nueva red que cuenta con los equipos de red que sirven de puente para establecer conexión con los servicios de internet de ISP mediante un direccionamiento 192.168.0.1 del Router que permita determinar rutas de acceso directo. Se le estableció la zona VLAN 5 (DMZ) mediante los puertos físicos Ethernet 0/6 y 0/7 del cortafuego, estableciendo dirección de enlace basados en los IP 192.168.3.1 (Et0/6) y 192.168.4.1 (Et0/7). Destacando, que cada circulo virtual formado estará conectado al su respectivo servidor, donde a ambas segmentaciones se les determinó un nivel de acceso de tipo de 50. (**ver figura 49**).

Para la activación del servidor proxy, se estableció dentro del Ubuntu server los servicios para los protocolos mencionadas en las configuraciones óptima de la red alámbrica, estableciendo de esta manera las direcciones IP de cada protocolo de manera que los hosts (PCs) o equipos de red puedan acceder a sus servicios, destacando que el proceso para transmisión de dato es regulado por el proxy mediante el protocolo TFP.

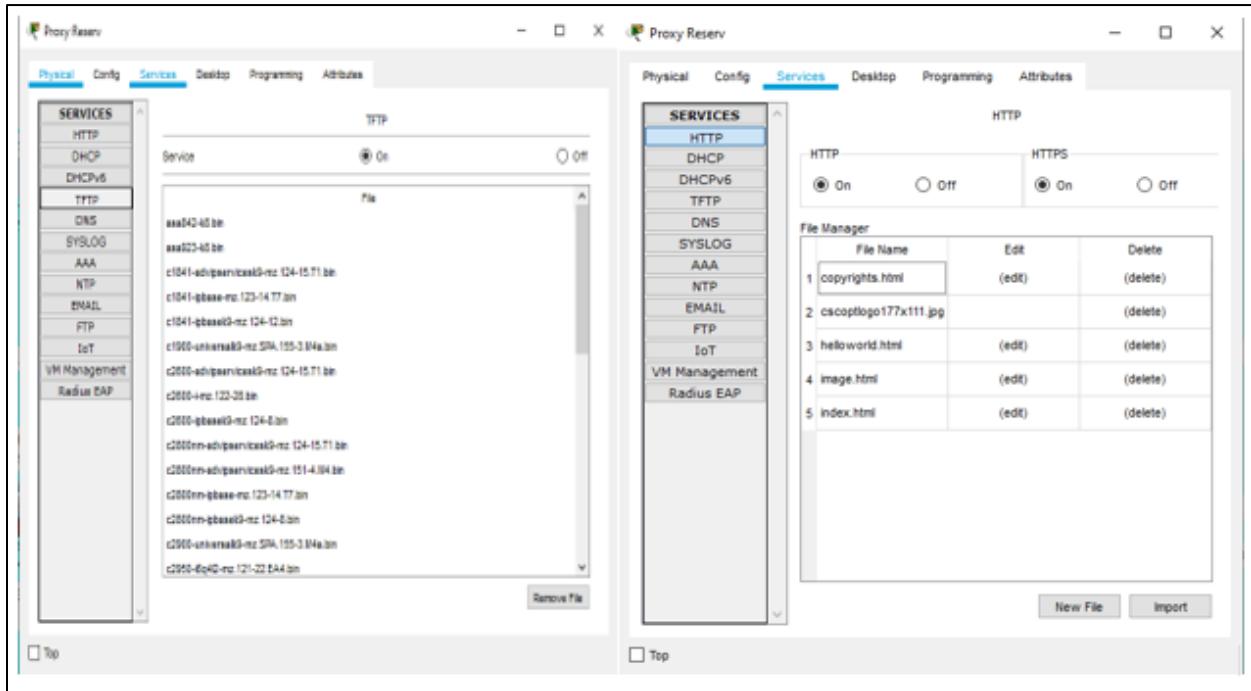


Figura 50. Activación servicios HTTP/HTTPS y TFTP.

Fuente: Elaboración propia.

En este sentido, se activan los protocolos HTTP/HTTPS para permiten a los hosts acceder a los servicios web, tanto del servidor local de nómica, como también hacia el servicio de dominio para la negación web. De la misma manera, se prenden los servicios TFTP para la trasmisión de datagramas mediante el protocolo UDP mediante archivos .bin, para establecer conectividad en la nueva red, sin necesidad de implementar los servicios del ISP para la transmisión de los datos. De esta manera, se mediante la activación de estos dos protocolos se necesita autenticar los servicios para la transferencia de los mismos. (**ver figura 50**).

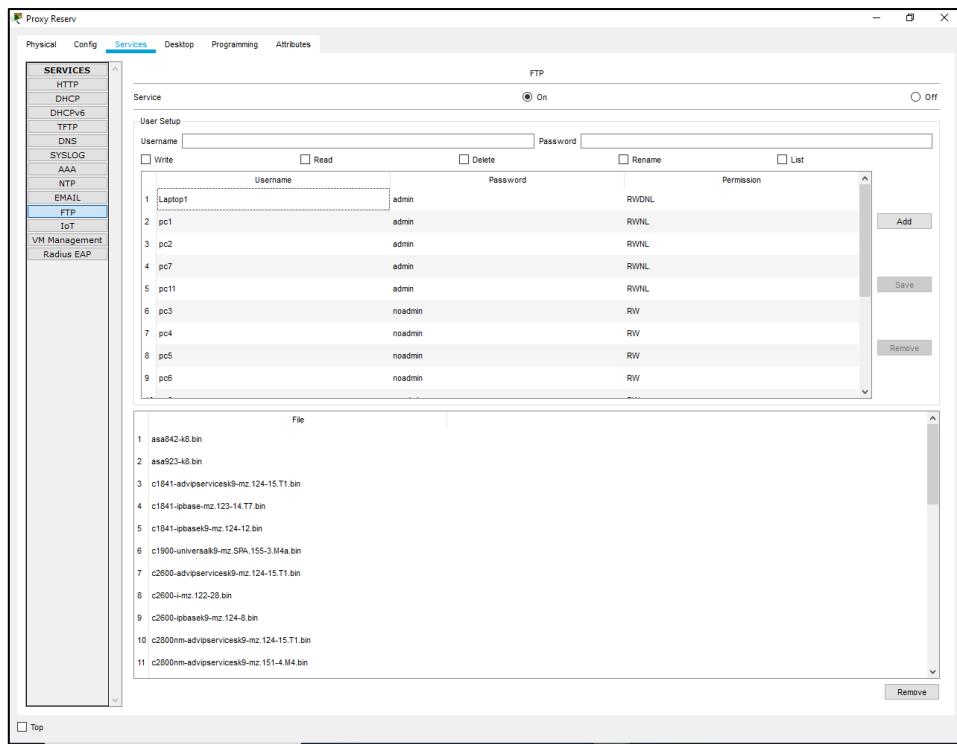


Figura 51. Activación protocolo FTP

Fuente: Elaboración Propria. (2022)

Por esta razón, en la figura se observa la activación del servicio FTP donde se asignan puestos de control completo para los equipos con direccionamiento IP estático, es decir, que estos son capaces de realizar procesos de escritura, lectura, eliminación, renombre y listado de la trasferencia de los archivos (datos). Caso contrario, para los equipos administrativos con direccionamiento dinámico los cuales simplemente tiene acceso a la lectura y escritura de este servicio, de manera que permita tener control dentro de la nueva red. (**ver figura 51**).

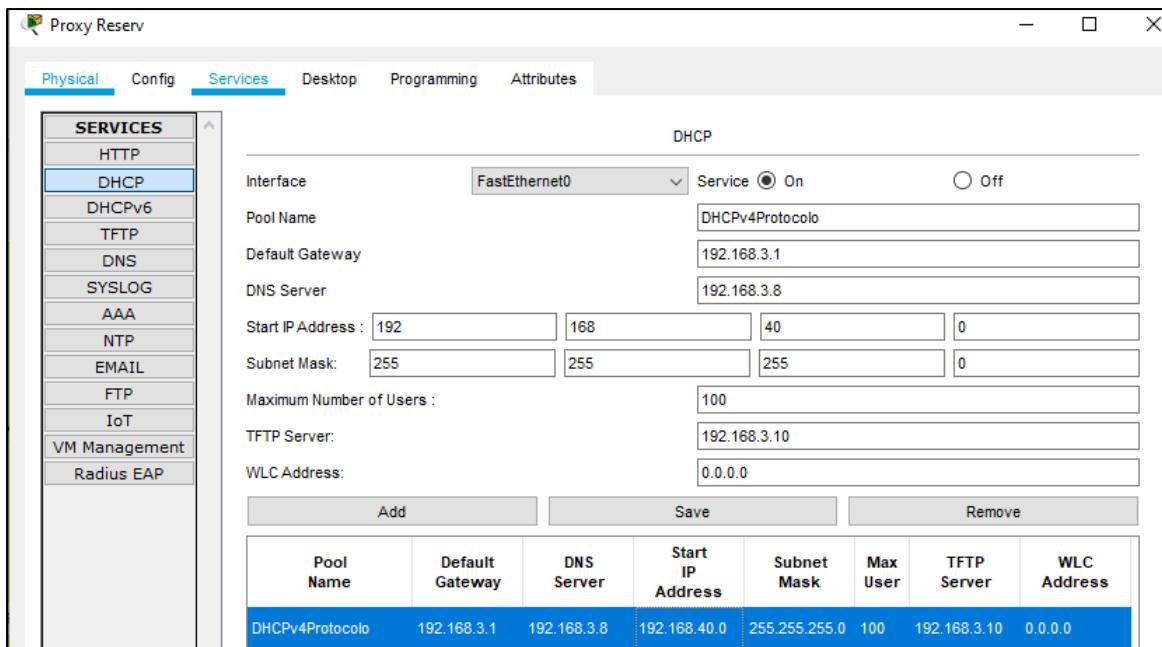


Figura 52. Activación protocolo DHCP.

Fuente: Elaboración Propia.

Ahora, para determinar los direccionamientos de las IP dinámicas en la figura se observa la activación protocolo DHCP, en el cual se estableció una dirección de poso inicial de 192.168.3.1/24 que se necesita para ubicar el protocolo dentro de servidor proxy, por otra parte, se le consigna una IP inicial para su servicio de 192.168.40.0/24 con límite de usuarios para el servicio de 100. Cabe destacar, que debido a que algunos equipos administrativos se lo implemento este servicio, es necesario adaptarles una dirección de enlace hacia el servicio TFTP dado a la trasmisión dentro de la red se va a representan mediante datagramas. Debido a que se implementa los protocolos FTP Y TFTP para transmisiones TCP, se ve necesario activar en conjunto el protocolo NTP. (**ver figura 52**).

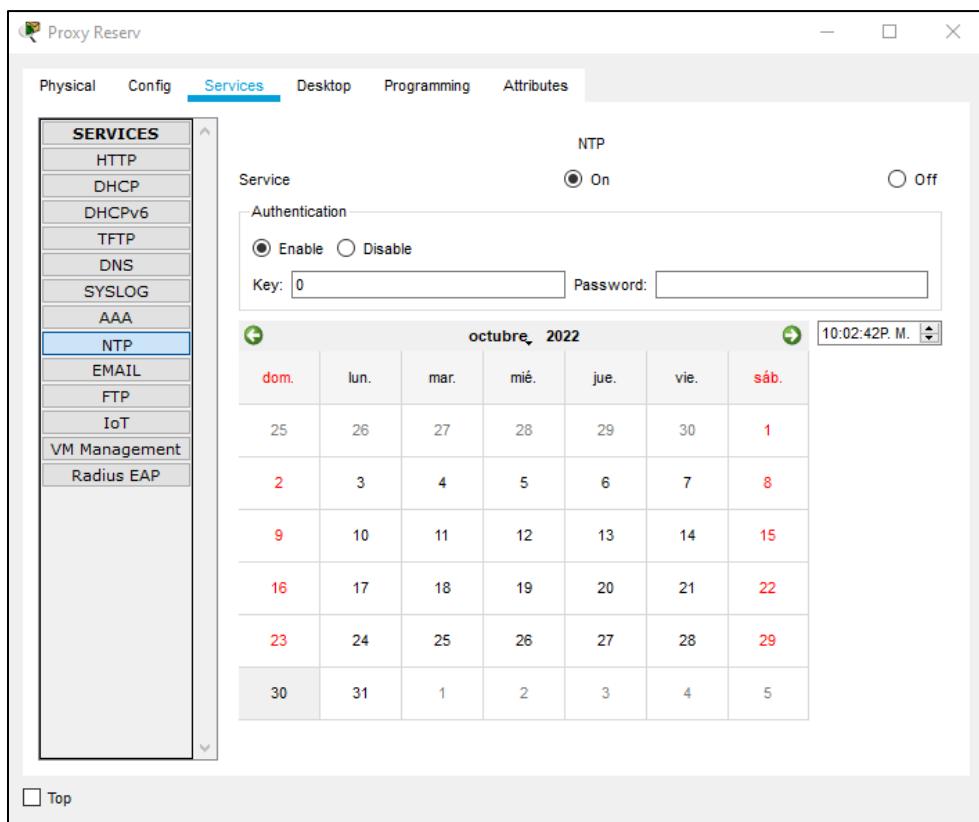


Figura 53. Activación protocolo NTP.

Fuente: Elaboración Propia. (2022)

Este protocolo permite controlar el estado de servicio de un equipo dentro de la red, es decir, funciona de mapeado para determinar la ubicación de un equipo donde estable direcciona del equipo a buscar, junto a la hora específica de su transporte dentro de red en tal caso de a ver aplicado un proceso de trasferencia de dato, dentro de la activación de este protocolo (**ver figura 53**) se determina un clave de inicio de sesión junto a una contraseña para la activación del servicio dentro de un equipo administrativo. En este mismo orden de idea, se vio la necesidad de activar un servicio de dominio dentro de la red, que permitiera agilizar los procesos de consultas.

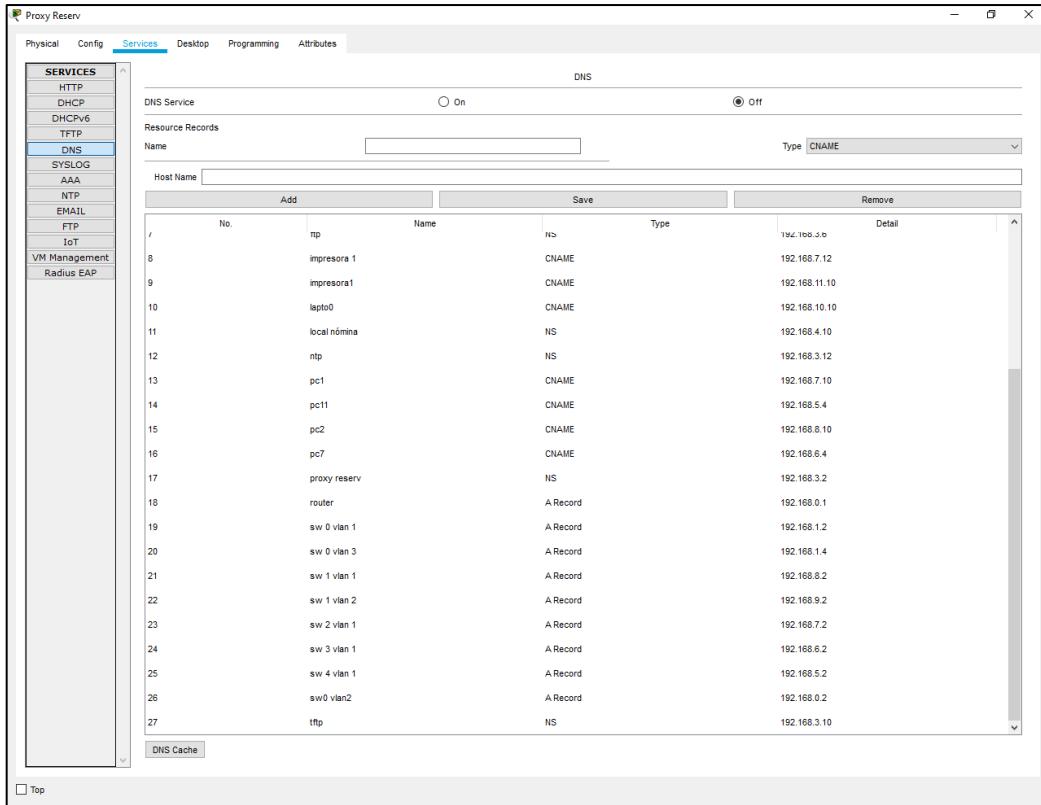


Figura 54. Activación protocolo DNS.

