UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

PROPUESTA DE ACTUALIZACIÓN DE LA RED INTERNA DEL CENTRO TECNOLÓGICO ARAGÓN

TESIS

Para obtener el título de:

INGENIERO EN COMPUTACIÓN

PRESENTA:

RENÉ ADRIÁN DÁVILA PÉREZ

DIRECTOR:

M. EN C. JESÚS HERNÁNDEZ CABRERA

Ciudad Nezahualcóyotl, Estado de México, 2019

"Toda la naturaleza es un anhelo de servicio; sirve la nube, sirve el aire, sirve el surco. Donde haya un árbol que plantar, plántalo tú; donde haya un error que enmendar, enmiéndalo tú; donde haya un esfuerzo que todos esquiven, acéptalo tú.

Sé el que aparte la estorbosa piedra del camino, sé el que aparte el odio entre los corazones y las dificultades del problema.

Existe la alegría de ser sano y de ser justo; pero hay, sobre todo, la hermosa, la inmensa alegría de servir.

¡Qué triste sería el mundo si todo en él estuviera hecho, si no hubiera rosal que plantar, una empresa que emprender!

Que no te atraigan solamente los trabajos fáciles: ¡Es tan bello hacer lo que otros esquivan!

Pero no caigas en el error de que sólo se hace mérito con los grandes trabajos; hay pequeños servicios que son buenos servicios: Adornar una mesa, ordenar unos libros, peinar a una niña. Aquel que critica, éste es el que destruye, sé tú el que sirve.

El servir no es faena de seres inferiores. Dios, que da el fruto y la luz, sirve. Pudiera llamársele así: el que sirve. Y tiene sus ojos fijos en nuestras manos y nos pregunta cada día: ¿Serviste hoy? ¿Al árbol? ¿A tu amigo? ¿A tu madre?".

El Placer de Servir

Gabriela Mistral

Agradecimientos

Agradezco a la vida por ofrecerme su fuerza durante casi 3 décadas, cada día es un privilegio.

A mis padres Rosa y René, gracias por forjar en mi un camino del cual sigo buscando ser digno al seguir sus pasos, las palabras no me son suficientes para expresar mi gratitud a su paciencia, perseverancia y cariño mostrados ante mis pasos sinuosos durante todos estos años.

A mis hermanos Luis Alberto y Juan Manuel, gracias por su fe en mi camino, me siento contento de seguir aprendiendo cosas importantes de la vida a su lado, no tengo duda que pese a las tormentas llegaremos a buen puerto.

A mi gatita Cinthia, eternas e infinitas gracias por ser un ejemplo hermoso de profesionalismo, pasión y dedicación, es un privilegio ver el hermoso brillo multicolor de tus alas al verte en tu camino exitoso.

A mis tíos Leonardo y Octavio, gracias por su confianza, apoyo y buenos deseos hacia conmigo.

A mi madrina Carmen, gracias por siempre hacerme sentir en mi hogar con el simple hecho de sentir su abrazo sincero, gracias por no tener duda en el camino que he seguido, siempre será una segunda madre para mí.

A mis primos Olga e Ignacio, gracias por su confianza en mis conocimientos y por los grandes momentos que han compartido conmigo desde pequeño, me enseñaron a ser recíproco.

A mi primo Pedro Guillermo, gracias por tu confianza ciega en mi camino, siempre has tenido las palabras adecuadas para impulsar mi espíritu e ir hacia adelante, te di mi palabra y no pienso fallarte.

A mi prima Delia Vanessa, gracias por el cariño que me ofreciste y por exhortarme a que no perdiera la esencia de mi persona jamás, con el tiempo comprendí el significado de tus palabras.

A mi prima Ericka, gracias por todo el apoyo que siempre me has ofrecido sin pedir nada a cambio, tienes un corazón enorme e inmortal.

A mis primas Sandra, Yazmin, Anallely y Nataly, gracias por su cariño, buena voluntad y confianza en lo que realizo.

A mi asesor y profesor M. en C. Jesús Hernández Cabrera, ha sido un gran honor el seguir forjando mi camino profesional con su ejemplo de excelencia, dedicación y buena voluntad, gracias en verdad.

Con mucha dicha puedo expresar que "casi" todo se lo debo a M. en C. Marcelo Pérez Medel, me siento realmente agradecido por la confianza que me ha brindado, por los momentos que comparte con nosotros, y si es Síndrome de Estocolmo decir que una de las mejores etapas de mi vida la viví en su laboratorio, es entonces el mejor padecimiento que haya tenido.

A mi revisor y profesor Ing. Gerardo Torres Rodríguez, gran parte de este trabajo y de mis primeros pasos profesionales, se los debo a sus enseñanzas, agradezco su buena voluntad hacia conmigo, es un gran ejemplo profesional por seguir para mí.