Fuente: Elaboración Propia. (2022)

De esta manera, en la figura se observa el encendido del servicio DNS donde se establecen aquellos equipos con direccionamiento dinámico de la nueva red, donde dependiendo del tipo servicio, se representó como un servidor, host o direccionamiento. De manera, que se les pueden llegar a acceder de manera más rápida y eficaz en la red, siempre y cuando se tengas los permisos necesarios para dicha acción. (**ver figura 54**).

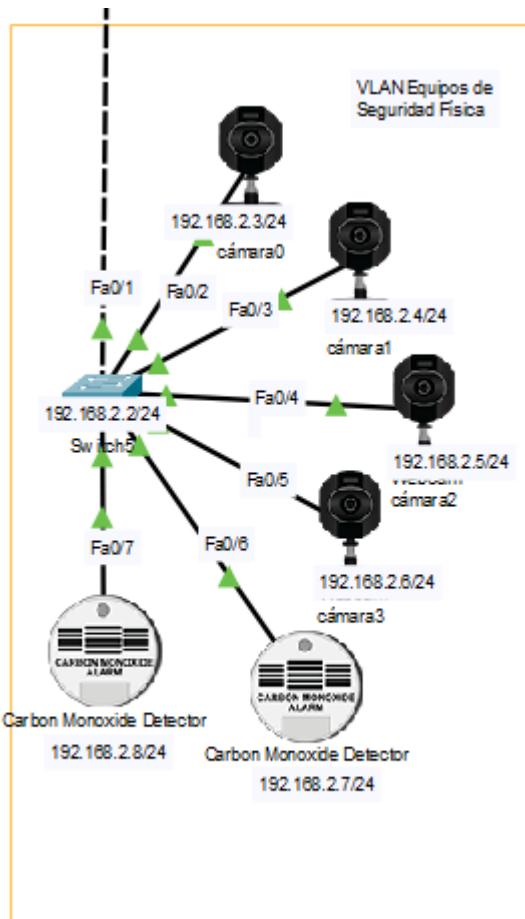


Figura 55. VLAN Equipos de Seguridad Física.

Fuente: Elaboración propia.

Por otra parte, en la figura 50 se observa la VLAN Equipos de Seguridad Física, establecida por el puerto Et 0/5 del cortafuego con direccionamiento 192.168.2.1/24 desde el cual se origina una conexión de punto a punto hacia el switch 5, donde se conectarán las cámaras de seguridad y detectores de monóxido de carbono, de manera que permita aislar los procesos de transferencia de archivos dentro de la red. Asimismo, se determinó un nivel de acceso para esta VLAN de 50. (ver figura 55)

```

Switch5
Physical Config CLI Attributes
IOS Command Line Interface
*Interface Vlan2 does not exist.

Vlan1 is up, line protocol is up
Hardware is CPU Interface, address is 0090.214b.dd2d (bia
0090.214b.dd2d)
Internet address is 192.168.2.2/24
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARP, ARP timeout 04:00:00
Last input 21:40:21, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
563859 packets output, 0 bytes, 0 underruns
0 output errors, 23 interface resets
0 output buffer failures, 0 output buffers swapped out
Switch#

```

Ctrl+F6 to exit CLI focus Copy Paste

Top

Figura 56. Activación del Switch n°5.
Fuente: Elaboración Propia. (2022)

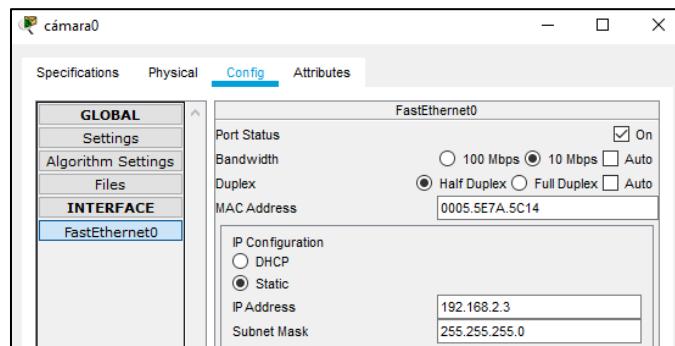


Figura 57. Configuración de las cámaras de seguridad.
Fuente: Elaboración propia.

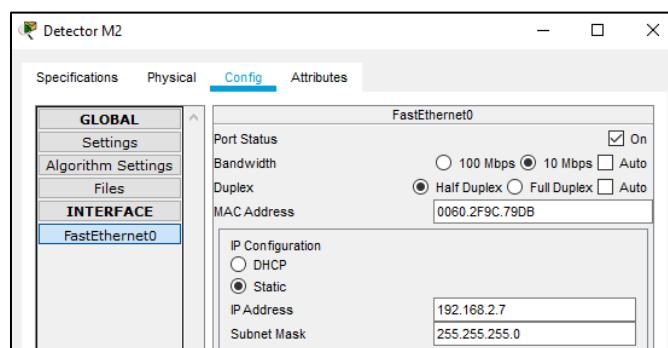


Figura 58. Configuración de los detectores de monóxido de carbono.
Fuente: Elaboración propia.

De esta forma, **en la figura 56** se observa la activación del servicio de VLAN para el switch 5 mediante una dirección IP de 192.168.2.2/24 desde el cual trabajarán todos los equipos conectados por sus puertos de entrada. Además, se estableció una conexión de punto a punto automática, es decir, que manejan niveles de transmisión half-duplex, por lo cual, tanto las cámaras de seguridad como los detectores de monóxido van a manejar velocidades de 10 Mbps. (**ver figura 57 y 58**).

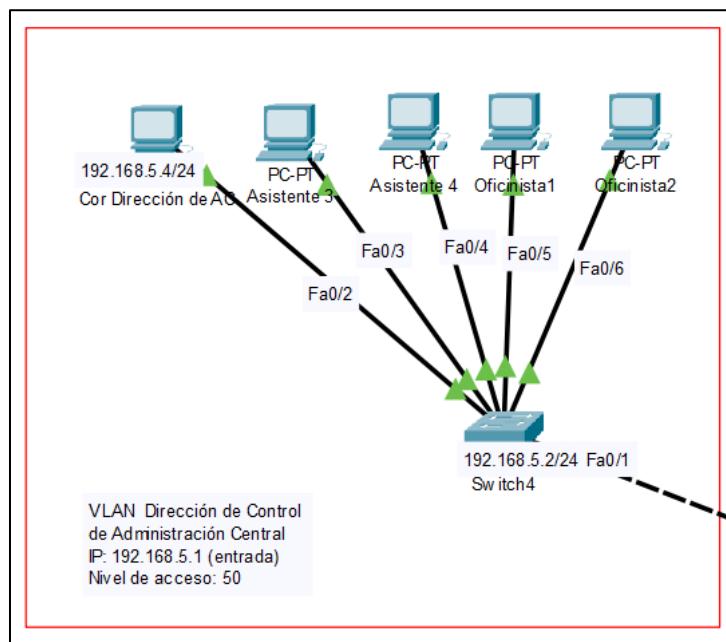


Figura 59. VLAN Dirección de Control de Administración Central.

Fuente: Elaboración propia. (2022)

The screenshot shows the Cisco IOS Command Line Interface (CLI) window titled "Switch4". The tab bar at the top has "Physical", "Config", "CLI" (which is highlighted in blue), and "Attributes". Below the tabs is the title "IOS Command Line Interface". The main pane displays the output of the command "Switch# show interface vlan 1". The output details the configuration and statistics for VLAN 1, including its IP address (192.168.5.2/24), MTU, reliability, encapsulation type (ARPA), and various counters for input and output traffic.

```

Switch#
Switch#show interface vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 000c.8533.5e6d (bia 000c.8533.5e6d)
  Internet address is 192.168.5.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1682 packets input, 530955 bytes, 0 no buffer
    Received 0 broadcasts, 0 IP multicast
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    563859 packets output, 0 bytes, 0 underruns
    0 output errors, 23 interface resets
    0 output buffer failures, 0 output buffers swapped out

Switch#

```

At the bottom of the CLI window, there are buttons for "Copy" and "Paste", and a checkbox labeled "Top".

Figura 60. Activación del Switch n°4.

Fuente: elaboración propia. (2022)

Luego, se establece una conexión desde el puerto Ethernet 0/4 del cortafuego desde el cual se transporta un VLAN de direccionamiento 192.168.5.1 desde van a trabajan el equipo de red y administrativos de la zona del departamento de Dirección de Control de la Administración Central de la Contraloría. Donde se determina un direccionamiento estático para el conmutador (switch 4), junto a la pc11 que sirve para controlar la VLAN, los demás equipos presentan una dirección dinámica (**ver figura 59**). Ahora, para la activación del servicio de la VLAN dentro del switch se estableció una dirección de control inicial 192.168.5.2/24 con conexión de punto a punto de modelo full-dúplex para todos puertos de entrada (**ver figura 60**). De la misma manera, se determinó un nivel de control de seguridad de nivel 50 para esta zona. Cabe destacar, que se determina dentro de la configuración de los servidores (Proxy y Local de Nómina) asignar un sistema de resguardo en la nube mediante Google Drive que logre mantener la seguridad de los datos establecidos dentro de estos elementos.

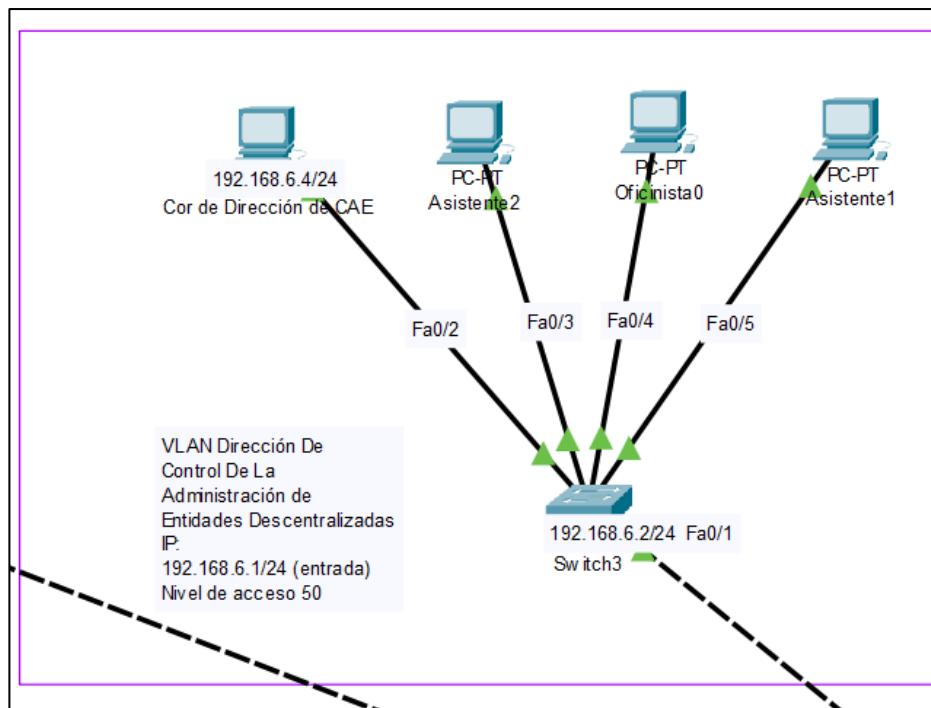


Figura 61. VLAN Dirección de Control de la Administración de Entidades Descentralizadas.
Fuente: Elaboración Propia. (2022)

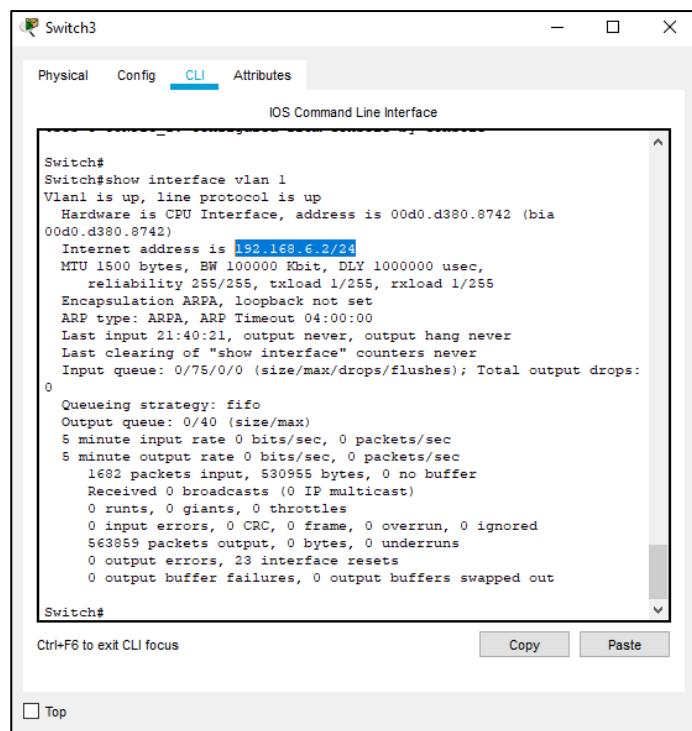


Figura 62. Activación del Switch n°3.
Fuente: Elaboración Propria. (2022)

Por otra parte, encontramos la segmentación de la VLAN Dirección de Control de la Administración de Entidades Descentralizadas, configurada en el cortafuego por el puerto de enlace Ethernet 0/3 hacia el departamento de Dirección de Control de la Administración de Entidades Descentralizadas, donde se aplicó un nivel de seguridad de nivel 50, desde el cual se transporta un direccionamiento de 192.168.6.1/24 donde se suministran los IP correspondientes a los equipos de esta área (**ver figura 61**). Donde abarca una dirección estática para el switch 3 de 192.168.6.2/24 mediante conexión full-dúplex para todos los puertos de enlace. De la misma forma, se establece a un equipo (pc7) como host con direccionamiento 192.168.6.4/24 central para el control de la zona. (**Ver figura 62**).

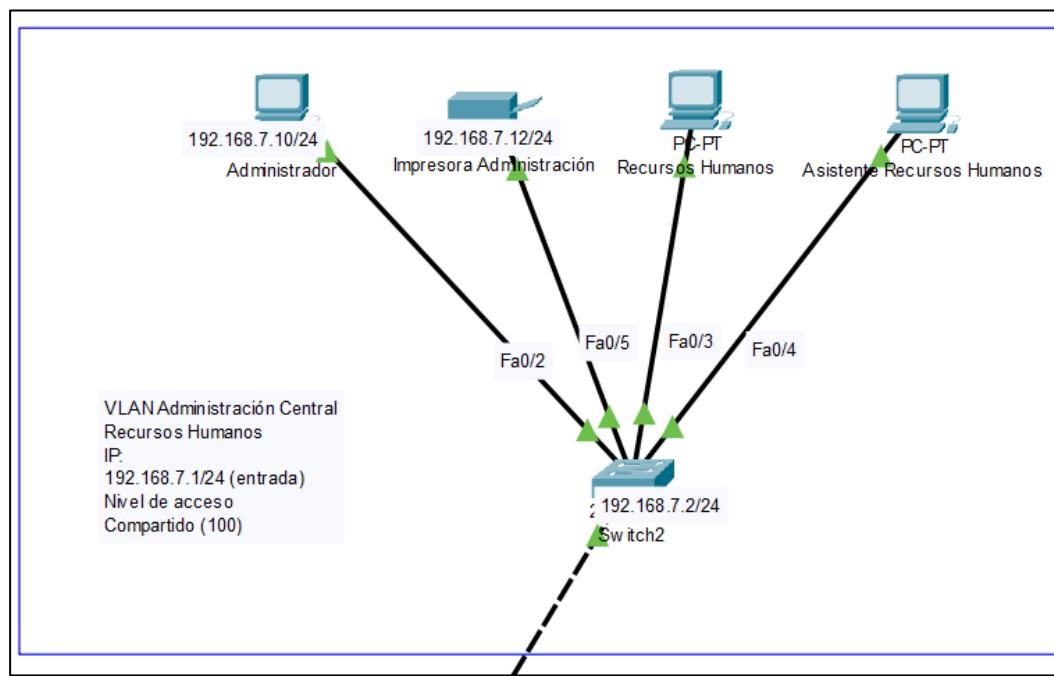


Figura 63. VLAN Administración Central y Recursos Humanos.

Fuente: Elaboración Propia. (2022)

```

Switch#
Switch#show interface vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 00d0.ba8a.4478 (bia
00d0.ba8a.4478)
    Internet address is 192.168.7.2/24
    MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    ARP type: ARPA, ARP Timeout 04:00:00
    Last input 21:40:21, output never, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
0
    Queueing strategy: fifo
    Output queue: 0/40 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
      1682 packets input, 530955 bytes, 0 no buffer
      Received 0 broadcasts (0 IP multicast)
      0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      563859 packets output, 0 bytes, 0 underruns
      0 output errors, 23 interface resets
      0 output buffer failures, 0 output buffers swapped out

Switch#

```

Ctrl+F6 to exit CLI focus

Top

Figura 64. Activación del Switch n°2.
Fuente: Elaboración Propia. (2022)

De la misma manera, encontramos la VLAN 2 proveniente de la puerta de enlace Ethernet 0/2 del cortafuego con un direccionamiento IP de 192.168.7.1/24 para los departamentos de Administración Central y Recursos Humanos de la Contraloría, suministrada por el switch 2 establecido por una dirección estática de 192.168.7.2(**ver figura 63**)activado por conexión de punto a punto mediante un proceso half-dúplex, solo para la puerta de enlace 0/2, es decir, para la pc1 con direccionamiento estático 192.168.7.10(**ver figura 64**). Los demás equipos de la zona, se les estableció un proceso de full-dúplex; aplicándose un control de seguridad de nivel 100.

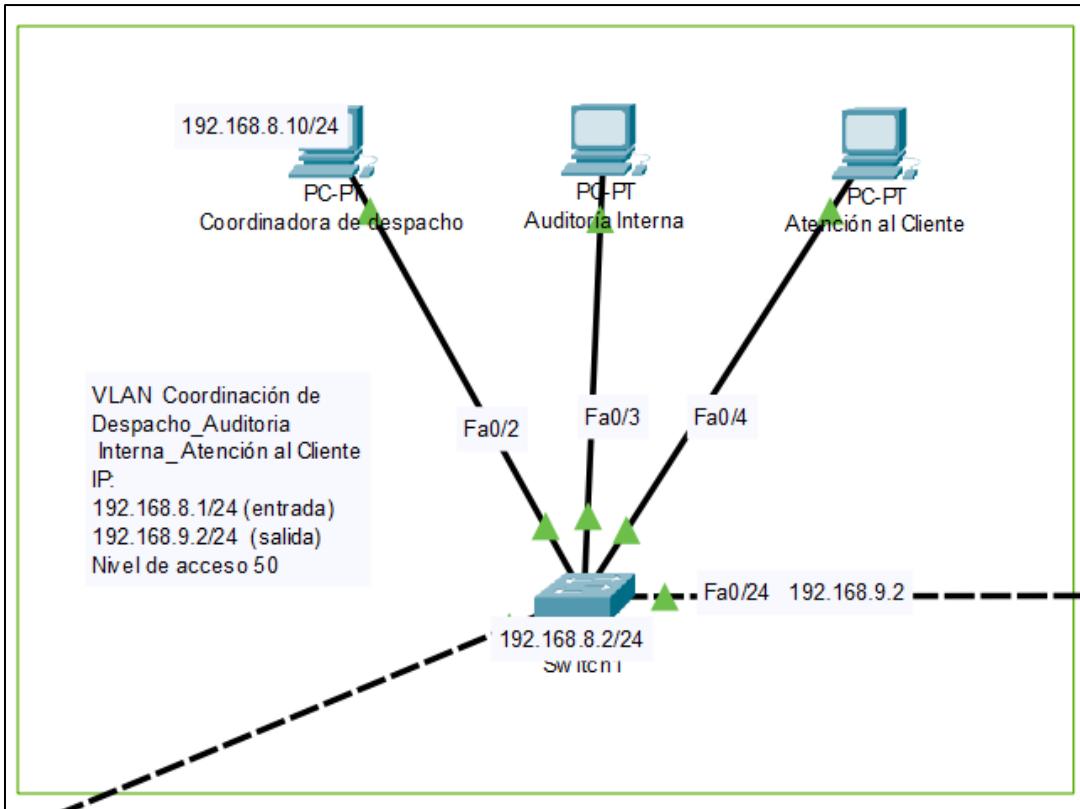


Figura 65. VLAN Coordinación de Despacho Auditoría Interna Atención al Cliente.

Fuente: Elaboración Propia. (2022)

```

Switch1
Physical Config CLI Attributes
IOS Command Line Interface
*SYS-5-CONFIG_I: Configured from console by console
Switch#show interface vlan 1
Vlan1 is up, line protocol is up
Hardware is CPU Interface, address is 00d0.d301.71b9 (bia
00d0.d301.71b9)
Internet address is 192.168.8.2/24
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 21:40:21, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  563859 packets output, 0 bytes, 0 underruns
  0 output errors, 23 interface resets
  0 output buffer failures, 0 output buffers swapped out
Switch#
Ctrl+F6 to exit CLI focus
Copy Paste
Top

Switch1
Physical Config CLI Attributes
IOS Command Line Interface
*SYS-5-CONFIG_I: Configured from console by console
Switch#show interface vlan 2
Vlan2 is down, line protocol is down
Hardware is CPU Interface, address is 00d0.d301.7101 (bia
00d0.d301.7101)
Internet address is 192.168.9.2/24
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 21:40:21, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  563859 packets output, 0 bytes, 0 underruns
  0 output errors, 23 interface resets
  0 output buffer failures, 0 output buffers swapped out
Switch#
Ctrl+F6 to exit CLI focus
Copy Paste
Top

```

Figura 66. Activación del Switch n° 1.

Fuente: Elaboración Propia. (2022)

En otra medida, tiene la creación de la VLAN 1 proveniente de la puerta de enlace 0/1 desde el cortafuego con un direccionamiento IP de 192.168.8.1/24, que abarca a los departamentos de Coordinador/a de Despacho, Auditoria Interna y Atención al Cliente (ver figura 65). Esta entrada del servicio VLAN es suministrada mediante un switch 1, donde se regulan 2 direccionamientos VLAN debido a que existe una conexión interna para los departamentos antes mencionados, pero desde la puerta de enlace 0/24 del comutador sale una conexión de entrada hacia el otro cortafuego (ASA1) mediante un direccionamiento de 192.168.9.2/24 (ver figura 66). Cabe destacar que la VLAN 1 del comutador (192.168.8.1) se le establecieron procesos de conexión full-duplex para todos sus puertos ejecutando el 24 con un nivel de seguridad de nivel 50, caso contrario para la VLAN 2 en la cual se desglosó un proceso half-duplex con un nivel 100.

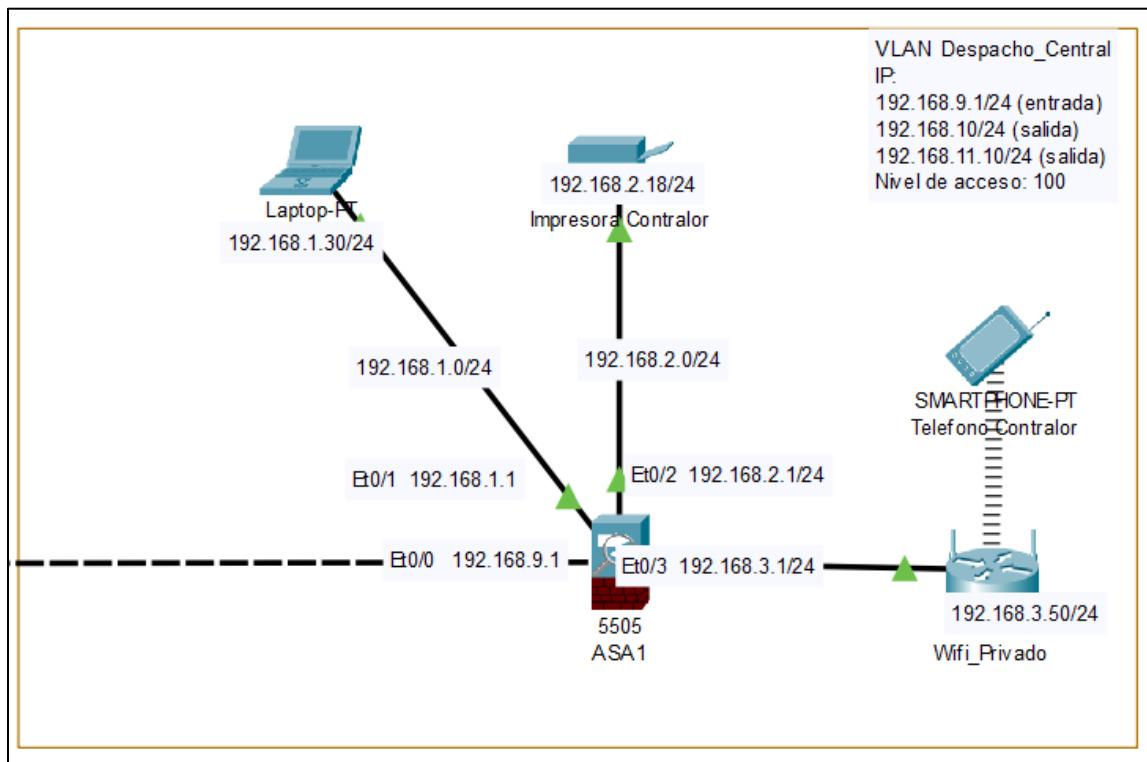


Figura 67. VLAN Despacho Central.

Fuente: Elaboración Propia.

De esta forma, encontramos la VLAN Despacho Central donde se estableció un cortafuego para activar una subred del Network de este diseño, mediante direcciones IP de 192.168.1.1/24 y 192.168.2.1/24 de los puertos Et0/1 y Et0/2, debido a que se conectan los equipos de despacho de la Contraloría (portátil e impresora), logrando de esta manera segmentar cada dispositivo, dado a que esta oficina maneja todos los accesos dentro de la red, es decir, que su nivel de acceso es de

100. Asimismo, se les asignó niveles de conexión de punto a punto mediante un proceso half-dúplex. Por otra parte, se determinó dentro del puerto físico Et0/3 se configura un punto de acceso wifi privado mediante un Router WiFi enlazado hacia el ASA1. (**ver figura 67**).

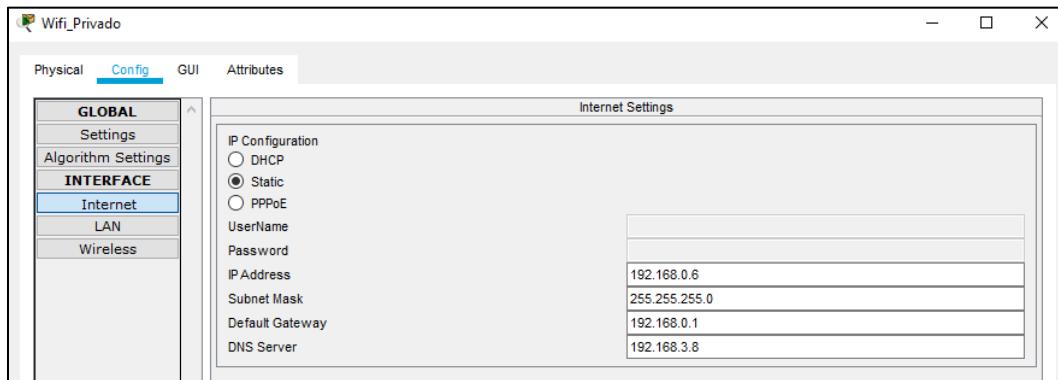


Figura 68. Configuración Network del router para acceso wifi privado.

Fuente: Elaboración propia.

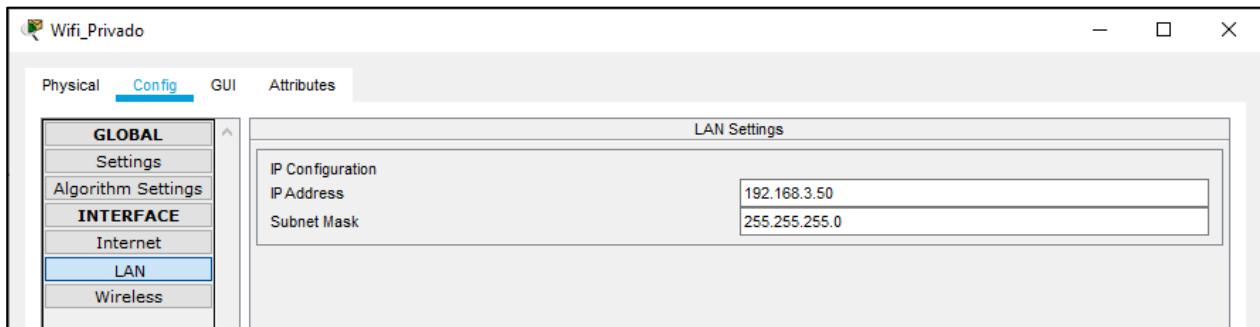


Figura 69. Configuración LAN del router para acceso wifi privado.

Fuente: Elaboración propia.

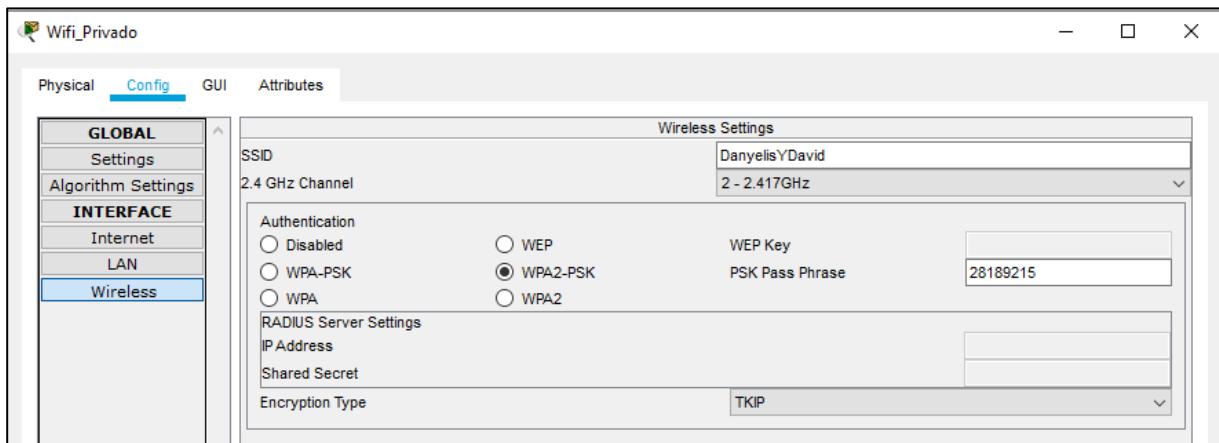


Figura 70. Configuración Wireless del router para acceso wifi privado.