A mi revisor y amigo, M. en C. Felipe de Jesús Gutiérrez López, muchas gracias por enseñarnos a ser profesionales en lo que sea que busquemos emprender, es muy divertido trabajar contigo y aprender de tu vasta experiencia.

A mi revisor, jefe y amigo Ing. Jorge Arturo López Hernández, Yorch muchas gracias por todo lo que compartes con nosotros, desde fomentar elementos profesionales, hasta compartir buenos memes, es una dicha poder colaborarte y poder compartir momentos.

A mi amigo M. en C. Jorge Iván Campos Bravo, muchas gracias por tu generosidad George, eres un ejemplo de cómo afrontar adversidades difíciles sin perder la sonrisa.

A mi amigo Armando, gracias por la confianza, sinceridad y lealtad que has compartido conmigo, gran parte de este trabajo se debe a creer en mí profesionalmente, siempre buscando el crecimiento colectivo.

A mi amigo Ulises, gracias por tu transparencia y lealtad, me siento feliz de poder haber recorrido este camino contigo.

A mi amigo y profesor Alejandro, muchas gracias Alex por siempre incluirme en tus experiencias, proyectos y familia, atesoro los momentos que hemos compartido.

A mis amigos Ariadne y Misael, gracias por siempre tener el deseo de compartir momentos conmigo, tienen un gran corazón, me hace feliz saber que los veré al día siguiente y que aún tendremos muchos años más por delante.

A mis amigas Ximena, Stephannie, y Dialid, muchas gracias por la confianza que depositan en mi, y por su constancia en este camino compartido.

And finally to my international Friends, Charmaine, Mina & Martin, thank you for all your kindness, for the moments we share, you made one of the best months happen in my entirely life, with simple things like a smile, laughs, songs, and pool parties, your friendship it's a treasure to me from now on.

Contenido

1. Introducción. 8

2. Marco Teórico. 10

2.1. Conceptos. 10

2.1.1. Redes de Computadoras. 10

2.1.2. Dispositivos de Red. 14

2.1.3. Topología de Red. 20

2.1.4. Redes Internas y Externas. 22

2.1.5. Redes LAN. 22

2.1.6. Internet. 24

2.1.7. Ancho de Banda. 25

2.1.8. Protocolo de Red. 27

2.1.9. Redes Inalámbricas. 28

2.1.10. VLAN. 29

2.1.11. NAT. 31

2.1.12. Traffic Shaping. 32

2.1.13. Web Filter. 33

2.2. Modelo OSI. 34

2.2.1. Características Generales. 34

2.2.2. Funcionamiento de cada Capa. 35

2.3. Seguridad en Infraestructura de Red. 41

2.3.1. Conceptos básicos y buenas prácticas generales de Seguridad en Red. 42

2.3.2. Políticas de Seguridad. 49

2.3.3. Seguridad en Internet. 51

2.3.4. Firewall. 54

2.3.5. DMZ. 55

3. Red Actual. 58

3.1. Estado actual de la red basado en diseño. 58

3.2. Estado actual de la red basado en funcionamiento. 66

3.3. Estado actual de la red basado en testimonios. 68

4. Necesidades por Área. 71

4.1. Planta Baja. 71

4.2. Primer Piso. ... 72
4.3. Segundo Piso. ... 74
5. Propuesta de Actualización. ... 76
5.1. Actualización de Diseño. ... 77
5.1.1. Topología Actualizada. ... 77
5.1.2. Dispositivos de Red. ... 80
5.1.3. Cableado Estructurado. ... 84
5.2. Actualización de Funcionamiento. ... 88
5.2.1. Red Interna segmentada en VLAN. ... 89
5.2.2. Direccionamiento. ... 91
5.2.3. Configuraciones Iniciales en Dispositivos de Red y Seguridad. ... 96
5.3. Políticas para control de tráfico y seguridad. ... 122
5.3.1. Control de ancho de banda mediante Traffic Shaping. ... 122
5.3.2. Políticas de Seguridad para contenido en Internet. ... 130
5.3.3. Políticas de Seguridad en Servidores. ... 135
6. Consideraciones Económicas y Viabilidad. ... 143
6.1. Justificación de Dispositivos de Red. ... 143
6.2. Justificación de Cableado Estructurado. ... 147
6.3. Justificación de Viabilidad con la Infraestructura Actual. ... 148
6.4. Bases para expansión y actualización. ... 149
7. Conclusiones. ... 152
8. Referencias. ... 154

1. Introducción.

Uno de los preceptos más importantes para la Universidad Nacional Autónoma de México es la formación integral tanto de alumnos como académicos, esa razón impulsa la creación de espacios de desarrollo, buscando abarcar cada campus perteneciente a la Universidad, construyendo espacios dotándolos con la tecnología necesaria para múltiples disciplinas.