Fuente: Elaboración propia.

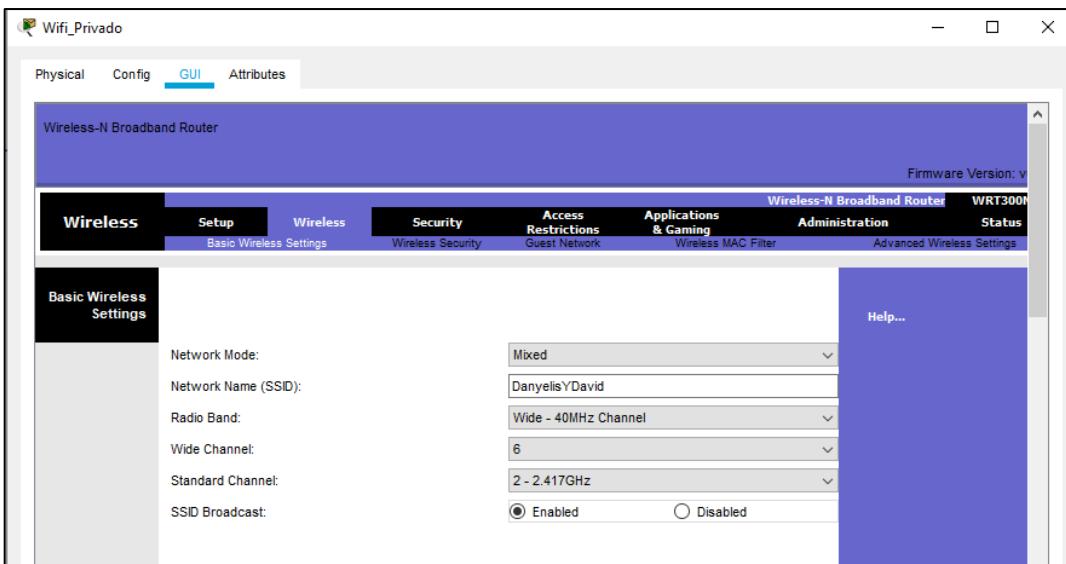


Figura 71. Configuración Network del router para acceso wifi privado (SSID).
Fuente: Elaboración propia.

Internet Setup	
Access Policy:	1(Seguridad)
Enter Policy Name:	Seguridad
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Edit List (This Policy applies only to PCs on the List.)	
Applied PCs	<input type="radio"/> Always <input checked="" type="radio"/> Never <input type="radio"/> Specific Time
Access Restriction	<input checked="" type="checkbox"/> EveryDay <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
Schedule	Days: Times: 23 : 59 to 23 : 59
Website Blocking by URL Address	URL 1: www.pornhub.com URL 3: www.Ad.Doubleclick.net URL 2: www.MySpace.com URL 4: www.Ad.Yielmanager.com
Website Blocking by Keyword	Keyword 1: Keyword 3: Keyword 2: Keyword 4:
Blocked Applications	Note: only three applications can be blocked per policy. Applications: FTP(21-21), POP3(110-110), IMAP(143-143), SMTP(25-25), NNTP(119-119), Telnet(23-23), SNMP(161-161), TFTP(69-69), IKE(500-500), DNS(53-53) Blocked List: HTTP(80-80), HTTPS(443-443), Ping(0-0) Buttons: >>, <<

Figura 72. Restricciones de seguridad para el router wifi privado.
Fuente: Elaboración propia.

Internet Setup

Access Policy:	1(Seguridad)	Delete This Entry	Summary
Enter Policy Name:	Seguridad		
Status:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
Edit List (This Policy applies only to PCs on the List.)			
Applied PCs	<input type="radio"/> Always <input checked="" type="radio"/> Never <input type="radio"/> Specific Time		
Access Restriction			
Schedule	<input checked="" type="checkbox"/> EveryDay <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun Days: 23 : 59 to 23 : 59		
Website Blocking by URL Address	URL 1: www.pornhub.com URL 3: www.Ad.Doubleclick.net URL 2: www.MySpace.com URL 4: www.Ad.Yieldmanager.com		
Website Blocking by Keyword	Keyword 1: Keyword 3: Keyword 2: Keyword 4:		
Blocked Applications	Note: only three applications can be blocked per policy. Applications: FTP(21-21) POP3(110-110) IMAP(143-143) SMTP(25-25) NNTP(19-119) Telnet(23-23) SNMP(161-161) TFTP(69-69) IKE(500-500) DNS(53-53)		
	Blocked List HTTP(80-80) HTTPS(443-443) Ping(0-0) >> <<		

Figura 73. Restricciones de seguridad 1 para el router wifi privado.

Fuente: Elaboración propia.

Internet Setup

Access Policy:	3(Políticas)	Delete This Entry	Summary
Enter Policy Name:	Políticas		
Status:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
Edit List (This Policy applies only to PCs on the List.)			
Applied PCs	<input type="radio"/> Always <input type="radio"/> Never <input checked="" type="radio"/> Specific Time		
Access Restriction			
Schedule	<input checked="" type="checkbox"/> EveryDay <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun Days: 08 : 30 to 13 : 00		
Website Blocking by URL Address	URL 1: www.facebook.com URL 3: www.twitter.com URL 2: www.gmail.com URL 4: www.youtube.com		
Website Blocking by Keyword	Keyword 1: Keyword 3: Keyword 2: Keyword 4:		
Blocked Applications	Note: only three applications can be blocked per policy. Applications: Ping(0-0) HTTPS(443-443) FTP(21-21) POP3(110-110) IMAP(143-143) SMTP(25-25) NNTP(19-119) Telnet(23-23) SNMP(161-161) TFTP(69-69) IKE(500-500) DNS(53-53)		
	Blocked List HTTP(80-80) >> <<		

Figura 74. Restricciones de políticas para el router wifi privado.

Fuente: Elaboración propia.

Internet Setup

Applied PCs Access Restriction Schedule Website Blocking by URL Address Website Blocking by Keyword Blocked Applications	<div style="margin-bottom: 10px;"> Access Policy: <input type="button" value="4(Policas2)"/> <input type="button" value="Delete This Entry"/> <input type="button" value="Summary"/> Enter Policy Name: <input type="text" value="Politicas2"/> </div> <div> Status: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <input type="button" value="Edit List"/> (This Policy applies only to PCs on the List.) </div> <div style="margin-top: 10px;"> <input type="radio"/> Always <input type="radio"/> Never <input checked="" type="radio"/> Specific Time </div> <div style="margin-top: 10px;"> Days: <input checked="" type="checkbox"/> EveryDay <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun </div> <div style="margin-top: 10px;"> Times: <input type="text" value="08"/> : <input type="text" value="30"/> to <input type="text" value="16"/> : <input type="text" value="00"/> </div> <div style="margin-top: 10px;"> URL 1: <input type="text" value="www.mercadolibre.com"/> URL 3: <input type="text" value="www.patria.org"/> URL 2: <input type="text" value="www.bancodevenezuela.com"/> URL 4: <input type="text" value="www.instagram.com"/> </div> <div style="margin-top: 10px;"> Keyword 1: <input type="text"/>Keyword 3: <input type="text"/> Keyword 2: <input type="text"/>Keyword 4: <input type="text"/> </div> <div style="margin-top: 10px;"> Note: only three applications can be blocked per policy. </div> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="flex: 1;"> Applications <div style="border: 1px solid #ccc; padding: 5px; height: 150px; overflow-y: auto;"> HTTPS(443-443) FTP(21-21) POP3(110-110) IMAP(143-143) SMTP(25-25) NNTP(119-119) Telnet(23-23) SNMP(161-161) TFTP(69-69) IKE(500-500) DNS(53-53) </div> </div> <div style="flex: 1; text-align: center;"> <input type="button" value=">>"/> <input type="button" value="<<"/> </div> <div style="flex: 1;"> Blocked List <div style="border: 1px solid #ccc; padding: 5px; height: 150px; overflow-y: auto;"> Ping(0-0) HTTP(80-80) </div> </div> </div>
---	---

Figura 75. Restricciones de política para el Router wifi privado.

Fuente: Elaboración propia.

De esta manera, en las figuras **68, 69 y 70** se observa la configuración de las fases del enrutador inalámbrico para establecer servicio wifi privado, donde se determinaron los direccionamientos del Network basados en las IP de enlace del Router principal ubicado en la VLAN Entrada, asimismo, se activa un servicio LAN en caso de necesitar establecer conexión por cable en este dispositivo. Además, se determinó un ruto de enlace lógica ligado hacia el cortafuego ubicado en la VLAN de Despacho Central, determinando una dirección IP 192.168.3.50/24. De la misma manera, se activar el comando SSID dentro de este enrutador que permita ocultar el punto de acceso, de manera que solo el personal autorizado pueda acceder a sus servicios. Asimismo, se estableció una la configuración Wireless, donde de asignar un clave de modelo WPA2-PSK con una encriptación TKIP, que garantice la seguridad de los equipos que se intente conectar a este elemento.

Asimismo, se determinar direcciones de restricción en este equipo de manera que permita bloqueo el acceso en la web de ciertas URLs, que puedan llegar a establecer algún evento maligno dentro de la red (**ver figura 72 y 73**). De la misma forma, se determinan niveles de restricción con durabilidad para ciertos sitios web que son de utilidad para la Contraloría, cabe

destacar que cada una de estas restricciones son tomadas de los resultados obtenidos mediante las entrevistas. (**ver figura 74 y 75**).

En relación con los niveles de velocidad se maneja en el nuevo diseño de la red, se determinó mediante la estructuración lógica dos modelos de velocidad en el transporte de datos, es decir que las segmentaciones constante tráfico están configuradas con una subida y descarga de datos de 1000 Mbps mediante los procesos de half-dúplex, por otra parte, se determinar velocidades de 100 Mbps mediante el proceso de conexión full-dúplex.

The screenshot shows a Windows Command Prompt window titled "Coordinadora de despacho". The window has tabs at the top: Physical, Config, Desktop (which is selected), Programming, and Attributes. The main area displays the output of a ping command. The output shows multiple replies from the IP address 192.168.8.3, each with bytes=32, time<1ms, and TTL=128. It also shows ping statistics for 192.168.8.3, indicating 25 packets sent, 25 received, 0 lost, and 0% loss. The approximate round trip times are listed as minimum = 0ms, maximum = 16ms, and average = 1ms. At the bottom of the window, there are control characters: Control-C, ^C, and C:\>. A "Top" button is visible at the bottom left.

```
Reply from 192.168.8.3: bytes=32 time<1ms TTL=128
Reply from 192.168.8.3: bytes=32 time<1ms TTL=128
Reply from 192.168.8.3: bytes=32 time=1ms TTL=128
Reply from 192.168.8.3: bytes=32 time<1ms TTL=128
Reply from 192.168.8.3: bytes=32 time<1ms TTL=128
Reply from 192.168.8.3: bytes=32 time<1ms TTL=128
Reply from 192.168.8.3: bytes=32 time=3ms TTL=128
Reply from 192.168.8.3: bytes=32 time<1ms TTL=128
Reply from 192.168.8.3: bytes=32 time=1ms TTL=128
Reply from 192.168.8.3: bytes=32 time=3ms TTL=128
Reply from 192.168.8.3: bytes=32 time=1ms TTL=128
Reply from 192.168.8.3: bytes=32 time=16ms TTL=128
Reply from 192.168.8.3: bytes=32 time<1ms TTL=128
Reply from 192.168.8.3: bytes=32 time=1ms TTL=128
Reply from 192.168.8.3: bytes=32 time=1ms TTL=128
Reply from 192.168.8.3: bytes=32 time=1ms TTL=128
Reply from 192.168.8.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.8.3:
    Packets: Sent = 25, Received = 25, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 1ms

Control-C
^C
C:\>
```

Figura 76. Velocidades de la nueva red (half-dúplex).

Fuente: Elaboración Propia. (2022)

En la **figura 76** se observan la prueba de velocidad de la nueva red en relación a los equipos con direccionamiento de IP estático mediante el servicio brindado por cortafuegos gracias a la ruta de acceso hacia el Gateway, para garantizar los procesos operativos que se realicen, por lo

cual está manejando promedios de respuesta máxima de 2 milisegundos por paquete, con un tiempo de vida entre paquetes (TTL) de ciento veinte (120) ms por paquete.

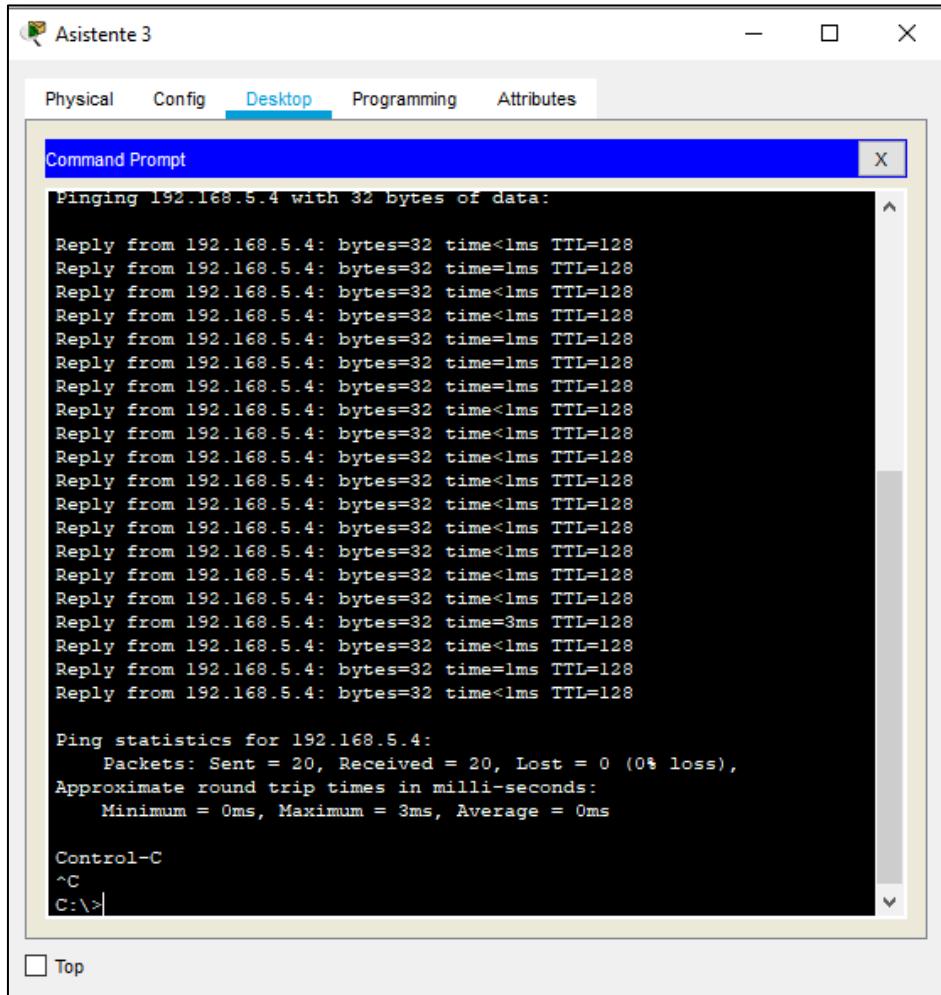


Figura 77. Velocidades de la nueva red (full-dúplex).

Fuente: Elaboración propia. (2022)

Por otra parte, en la **figura 77** se visualiza el otro modelo (half-dúplex) que se configuró para los equipos con direccionamiento de IP dinámico debido a que no necesitarán realizar grandes procesos de transporte de data, por lo cual se maneja un promedio de velocidades de 100 Mbps. En esta ocasión, se obtuvo un promedio de subida y descarga igual al anterior (2 milisegundos); sin embargo, el tiempo de vida (TTL) varía a doscientos cincuenta y dos (255) ms por paquete, debido a la configuración dada mediante conexión Fast-Ethernet de los Switch. Cabe destacar, que los servidores también trabajarán con este tipo de velocidad.

Entrando con la estructuración y representación física de la nueva red alambica para la contraloría del Municipio Antolín del Campo, se establece el transporte del cableado Ethernet por

medio de las canales de red las cuales se están ubicadas arras de techo de manera que permita mantener la seguridad física del elemento transportado, así mismo ayudara a identificar las conexiones para cada máquina dentro de las zonas de trabajo. Por otra parte, se identifica la sede para resguardo de los equipos de red, donde además se establece dentro esta sede un armario para establecer los racks correspondientes para mantener control y funcionalidad de la nueva red. De esta manera, para lograr mantener un control de todos los elementos que forman parte de cada segmentación representante en este diseño, se determinó establecer una esquematización completado de la red LAN. Además, se estableció los materiales necesarios para la estructuración de este nuevo diseño en cada planta de la Contraloría.

Equipos Administrativos/Seguridad física										
Equipo	Descripción	IP	Capa de Red	Interfaz Entrada	Interfaz Salida	Gateway	Nombre del Gateway	Nombre de la VLAN	Velocidad ancho de banda	
Laptop	Despacho de la Contraloría	192.168.1.30	255.255.255.0	Fa0	Et 0/1	192.168.1.1	Cortafuegos 2	Despacho_Central	100 Mbps	
PC 1	Administradora de la Contraloría	192.168.7.10	255.255.255.0	Fa0	Fa0/2	192.168.7.1	Switch 2	Adminitration Central Recursos Humanos	100 Mbps	
PC 2	Coordinadora de Recursos Humanos	Dinámica	255.255.255.0	Fa0	Fa0/3				10 Mbps	
PC 3	Asistente de Recursos Humanos		255.255.255.0	Fa0	Fa0/4				10 Mbps	
PC 4	Coordinadora de Despacho	192.168.8.10	255.255.255.0	Fa0	Fa0/2	192.168.8.1	Switch 1	Coordinación de Despacho_Auditoria Interna_Atención al Cliente	100 Mbps	
PC 5	Auditoria Interna	Dinámica	255.255.255.0	Fa0	Fa0/3				10 Mbps	
PC 6	Atención al Cliente		255.255.255.0	Fa0	Fa0/4				10 Mbps	
PC 7	Coordinadora de dirección de la Administración Central	192.168.6.4	255.255.255.0	Fa0	Fa0/2	192.168.6.1	Switch 3	Dirección de Control de la Administración Central	100 Mbps	
PC 8	Primer(a) Asistente de la Coordinadora de dirección de la Administración Central	Dinámica	255.255.255.0	Fa0	Fa0/5				10 Mbps	
PC 9	Segundo(a) Asistente de la Coordinadora de dirección de la Administración Central		255.255.255.0	Fa0	Fa0/3				10 Mbps	
PC 10	Oficinista de Asistente de la Coordinadora de dirección de la Administración Central		255.255.255.0	Fa0	Fa0/4				10 Mbps	
PC 11	Coordinadora de dirección de la administracion de entidades descentralizadas	192.168.5.4	255.255.255.0	Fa0	Fa0/2	192.168.5.1	Switch 4	Control de la administración de Entidades Descentralizadas	100 Mbps	
PC 12	Primer(a) Asistente de Coordinadora de dirección de la administracion de entidades descentralizadas	Dinámica	255.255.255.0	Fa0	Fa0/3				10 Mbps	
PC 13	Segundo(a) Asistente de Coordinadora de dirección de la administracion de entidades descentralizadas		255.255.255.0	Fa0	Fa0/4					
PC 14	Primer(a) Oficinista de Coordinadora de dirección de la administracion de entidades descentralizadas		255.255.255.0	Fa0	Fa0/5					
PC 15	Segundo(a) Oficinista de Coordinadora de dirección de la administracion de entidades descentralizadas		255.255.255.0	Fa0	Fa0/6					
Impresora 1	Impresora de la Administradora Central	192.168.7.12	255.255.255.0	Fa0	Fa0/5	192.168.7.1	Switch 2	Adminitration Central Recursos Humanos	10 Mbps	
Impresora	Impresora de Despacho Central	192.168.2.18	255.255.255.0	Fa0	Et 0/2	192.168.2.1	Cortafuegos 2	Despacho_Central		
Cámara 1	Camaras de seguridad de la zona de resguardo	192.168.2.3	255.255.255.0	Fa0	Fa0/2	192.168.2.1	Switch 5	Equipos de Seguridad Física		
Cámara 2		192.168.2.4	255.255.255.0	Fa0	Fa0/3					
Cámara 3		192.168.2.5	255.255.255.0	Fa0	Fa0/4					
Cámara 4		192.168.2.6	255.255.255.0	Fa0	Fa0/5					
Detector de Monóxido 1		192.168.2.7	255.255.255.0	Fa0	Fa0/6					
Detector de Monóxido 2		192.168.2.8	255.255.255.0	Fa0	Fa0/7					
Servidor	Proxy	192.168.3.2	255.255.255.0	Fa0	Et0/7	192.168.3.1	Cortafuegos 1	DMZ	10 Mbps	
Servidor	Local de Nómina	192.168.4.10	255.255.255.0	Fa0	Et/06	192.168.4.1				

Cuadro 18. Esquematización de los equipos administrativos y de seguridad del nuevo diseño.

Fuente: Elaboración propia. (2022)

De esta manera, en el **cuadro 18** se observa todos los elementos que van a formar parte de este diseño planteado, de manera que permita visualizar los componentes de cada segmento (VLAN) dentro de la infraestructura LAN, indicando sus puertas de enlace lógicos y físicas para su conectividad. Donde, además dispone representar las puertas de enlaces correspondientes en conjunto con la dirección IP establecida para cada equipo, junto a los a velocidades que les corresponde de manera que permita en el futuro realizar funciones de actualizaciones/mantenimiento óptimas dentro de la red.

Elemento	Cantidad
Cable Coaxial	13,9 m
Cable de Red	130,91 m
Conectores Rj45	38 unidades
Jack Coupler	19 unidades
Botas de Red	38 unidades
Canaletas	44 unidades
Tomas de red	11 unidades

Cuadro 19. Materiales para la estructuración de la planta alta.

Fuente: Elaboración propia. (2022)

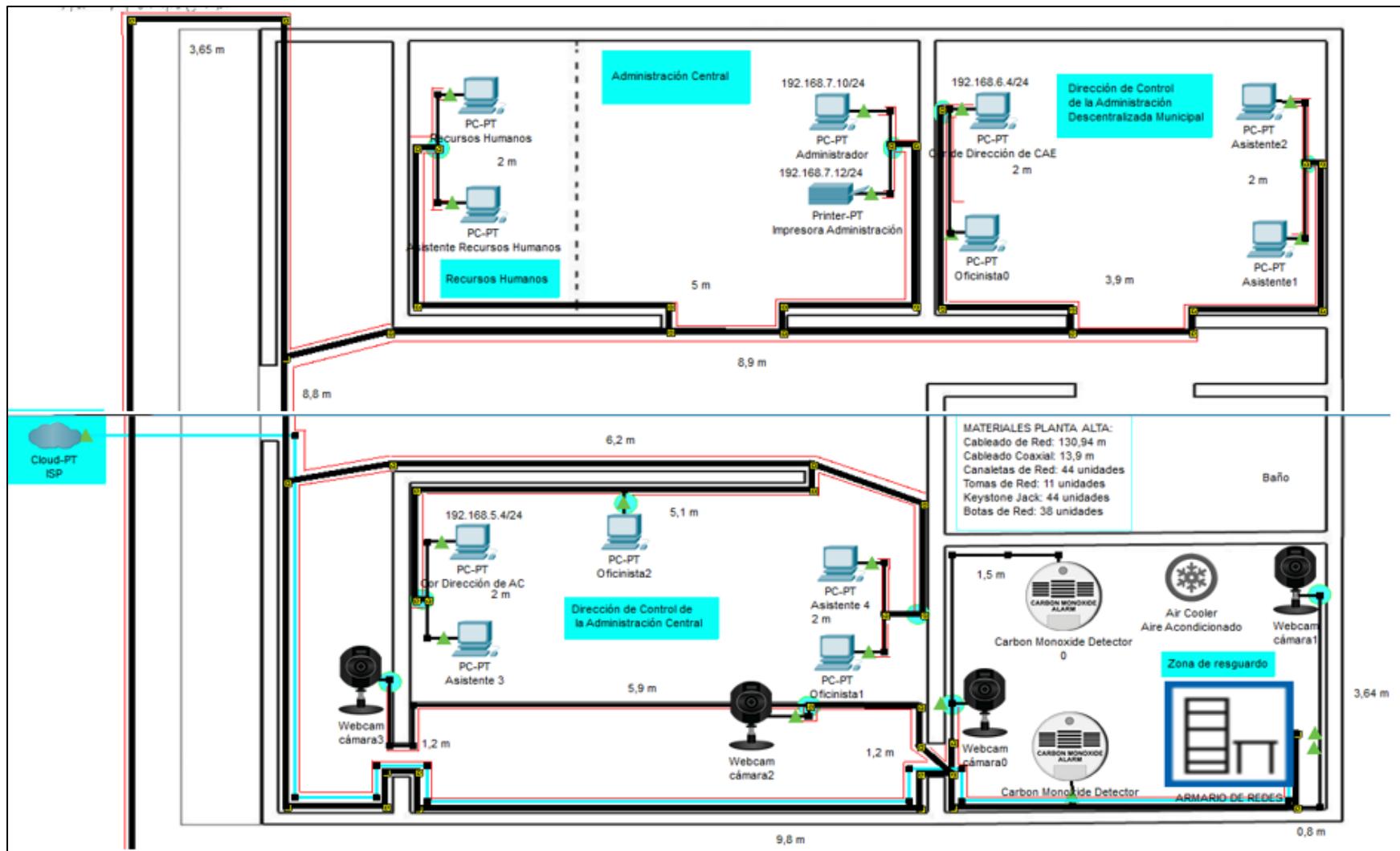


Figura 78. Estructuración y representación física de la planta alta para la nueva red.

Fuente: Elaboración Propria. (2022)

En la **figura 78**, se identifica el suministro de transporte de red de la planta alta de la Contralor, que se implementa para el nuevo diseño de la red. Primero, dado a que el Organismo no presenta un espacio abierto para ubicar el armario de redes mediante cual se establecen las conexiones por cablea, se ve la necesidad de abrir espacio para asignar una zona de resguardo de los equipos que permita transportar el cableado coaxial y el cableado UTP. (**ver figura 78**)

Luego se a ver realizado esta acción anterior, se establece una conexión mediante cableado coaxial provenientes del proveedor de internet, transportado mediante un orificio realizado cerca la ventana de dicha planta, asimismo, este cableado será conducido arras de techo mediante la implementación de canaletas de 3 entrada, donde se establecen canaletas individuales su trasladado hacia el armario de redes abarcando un total de material de 13,9 m de cableado coaxial y 4 unidades de canaletas. La razón, por lo cual se considera este diseño para el traspaso de cableado hacia el armario, se basa que si en el futuro se ve la necesidad cambiar de ISP el procedimiento para la instalación del nuevo servicio se puede realizar de manera más fácil y segura, ayudando de esta manera a evitar problemas con el procedimiento que se plantea a continuación. (**ver cuadro 18**)

Ahora, para conectar a los equipos de red ubicados en el armario con los equipos administrativos de lo departamento de este piso, se determinó implementar el cableado de red también arras de techo, pero sin realizar perforaciones en las paredes, sino que se ira construyendo pista mediante las canaletas para el transporte del cableado, el cual saldrá mediante un a cada departamento mediante tomas de red en las cuales se ubican Jack Coupler para poder conectar al cableado de red mediante puntos de acceso físico. Dando entonces un total de materiales a utilizados de 130,94 m de cableado de red, junto a total de 44 unidades de canaletas para toda el área de la planta alta de la Contraloría. Además, se necesitó implementar 11 unidades para tomas de red junto a 44 conectores Jack Coupler. (**ver cuadro 18**). Por otra parte, ubicamos los recursos necesarios para la estructuración de la planta baja.

Elemento	Cantidad
Cable de Red	130,91 m
Conectores Rj45	38 unidades
Jack Coupler	19 unidades
Botas de Red	38 unidades
Canaletas	44 unidades
Tomas de red	6 unidades

Cuadro 20.Materiales para la estructuración de la planta alta.

Fuente: Elaboración propia. (2022)

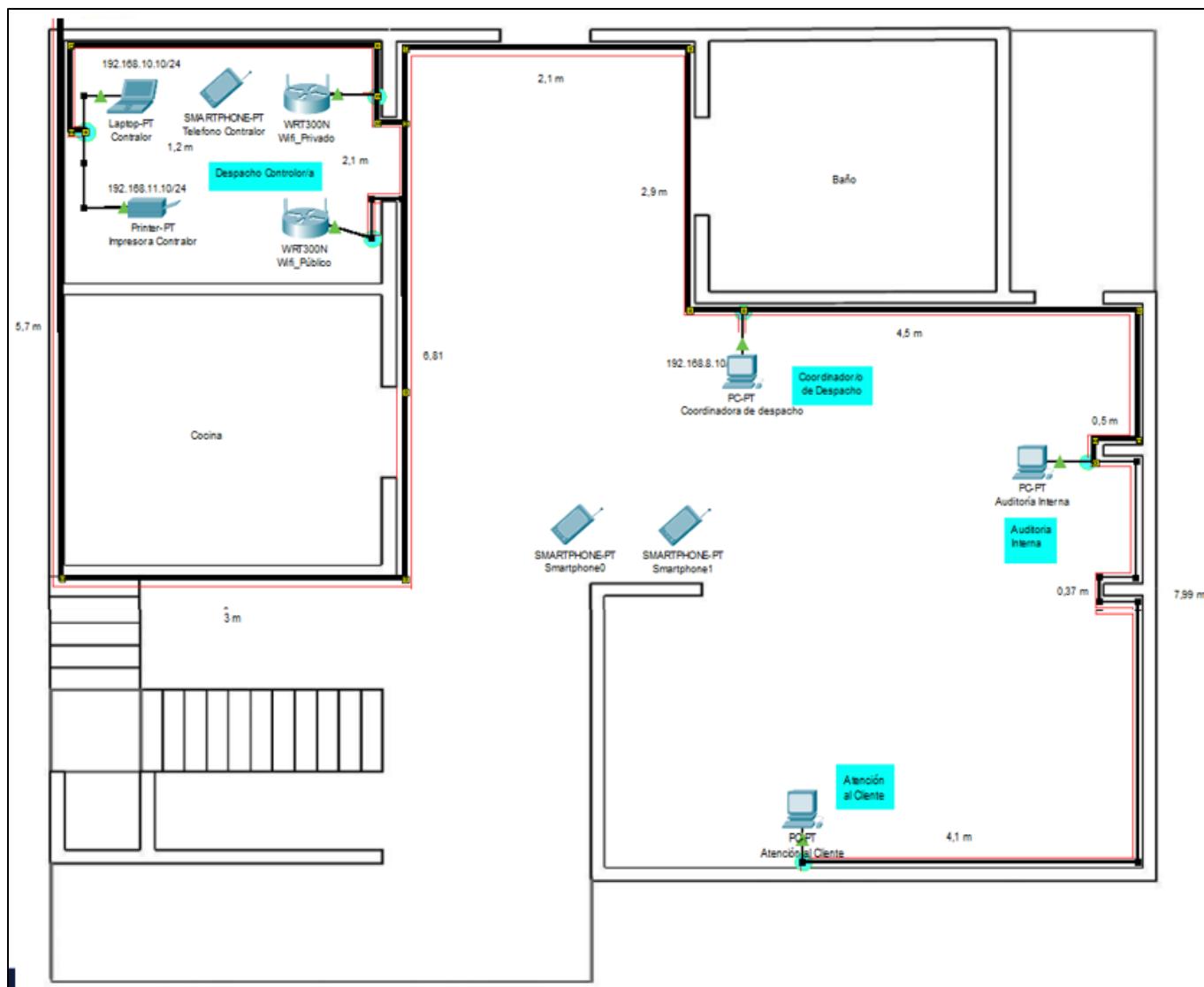


Figura 79. Estructuración y representación física de la planta baja para la nueva red.