En el año 1996, como parte de un proyecto con el BID (Banco Interamericano de Desarrollo), la Facultad de Estudios Superiores Aragón edificó el Centro Tecnológico Aragón, unidad multidisciplinaria para el fomento académico de la comunidad estudiantil, ese lugar tiene como objetivos: poner en práctica conocimientos adquiridos, divulgación científica o profesional, realización de proyectos para instituciones gubernamentales, apoyo a la comunidad estudiantil en su proceso de titulación.

Para satisfacer los objetivos mencionados, el Centro Tecnológico Aragón desde su apertura en 1996, cuenta con infraestructura tecnológica, particularmente sistemas de comunicaciones, destacando infraestructura de Red de Datos para dispositivos electrónicos orientados a la ofimática: computadoras, impresoras, dispositivos móviles; facilitando y agilizando tareas dentro de los laboratorios, auditorios y espacios de desarrollo.

No obstante, el uso de tecnología demanda constantes periodos de actualización, con ventanas de tiempo de al menos 10 años entre cada período. Desde hace aproximadamente 22 años no se han realizado actualizaciones en la infraestructura de Red de Datos, en consecuencia, la infraestructura actual ya presenta un considerable rezago tecnológico, con proyecciones de riesgo e impacto negativo, comprometiendo información de todas las áreas.

Lo anterior, marca la pauta a presentar este trabajo como propuesta de actualización, con la finalidad de fincar bases, para una mejora sustancial en control, manejo y seguridad de la información.

Primero se abordarán conceptos actuales en temas de Redes de Datos, técnicas de control de tráfico, medidas y políticas de seguridad. Presentar modelos de estándares, dispositivos para establecer políticas de seguridad y mejorar el desempeño en el tráfico de la información.

Se presentará el estado actual de la infraestructura de Red de Datos, el modelo de red a nivel lógico, a nivel de topología, los testimonios recopilados de los miembros integrantes de las diferentes áreas y laboratorios, con fines informativos, destacando las áreas de oportunidad a mejorar.

Se expondrán las necesidades por áreas y laboratorios, tomadas de un sondeo realizado dentro de la unidad, señalando posibilidades, impactos y viabilidad de los requerimientos.

Posteriormente entra en materia la propuesta de actualización con base en los temas previos, haciendo énfasis de mejoras en modelo, diseño, topología, dispositivos de red, cableado estructurado, configuraciones, persiguiendo la optimización, mejorando la eficiencia y dotando la seguridad para la información.

Finalmente, se hablará de las consideraciones económicas, la relación costo-beneficio de la propuesta en materia de: adquisición de dispositivos de red necesarios, el impacto de un nuevo cableado estructurado. Cerrando con la mejora continua y escalabilidad para periodos de actualización posteriores.

2. Marco Teórico.

En este capítulo hablaremos de conceptos básicos necesarios en temas de Redes de Computadoras, Modelos, Estándares y Seguridad en Infraestructura de Red. El propósito es sentar la base teórica para abordar los siguientes apartados con información más precisa.

2.1. Conceptos.

Los temas de redes de computadoras son vastos y se pueden clasificar en los siguientes niveles:

- **Físico:** son los incluye cables, dispositivos, espacios físicos, materiales e incluso herramientas para la materialización de un diseño.
- **Modelo**: abarca los diseños, planos y diagramas basados en buenas prácticas.
- **Lógico**: involucra las configuraciones de las tablas de direccionamiento, políticas de rutas, control de tráfico, manejo de direccionamiento externo e interno basado en estándares;
- **Seguridad**: donde se establecen las políticas para el tráfico de información tanto interno como externo; las redes de voz y tecnologías de acceso inalámbrico.

Ahora bien, en el presente trabajo se mencionan principalmente temas para el manejo de la red alámbrica. Y solo se hará breve mención de algunas características elementales en redes inalámbricas.

2.1.1. Redes de Computadoras.

¿Qué es una Red?

Una Red es un conjunto de elementos o dispositivos que se interconectan entre sí para compartir recursos. En la vida cotidiana todo opera bajo modelos de redes,

desde el vasto universo hasta nuestras computadoras. Un ejemplo cotidiano es el transporte público de pasajeros, el cual involucra personas, propósitos, rutas y reglas de transporte; y la finalidad es asegurar que las personas lleguen de un punto a otro. Y este mismo concepto se aplica para las redes de las computadoras que permiten trasladar información de un punto a otro.[1]

Desde la segunda mitad del siglo XX, las computadoras gradualmente se convirtieron en una herramienta de trabajo muy útil para sectores públicos y privados. Se comenzó con un diseño centralizado, dónde un equipo de cómputo por área procesaba las necesidades de la institución, pero con el paso del tiempo ese modelo fue ampliamente superado por las crecientes demandas. No obstante, tanto las computadoras como los dispositivos de comunicación sufrieron una acelerada evolución en sus funciones y capacidades, por ende, en poco tiempo fue posible adoptar nuevos sistemas de comunicación a los que se les llamó **Redes de Computadoras.** Computadoras separadas se comenzaron a interconectar para compartir recursos entre las áreas de la institución y agilizar la productividad a través de un protocolo estandarizado[2].