Fuente: Elaboración Propria. (2022)

Por otra parte, en la **figura 79** se representan de manera detallada el transporte de red la planta baja de la Contraloría, donde se determina el traslado de cableado UTP mediante la zona de las escaleras de manera que permita comunicar ambas plantas, asimismo, se establecen canaletas arras de techo por las cuales pasara el cableado de red pasara cada departamento de la planta baja, donde también se establecen zonas de acceso físico mediante tomas de red con Jack Coupler para facilitar la conexión del cableado hacia los equipos. Generando de esta manera un total de materiales de 103,91 m de cableado UTP, asimismo, un total de 44 unidades de canaletas, además se necesitó implementar 6 tomas de red junto a 19 unidades de Jack Coupler. (**ver cuadro 19**)

En este mismo sentido, para todo el cableado de red UTP implementado para cada los equipos administrativos, equipos de red y de seguridad se implementaron conectores físicos rj45 de manera que brinden poder establecer conexiones dentro de los dispositivos, donde además se determinó botas de red para cada extremo de cableado de manera que brinde estabilidad a niveles seguridad física para cada cable. Dando de esta manera un total de 38 conectores rj45 y botas de red para el diseño de la nueva red. (**ver cuadro 19**)

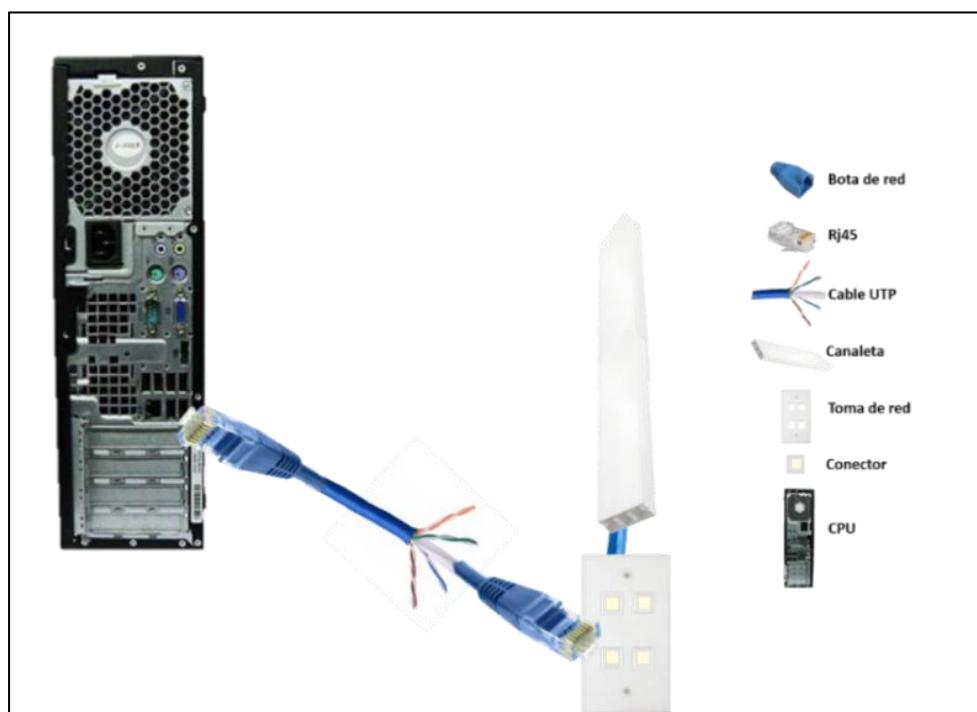


Figura 80. Distribución física para las conexiones de las máquinas de la Contraloría.
Fuente: Elaboración Propia. (2022)

En relación distribuciones físicas de los puntos de acceso formados por las tomas de red mencionados anteriormente (**ver figura 80**), estas están estructuradas por la llegada del cableado UTP transportado mediante las canaletas a cada departamento, donde se establece una conexión mediante una toma de red física mediante un conector (Coupler) unida mediante cable de red ponchado donde se le establece con rj45 junto bota de red correspondiente para cada extremo de cable.

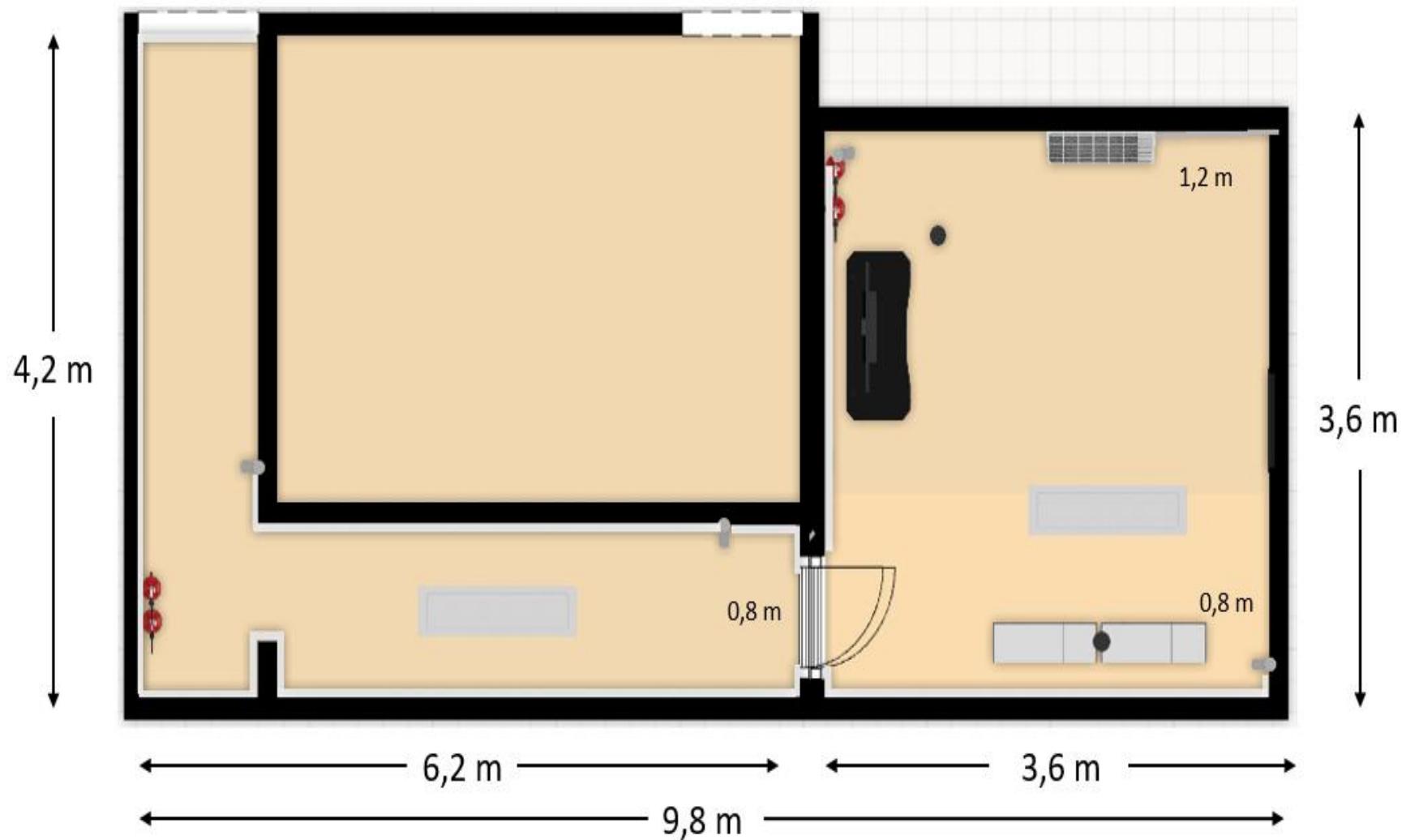


Figura 81. Vista aérea de la zona de resguardo de la nueva red.
Fuente: Elaboración Propia. (2022)



Figura 82. Vista lateral (3D) de la zona de resguardo.

Fuente: Elaboración propia. (2022)

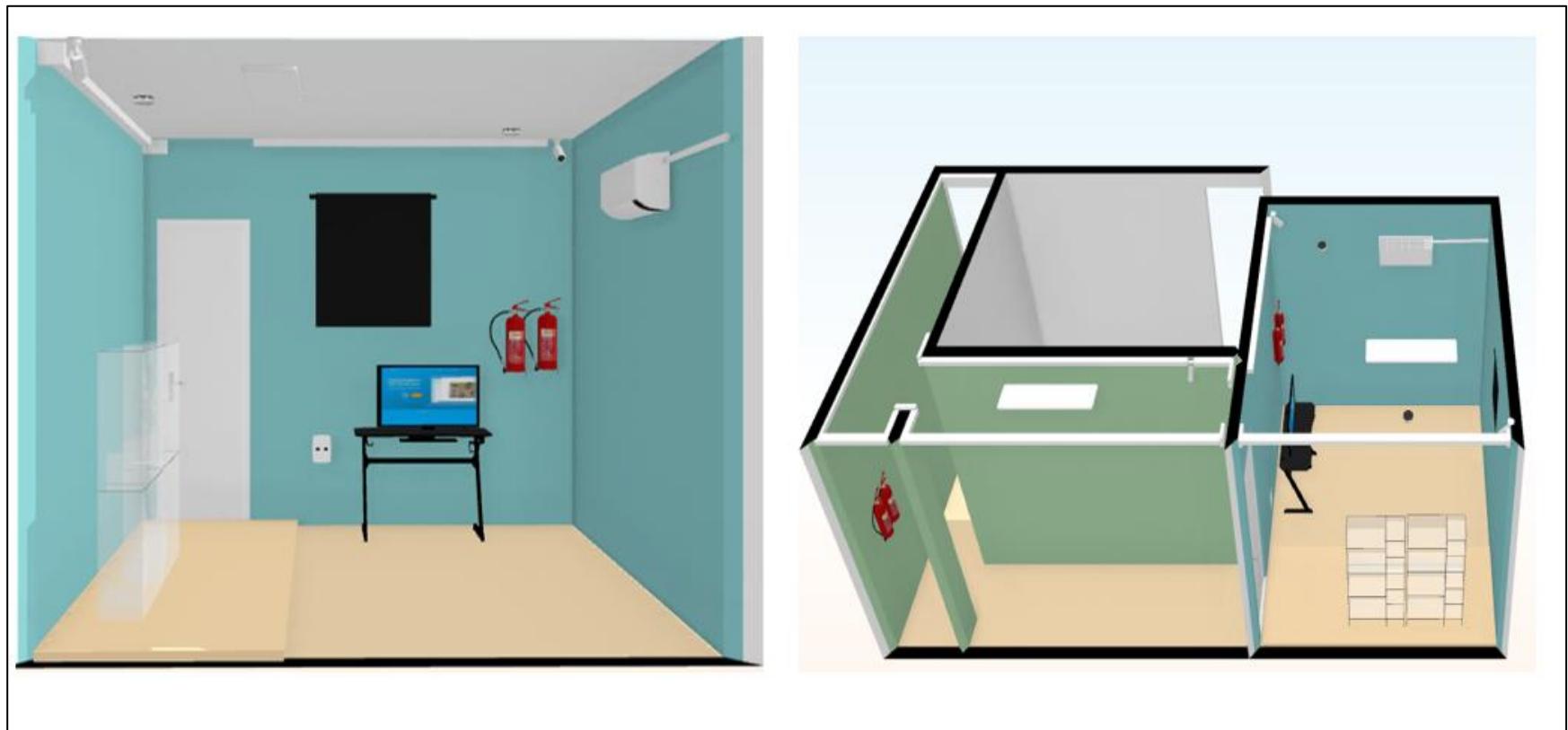


Figura 83. Distribución completa (3D) de la zona de resguardo.

Fuente: Elaboración propia. (2022)

Por otra parte, en la **figura 81** se observa el lugar de resguardo de los equipos de red donde el diseño de mismo se tuvo que realizar un orificio de entrada para generar una puerta para la zona, debido a que es un lugar sin acceso actualmente en la Contraloría. Este espacio está constituido por un espacio físico de doce con noventa y sies (12,96) metros cuadrados, donde ubica el armario de red en el cual se ubican todos los equipos de red, este armario tiene la disponibilidad de conectarse directamente hacia la corriente eléctrica, sin embargo, se le establece regletas reguladoras de voltaje junto a un protector de voltaje de manera que permite proteger la integridad física de los elementos almacenados en el armario, igualmente de determino una fuente de alimentación interrumpida que permita surtir a estos equipos de red en tal caso de exista caído del servicio eléctrico dentro de la Contraloría.

Así mismo, se establece un equipo de refrigeración (aire acondicionado) que se ubicara al frente del armario de redes, de manera que pueda proporcionar estabilidad de temperaturas a los equipos ubicados en dicho armario evitando así sobrecalentamientos de los mismos. De la misma manera, para establecer el desagüe del aire acondicionado se determina aplicar un orificio a la pared a mano derecha ubicada en la zona de resguardo para dar salida a la exterior (jardín) de la Contraloría para evitar accidentes dentro de área. Cabe destacar que este equipo estará conectado a la corriente con su respectivo protector de voltaje y regleta reguladora. (**ver figuras 81 y 82**)

De la misma manera, se establecen dos (2) equipo para la vigilancia (cámaras de seguridad) dentro de la zona de resguardo de manera que permitan mantener un control y protección de los equipos dentro del área. Por otra parte, se establecen otras dos cámaras en la parte externa de la zona de resguardo. Estos elementos de seguridad estarán conectados mediante cableado de red UTP transportador por canaletas arras de techo hasta el armario de red. (**ver figuras 82 y 83**)

Por otra parte, se establecen dos (2) detectores de humo y monóxido de carbono dentro de la zona de resguardo de manera de permitan prevenir o informar sobre problemas de incendios eléctricos dentro del lugar. De esta manera, brindar solución si llegara a pasar este fenómeno se establecen extintores de incendios especiales, distribuidos dentro y fuera de la zona de resguardo de manera de garantizar la estabilidad física de los equipos. Dentro esto mismo margen de ideas, se designan despegues de baño dentro de la zona de resguardo, debido a este lugar está localizado en cercanía a un baño, por lo cual se toma sumo preclusión en tal caso de existir inundaciones en el lugar, por lo cual se diseña un desnivel dentro de la zona. (**ver figura 83**)

En otra medida, para poder establecer de manera física todas las conexiones por cableado transportado por la canaletas se diseña un armario de redes ubicado en la zona de resguardo (**ver figura 64**), en el cual se ubicaran todos los equipos de red de la nuevo red alámbrica para la Contraloría de manera de poder resguardar estos elementos contra algún ataque físico que les pueda ocurrir, ya que representan toda la configuración lógica y física de la infraestructura de red de la Institución, además va a permitir poder realizar labores de mantenimientos o chequeo de una manera más rápida y sencilla.

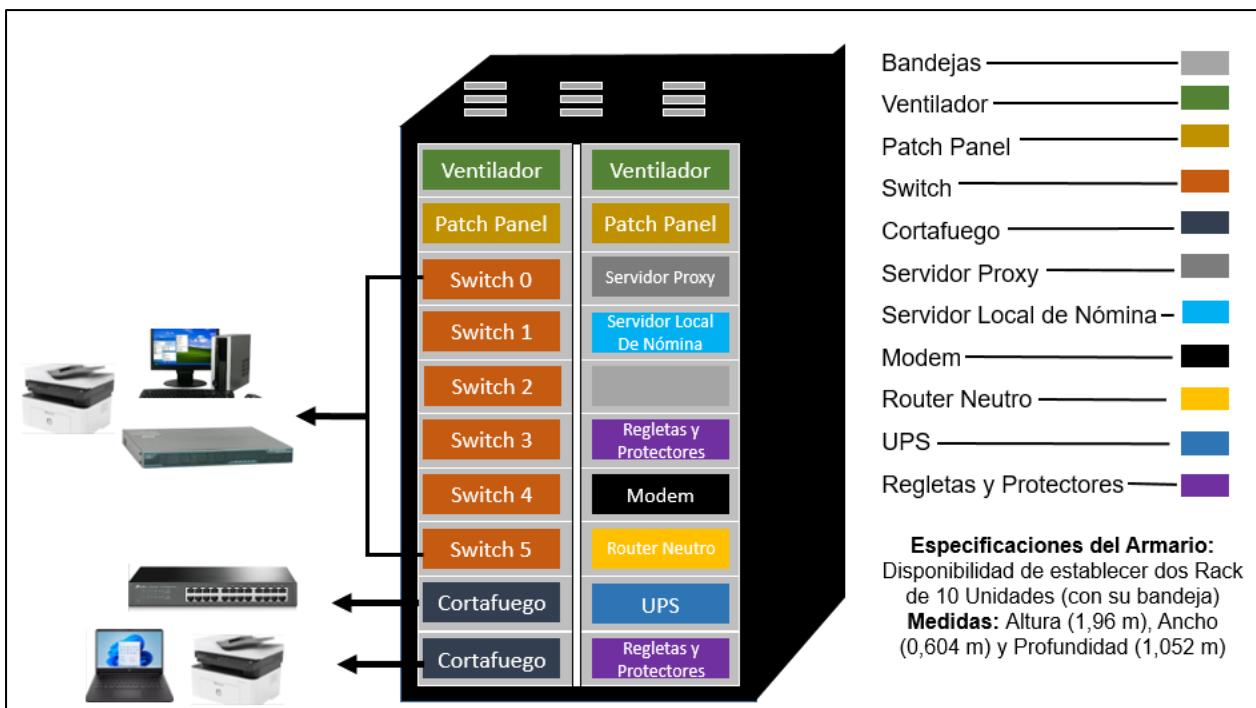


Figura 84. Estructura del armario de red.

Fuente: Elaboración Propia. (2022)

En la **figura 82**, se observan los elementos que están representando dentro de armario de red, identificando dos (2) racks para el almacenamiento de los equipos de la nueva red. En el primero de ellos se ubican todos los equipos de red encargados de transmitir, enrutar y segmentar las señales para las conexiones hacia los equipos administrativos y de seguridad y, el otro rack es establecido para almacenar los equipos de cómputo (servidores), en conjunto con los equipos encargados de captar la señal proveniente del servicio de internet. Destacando, que ambos racks cuentan con capacidad de 10 unidades, donde se incorporan ventiladores para su refrigeración.

En la **figura 82**, se observa la estructuración física de cada elemento ubicado dentro del primer rack del armario de red en el cual se establecen todos los equipos de conexión (Router) y

comutación necesarios para establecer conectividad en la red (Switch), en conjunto con los equipos escogidos para ayudar segmentar los niveles de acceso (cortafuegos) a la red de manera que faciliten su proceso de conexión por cableado de red y a su vez agilice los trámites de mantenimientos o actualizaciones de los equipos. Por otra parte, se representan de manera visual los dos modelos de cableado UTP Ethernet implementados, observando entonces un cableado directo sin trenzar para intercomunicar a los equipos de red entre sí (Switch-cortafuego) y un cableado trenzado para relacionar a las máquinas con la red (pc-Switch/cortafuegos).

Para finalizar con la estructuración física de la red, encontramos el segundo rack del armario de redes en el cual se establecen los equipos que contienen todos los servicios de la red (**ver figura 82**), es decir, los servidores Proxy y Nómina, debido a que estos necesitan estar ubicados en zonas diferentes para evitar problemas de interconexión debido al electromagnetismo, y también ayudando a controlar los accesos a los mismos. Además, mediante esta configuración establecida para el rack 1 y 2 es posible que en el futuro puedan asignarse nuevos equipos de red al armario sin la necesidad de tener que generar un nuevo diseño en la estructuración.

CONCLUSIONES

Luego de haber realizado un análisis general de la red existente en la Contraloría del Municipio de Antolín del Campo permitió determinar las fallas que presenta la misma, tales como: desconexiones en los equipos administrativos de las redes wifi, junto a la constante caída de los servicios del ISP, lo que genera fallas de latencia entre los departamentos que conforman el organismo. Así mismo, se reflejaron pérdidas de paquetes dentro de la red dado a la ineficiencia del estándar de los equipos de red, sumado a que dichos elementos no presentan las óptimas condiciones para brindar su servicio. Por otra parte, no cuentan con una zona para la protección física de estos elementos. Por su parte, se percibió el desconocimiento del personal de la contraloría referente al área de redes, lo que ha generado vulnerabilidad interna dentro de la institución, como la infección de equipos dentro de la red. Además, se logró identificar que no se cuenta con un departamento de sistemas que se encargue de brindar un servicio de soporte técnico interno en tal caso de existir alguna falla o inconveniente dentro del Organismo.

Del mismo modo, se logró determinar la normativa adecuada (EIA) para el levantamiento del cableado de red para el diseño propuesto, resaltando por ello un transporte aras del techo con una longitud máxima de 100 metros por cable. Así mismo, se identificaron los modelos de categorías óptimas para los nuevos equipos que conforman el diseño de red, donde se eligió la característica de estándar de categoría 5e para el cableado y todos los equipos de red de manera que permitan la alta compatibilidad entre ellos. De la misma forma, se determinó el modelo de equipo de cómputo necesario para la configuración del servidor proxy de reserva basado en una máquina HP que posee las características requeridas para la ejecución de los servicios; así como también se establecieron los equipos necesarios para la protección física de los elementos de la red. También se identificaron las configuraciones óptimas para el correcto funcionamiento de la nueva red, basado en un nivel de capas regidas por la normativa OSI.

Por otra parte, se logró identificar el modelo más adecuado para el diseño lógico y físico de la red, dando entonces una topología de red de árbol inicializada por un cortafuego central desde el cual se subdividen ramificaciones hacia los switches conformando una topología de estrella englobada dentro de la topología inicial. De la misma manera, se determinaron protocolos para el direccionamiento de red dinámico y estático según el nivel de importancia del equipo dentro de la infraestructura, basados en una máscara de red de capa 24 para todo el nuevo diseño.

Además, se determinó que la distribución de Linux de Ubuntu server es el adecuado para el levantamiento del servidor proxy para establecer los protocolos de servicios FTP, TFTP, DNS, HTTP, HTTPS y NTP para el óptimo funcionamiento de la red alámbrica. De igual manera, se establecieron las segmentaciones de red que permitan lograr mejorar la estabilidad de red, dado a que se logra otorgar controles y servicios de seguridad únicas para cada segmento. Igualmente, se logró fijar la configuración física adecuada para la zona de resguardo, junto a la implementación de un armario de red donde se ubicaron dos (2) modelos de rack junto a un estante para equipos, de manera que se eviten problemas de interferencia y latencia en la red.

Finalmente, se logró diseñar una red de área local alámbrica que permita la conectividad y seguridad óptima de los datos regulados mediante un servidor proxy para la Contraloría del Municipio de Antolín del Campo, la cual no solo mejorará las velocidades de trasferencia de datos, sino que también disminuirá el tiempo de espera de respuesta al momento de realizar una petición. Además, este nuevo diseño logra establecer parámetros que permiten dividir las áreas de trabajo de manera que se mitigue el riesgo de robo de información. De igual manera, se lograron establecerlos procesos para la protección física y lógica del nuevo diseño, donde se dejaron configurados puentes de enlace para la conectividad de futuros equipos o elementos en la red.

RECOMENDACIONES

Después de completar el desarrollo de la presente investigación, se pueden agregar recomendaciones en función de mejorar los aspectos funcionales y estructurales, o sea, aumentar los procesos de conectividad, de manera que permita aprovechar al máximo el rendimiento del nuevo diseño de red de área local alámbrica, prologando así su vida útil. Dichas recomendaciones se presentan a continuación:

- Conformar un Departamento de sistema, el cual sea el único que tenga acceso total a la red de manera que permita establecer nuevas configuraciones dentro de la red o hacia los servidores, y además de proporcionar medidas de respuesta inmediata dentro de la Contraloría, en caso de suceder alguna falla lógica o física dentro de la infraestructura de red.
- Contratar un nuevo proveedor de servicio de internet, el cual provea una mayor capacidad de ancho de banda de manera que permita aprovechar aún más el nuevo diseño planteado.
- Para mantener el óptimo funcionamiento de la red, se requiere implementar planes estratégicos para mejorar el conocimiento del personal de la contraloría en relación a las medidas de seguridad de la red, de manera que ayude a prevenir vulnerabilidad dentro de la red.
- Realizar pruebas para el control del transporte de electricidad dentro de la Contraloría, dado a que se observaron fallas constantes con el servicio eléctrico que pueden llegar a afectar al interruptor automático del lugar, generando así una sobrecarga eléctrica que pueda dañar a los equipos administrativos o de red.
- Llevar a cabo un estudio de la infraestructura de la sede de la Contraloría para determinar si existen posibles daños a nivel estructural y así evitar posibles daños de la red en caso de que ocurra algún fenómeno natural.
- Se recomienda contratar un servicio de respaldo AWS, que permita resguardar la información que se maneje dentro de los servidores en caso de suceder algún inconveniente de estos datos.

FUENTES REFERENCIALES

- American Data. (s.f.). *Redes de datos y sus componentes*. Recuperado el 30 de junio de 2022 de <https://www.data.cr/2021/06/02/redes-de-datos-y-sus-componentes/>
- Arias, F. (2004). *El proyecto de investigación: Introducción a la metodología científica*. (4ta. ed.). Caracas: Edit.Episteme.
- Arias, F. (2012). *El proyecto de investigación: Introducción a la metodología científica*. (4ta. ed.). Caracas: Edit.Episteme.
- Arias, F. (2006). *El proyecto de investigación: Introducción a la metodología científica*. (5ta. ed.). Caracas: Edit.Episteme.
- Asociación Profesional de Ingenierías de Seguridad y salud en las obras de Construcción. *Firewalls o servidores de seguridad*. Recuperado el 30 de junio de 2022 de https://www.issco.unige.ch/en/research/tutoriel_informatique/ES/firewalls_o_servidores_de_seguridad.html
- Balestrini, M. (2006). *Como se elabora el proyecto de investigación*. (7ma. ed.). Madrid: Edit. Planeta.
- Ballester, A. (2021). *Sistema de información para la toma de decisiones comerciales*. Recuperado el 16 de agosto de 2021, de: <https://www.gestiopolis.com/sistema-de-informacion-para-la-toma-de-decisiones-comerciales>.
- Borges, S. (27 de agosto de 2017). *Servidor Proxy*. Recuperado el 30 de junio de 2022 de <https://blog.infranetworking.com/servidor-proxy/>
- CONATEL. (). *Ley de Infogobierno*. Recuperado el 05 de julio de 2022 de <http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-de-Infogobierno.pdf>
- CONSTITUCIÓN DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA. Gaceta Oficial Extraordinaria N°36.860 de fecha 30 de diciembre de 1.999
- Cuadrocomparativo.org (s.f.). *Cuadro descriptivo: que es, elaboración y ejemplos*. Recuperado el 09 de julio de 2022 de <https://cuadrocomparativo.org/cuadro-descriptivo/>
- Curriculum Exploratorios en TIC. (s.f.). *Componentes de una red*. Recuperado el 30 de junio de 2022 de <http://contenidos.sucerman.com/nivel3/redes/unidad1/leccion2.html>
- Chafloque, J. (2018). *Propuesta de diseño de una red de datos de área local bajo la arquitectura de redes definidas por software para la red telemática de la Universidad Nacional Mayor de San Marcos*. Recuperado el 30 de junio de 2022 de

[https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10017/Chafloque_mj.pdf
?sequence=3&isAllowed=y](https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10017/Chafloque_mj.pdf?sequence=3&isAllowed=y)

Debian. (s.f.). *Configuración de red*. Recuperado el 30 de junio de 2022 de <https://debian-handbook.info/browse/es-ES/stable/sect.network-config.html>

Eumed.net. (s.f.). *Matriz DOFA*. Recuperado el 09 de julio de 2022 de https://www.eumed.net/libros-gratis/2011d/1042/matriz_dofa.html#:~:text=El%20prop%C3%B3sito%20de%20la%20matriz,eficiente%20de%20los%20objetivos%20organizacionales.

Fernández, L. (s/f). *Definición y Características: Croquis*. Recuperado el 05 de Junio de 2022 de <https://www.caracteristicas.co/croquis/>

Figueroa, M. (2016). *Análisis e Interpretación de los Datos*. Recuperado el 05 de julio de 2022 de <https://sabermetodologia.wordpress.com/2016/03/06/analisis-interpretacion-datos/>

Figueroa y Vincenty. (27 de abril de 2011). *Muestreo por convivencia*. Recuperado el 05 de julio de 2022 de <https://es.slideshare.net/selene1524/muestreo-por-conveniencia>

García, J. (2020). *Rediseño de red LAN de la compañía Core AdvanceGroup SAS*. Recuperado el 30 de junio de 2022 de https://repository.ucc.edu.co/bitstream/20.500.12494/34357/1/2020_Redise%C3%B3n_re_d_lan.pdf

Gómez, A. (s.f.). *Seguridad Informática Básico*. Recuperado el 30 de junio de 2022 de <https://www.ecoediciones.com/wp-content/uploads/2015/08/seguridad-informatica-basico.pdf>

Guzmán, D. (2018). *Redes de datos y sus componentes*. Recuperado el 30 de junio de 2022 de <https://www.data.cr/2021/06/02/redes-de-datos-y-sus-componentes/>

Hernández Sampieri, Fernández, c et al (2010). *Metodología de la investigación*. (6ta. ed.). México: Edit.McGraw-Hill

Hertzog, R y Mas, R. (2015). *El manual del administrador de Debian 10*. (1ra. ed.). Limburgo: Edit. Debian. Recuperado el 30 de junio de 2022 de <https://debian-handbook.info/browse/es-ES/stable/>

Hurtado, J. (2008). *Metodología de la Investigación Holística*. (3ra. ed.). Caracas: Edit. Sypal.

Koontz, H. y Weichrich, H. (2004). *Administración una perspectiva global*. (12va. ed.). Nueva York: Edit. McGraw-Hill.

Ledesma, D. (septiembre de 2018). *Reestructuración de la infraestructura de red LAN basado en las normas de cableado estructurado, y la aplicación de políticas de seguridad para el control de acceso mediante un servicio proxy Linux en la Unidad Educativa Hispanoamericano.* Recuperado el 30 de junio de 2022 de <https://dspace.ups.edu.ec/bitstream/123456789/17336/1/UPS-GT002618.pdf>

LEY DE INFOGOBIERNO. Gaceta Oficial Extraordinaria N.º 40.274 de fecha 17 de octubre de 2013

LEY ESPECIAL SOBRE DELITOS INFORMÁTICOS. Gaceta Oficial Extraordinaria N.º 37.313 de fecha 30 de octubre del año 2.001

LEY ORGÁNICA DE CIENCIA, TECNOLOGÍA E INNOVACIÓN. Gaceta Oficial Extraordinaria N.º 37.291 de fecha 26 de septiembre de 2.001

LEY ORGÁNICA DE TELECOMUNICACIONES. Gaceta Oficial Extraordinaria N.º 36.920 de fecha 28 de marzo del año 2.000

LEY SOBRE EL DERECHO DE AUTOR. Gaceta Oficial Extraordinaria N.º 4.638 Extraordinario defecha1 de octubre de 1.993

Leyva, N. (s.f.). *¿Qué es una red?* Recuperado el 30 de junio de 2022 de https://www.academia.edu/37005745/QUE_ES_UNA_RED

Limones, E. (07 de abril de 2021). *Topología de redes informáticas.* Recuperado el 30 de junio de 2022 de <https://openwebinars.net/blog/topologia-de-redes-informaticas/>

López, S. (s.f.). *Componentes de una red.* Recuperado el 30 de junio de 2022 de https://www.academia.edu/16384979/COMPONENTES_DE_UNA_RED

López, M. (s/f). *Cuadro descriptivo: qué es, elaboración y ejemplos.* Recuperado el 05 de julio de 2022 de <https://cuadrocomparativo.org/cuadro-descriptivo/>

Lucidchart. (2022). *¿Cuáles son tus necesidades de creación de diagramas de red?* Recuperado el 05 de julio de 2022 de <https://www.lucidchart.com/pages/es/que-es-un-diagrama-de-red>

McMillan James, Schumacher. (2005). *Investigación Educativa.* (5ta. ed.). California: Edit. Pearson Addison Wesley

Martínez, A. (05 de marzo de 2019). *Acerca de los puertos TCP/UDP; comparación, similitudes y diferencias.* Recuperado el 30 de junio de 2022 de

<https://www.hostdime.com.pe/blog/acerca-puertos-tcp-udp-comparacion-similitudes-diferencias/>

Mateu, L. (2004). *¿Qué es un Servidor y Tipos de Servidores?* Recuperado el 30 de junio de 2022 de <https://www.areatecnologia.com/informatica/servidor-y-tipos.html>

Merino y Pérez. (2011). *Definición de Red de Datos.* Recuperado el 05 de julio de 2022 de <https://definicion.de/red-de-datos/>

Napit. (s.f.). *Network Tuning: el rodillo compresor de los problemas de red.* Recuperado el 30 de junio de 2022 de <https://www.napit.com.br/es/network-tuning-el-rodillo-compresor-de-los-problemas-de-red/>

ORACLE COLOMBIA. (2018). Qué es una base de datos. Recuperado el 30 de junio de 2022 de [https://www.oracle.com/co/database/what-is-database/#:~:text=Una%20base%20de%20datos%20es,bases%20de%20datos%20\(DBMS%20\).](https://www.oracle.com/co/database/what-is-database/#:~:text=Una%20base%20de%20datos%20es,bases%20de%20datos%20(DBMS%20).)

Páez, L. (02 de junio de 2021). *Conoce que es una red LAN: la tecnología de conexión más directa y eficaz.* Recuperado el 30 de junio de 2022 de <https://www.crehana.com/blog/desarrollo-web/que-es-red-lan/>

Pardo, F. (s.f.). *Configuración de red.* Recuperado el 30 de junio de 2022 de https://www.academia.edu/6957295/Configuracion_de_red/

Pastar, O. (2022). *Infraestructura de red y cableado: ¿Por qué son tan importantes?* Recuperado el 30 de junio de 2022 de <https://www.universitatcarlemany.com/actualidad/infraestructura-red>

Pérez, A. (07 de junio de 2021). *Tipos de firewall: características y recomendaciones de uso.* Recuperado el 30 de junio de 2022 de <https://www.obsbusiness.school/blog/tipos-de-firewall-caracteristicas-y-recomendaciones-de-uso>

Pino, R. (2010). *Metodología de la Investigación.* (2da edición). Lima: Edit. San Marcos.

QuestionPro. (s.f.). *Tipos de encuesta.* Recuperado el 05 de julio de 2022 de <https://www.questionpro.com/es/tipos-de-encuestas.html>

Raffino, M. (2020). Investigación cualitativa y cuantitativa. Recuperado el 12 de julio de 2022, de <https://concepto.de/investigacion-cualitativa-y-cuantitativa/>

Reimann, R. (2021). *Implementar una red. ¿Qué aspectos se deberían considerar?* Recuperado el 30 de Julio de 2022 de

<http://www.emb.cl/gerencia/articulo.mvc?xid=1659&sec=3#:~:text=Para%20la%20correca%20implementaci%C3%B3n%20de,los%20protocolos%20y%20el%20hardware>

Rodríguez, D. (13 de agosto de 2019). *Entrevista formal: características y preguntas de ejemplo*. Recuperado el 05 de julio de 2022 de <https://www.lifeder.com/entrevista-formal/>.

Rojas, R. (1977). *Guía para realizar investigaciones sociales*. (1era. ed.). México: Edit.PYV.

Rouse, M. (s.f.). *Topología de red*. Recuperado el 30 de junio de 2022 de <https://www.computerweekly.com/es/definicion/Topologia-de-red>

México: Edit. McGraw-Hill.. (2003). Metodología de la Investigación (4ta. ed.).

Taylor S y Bogdan, R. (2000). *Introducción a los métodos cualitativos de investigación*. (3ra. ed.). España: PAIDOS.

UniversitatCarlemany. (08 de junio). *Infraestructura de red y cableado: ¿por qué son tan importantes?* Recuperado el 30 de junio de 2022 de <https://www.universitatcarlemany.com/actualidad/infraestructura-red>

VMware. (s.f.). *Configuración de red*. Recuperado el 30 de junio de 2022 de <https://www.vmware.com/es/topics/glossary/content/network-configuration.html>

Verizon, F. (s/f). *Ancho de Banda*. Recuperado el 30 de junio de 2022 de <https://espanol.verizon.com/info/definitions/bandwidth/>

Zamora, I. (s.f.). *Componentes de una red*. Recuperado el 30 de junio de 2022 de https://www.academia.edu/10437262/Componentes_de_una_red

Zheng, L. (12 de mayo de 2017). *Diseño e implementación de una red LAN para la empresa Palinda*. Recuperado el 30 de junio de 2022 de <https://repositorio.usfq.edu.ec/bitstream/23000/6383/1/130874.pdf>

Znet. (s.f.). *¿Qué es la infraestructura de redes y el cableado estructurado?* Recuperado el 30 de junio de 2022 de <https://www.z-net.com.ar/blog-post/que-es-la-infraestructura-de-redes-y-el-cableado-estructurado/>

ANEXOS

Anexo 1. Formato de entrevista realizada al personal administrativo de la Contraloría del Municipio Antolín del Campo

PERSONAL ADMINISTRATIVO			
Entrevista para la recopilación de información referente al estado de Red LAN de la Contraloría del Municipio Antolín del Campo			Fecha
Realizado por:	Br. David Moro Br. Danyelis Paz Castillo	Modelo	1
Nombre del entrevistado:		Cargo:	
PREGUNTAS			OBSERVACIONES
¿Con qué medios se cuenta dentro de la Contraloría para proporcionar conectividad a los equipos informáticos? ¿Cuál ha sido su experiencia con dichos medios?			
¿Cuáles son las funciones que se llevan a cabo en el departamento al que pertenece?			
¿Cómo es la conectividad dentro del departamento al que pertenece? ¿Todos los equipos tienen acceso al servicio?			
¿Qué impacto genera la conectividad de los equipos en las labores diarias de su departamento?			
¿Qué tipo de fallas de conectividad se presentan en su departamento? ¿Con qué frecuencia ocurren?			
Al existir un flujo de trabajo mayor al habitual dentro de su departamento, ¿cómo se comporta la conectividad de los equipos?			

<p>¿Qué servicios proporcionados por la red son indispensables para el funcionamiento de su departamento? ¿Considera que necesita algún otro servicio?</p>	
<p>¿Cuál es el nivel de confidencialidad de la información que se maneja en su departamento?</p>	
<p>¿Dentro de su departamento existe algún espacio destinado para los equipos de red? ¿Alguna vez se han presentado situaciones de riesgos respecto a dichos equipos?</p>	
<p>¿Alguna vez se han suscitado situaciones de pérdida o robo de información digitalizada dentro de la Contraloría? ¿Cómo han sido manejadas?</p>	
<p>¿Algún equipo informático se ha visto afectado por aplicaciones maliciosas? ¿Con qué frecuencia se presentan este tipo de hechos?</p>	
<p>¿Cómo es el proceso para la solución de las afecciones a la red? ¿Se cuenta en la contraloría con un personal de planta que brinde soporte técnico?</p>	
<p>¿Cómo es el proceso de intercambio de información entre los departamentos de la Contraloría? ¿Qué debilidades cree usted que presenta dicho proceso?</p>	

Anexo 1. Formato de entrevista realizada al personal administrativo de la Contraloría del Municipio Antolín del Campo.

Fuente: Elaboración propia (2022).

Anexo 2. Formato de entrevista realizada al personal de soporte técnico externo de la Contraloría del Municipio Antolín del Campo

PERSONAL DE SOPORTE TÉCNICO EXTERNO			
Encuesta para la recopilación de información referente al estado de Red LAN de la Contraloría del Municipio Antolín del Campo			Fecha
Realizado por:	Bachiller David Moro Bachiller Danyelis Paz Castillo	Modelo	2
Nombre del entrevistado:		Cargo:	
PREGUNTAS			OBSERVACIONES
¿Qué tipo de infraestructura de red (alámbrica, inalámbrica o combinada) se encuentra implementada en la Contraloría actualmente?			
¿Considera que la Contraloría cuenta con los equipos de red necesarios para cumplir con un trabajo eficiente? ¿Por qué?			
Nombre y describa los equipos de red que se encuentran en funcionamiento dentro de la Contraloría			
¿La infraestructura de red implementada en la actualidad satisface las necesidades de transmisión de información de la Contraloría?			
¿Cómo describiría la rapidez y eficiencia del servicio de conectividad a internet que se brinda en la Contraloría?			
¿Cuántos equipos con conectividad a la red posee la Contraloría actualmente? ¿Cómo es la conectividad de los mismos?			
Al existir un flujo de trabajo mayor al habitual dentro de la Contraloría, ¿cómo se comporta la conectividad de los equipos?			
¿Qué tipo de fallas de conectividad se presentan en la contraloría? ¿Con qué frecuencia ocurren?			

¿Cuáles considera usted que podrían ser las razones de las fallas de conectividad de los equipos de la Contraloría?	
¿Cuáles departamentos de la Contraloría consumen más servicios de red? ¿Cómo es el balanceo de cargas de la red?	
¿Se encuentra segmentada la red de la Contraloría? ¿Cómo está segmentada? ¿Existe algún motivo para dicha segmentación?	
¿Cómo es el esquema de seguridad lógica que se maneja actualmente en la red de la Contraloría? ¿Qué departamentos están priorizados?	
¿Qué medidas preventivas se aplican para garantizar la seguridad de la información dentro de la red de la Contraloría?	
¿Alguna vez se ha suscitado situaciones que comprometieron la seguridad de la red y la integridad de la información? ¿Qué medidas correctivas se aplicaron?	
¿Es común que se presenten infecciones por malware en los equipos conectados a la red de la Contraloría?	
¿Qué servicios proporciona la red de la Contraloría? ¿Se aplican algún de restricción o esquema de acceso a dichos servicios?	
¿Cómo están configurados los servidores de la Contraloría? ¿Aparte de los servidores principales, existen servidores de respaldo?	
¿Se encuentra implementada alguna tabla de configuración de red? ¿Cuáles son sus especificaciones?	
¿Cómo es la distribución física de los equipos de red en la contraloría?	
¿En qué condiciones se encuentran los espacios destinados a albergar los equipos de red? (Refrigeración, disposición de equipos, etc.)	

¿Qué medidas se toman para garantizar la seguridad física de los equipos de red de la Contraloría?	
¿Cuál es el estado del cableado de red dentro de la contraloría? ¿Se encuentran debidamente identificados? ¿Con qué frecuencia se revisa la integridad de los mismos?	
¿Con qué protecciones cuenta el cableado de red de la Contraloría?	
¿Cómo se desarrolla el proceso de soporte técnico? ¿Cuánto tiempo toma solucionar las fallas que se presentan comúnmente?	
¿Personal ajeno al área de soporte técnico interactúa con los equipos y cableado de red? ¿Por qué motivos y con qué frecuencia?	

Anexo 2. Formato de entrevista realizada al personal de soporte técnico externo de la Contraloría del Municipio Antolín del Campo.

Fuente: Elaboración propia (2022).

Anexo 3. Vista exterior de la ventana de entrada del cableado coaxial proveniente del *ISP*



Anexo 3. Vista exterior de la ventana de entrada del cable coaxial proveniente del ISP.

Fuente: Elaboración propia (2022).

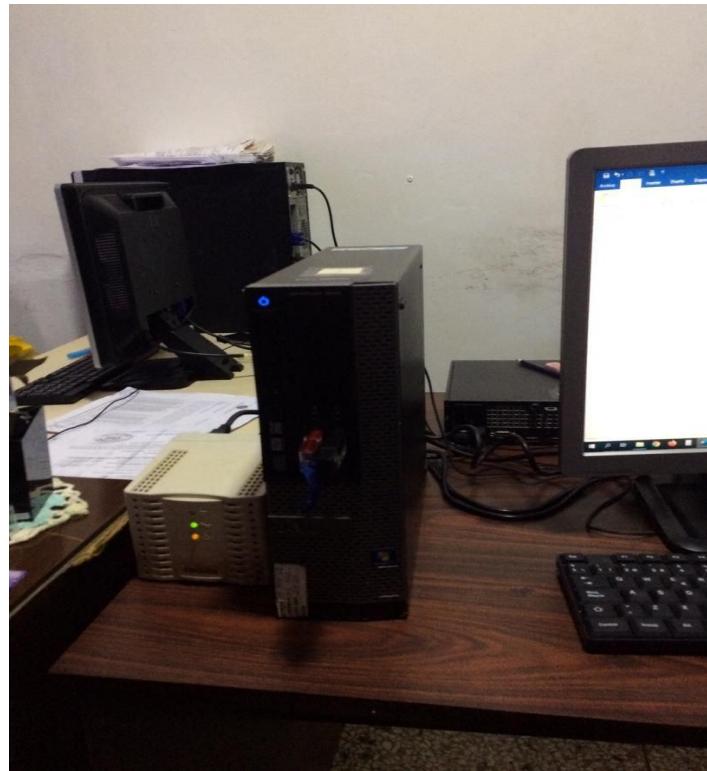
Anexo 4. Vista interior de la planta baja de la sede de la Contraloría del Municipio Antolín del Campo



Anexo 4. Vista interior de la planta baja de la sede de la Contraloría del Municipio Antolín del Campo.

Fuente: Elaboración propia (2022).

Anexo 5. Estaciones de trabajo del personal administrativo de la Contraloría del Municipio Antolín del Campo



Anexo 5. Estaciones de trabajo del personal administrativo de la Contraloría del Municipio Antolín del Campo.

Fuente: Elaboración propia (2022).