Una Red de Computadoras, al considerarse un **Sistema de Comunicación**, posee componentes elementales de comunicación: un *transmisor*, un *canal de transmisión* y un *receptor*. Al involucrar computadoras, los componentes incluyen elementos electrónicos físicos, lógicos y humanos en el esquema de comunicación.[3]

- **Transmisor:** se compone de una *fuente* que genera datos y un *transmisor* (dispositivo electrónico) que procesa los datos, codifica y transmite hacia el canal de transmisión.
- **Canal de transmisión:** es el medio físico (infraestructura) donde viajan los datos e información de un punto a otro.

[1] Castelli, M. (2005). LAN Switching first-step. Indianápolis, EE. UU.: Cisco Press. P. 3.
[2] Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson. P.2.
[3] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.2.

- **Receptor:** se compone de un *receptor* (dispositivo electrónico) donde los datos e información se decodifican para que el *destino* (persona) pueda aprovecharlos.

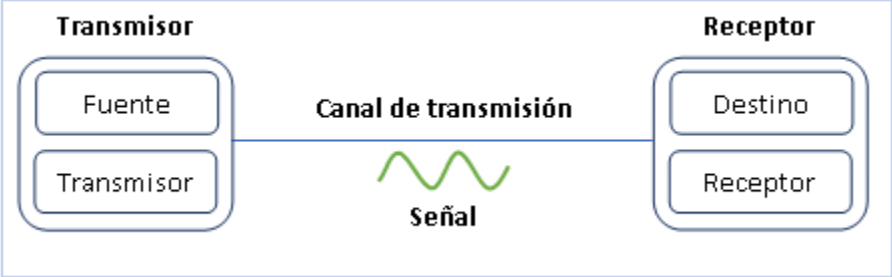


Figura 2.1 Componentes de un sistema de comunicaciones. [B1]

A los transmisores y receptores en una Red de Computadoras se les conoce como **nodos**, mientras que, a los canales de transmisión independientemente de la extensión se les conoce como **enlaces**. Y para establecer una comunicación adecuada es necesario seguir un **protocolo** o conjunto de reglas de comunicación.

Según el alcance de las redes de computadoras, se pueden clasificar en:

- LAN: son redes de alcance local, como las de nuestros hogares y oficinas, de ahí el nombre **L**ocal **A**rea **N**etwork.
- MAN: son redes metro metropolitanas (**M**etropolitan **A**rea **N**etwork)
- WAN: estas redes son amplias (**W**ide **A**rea **N**etwork).

Más adelante veremos que Internet engloba la clasificación de las redes. Ahora bien, las redes de computadoras ofrecen las siguientes características:

Compartir recursos. - Una característica básica en las Redes de Computadoras es la capacidad de compartir recursos, entre ellos: dispositivos físicos (impresoras, computadoras con propósitos específicos, unidades de almacenamiento masivo), información de interés para toda la empresa o institución. Esta característica se presenta de forma óptima siguiendo buenas prácticas al momento de realizar el diseño de la red.

Servicios. - Otra característica importante son servicios en Tecnologías de la Información, presentados en roles de servidor o cliente.

En el rol de servidor se hace uso de computadoras con altas capacidades conocidas como servidores, en ellos se pueden desarrollar e implementar diferentes productos para satisfacer necesidades en tecnologías de la información de lo general a lo particular, dichos productos se conocen como servicios.

En el rol de cliente, se tiene acceso al consumo de servicios en tecnologías de la información, la comunicación entre roles es posible mediante una Red de Computadoras en extensiones locales (LAN-Local Area Network) o remotas (a través de Internet).[4]

Algunas áreas y laboratorios del Centro Tecnológico Aragón cuentan con servidores, donde se alojan páginas web, servicios de correo electrónico, plataformas educativas, sistemas de bases de datos. Así mismo, la mayoría de las áreas y laboratorios consume servicios a través de Internet, esa razón resalta la importancia de la siguiente característica.

- **Estandarización**. – Es el establecimiento de normas a seguir para garantizar un desarrollo y productividad eficientes en materia de comunicación entre dispositivos de las áreas y laboratorios existentes en el Centro Tecnológico Aragón.
- **Flexibilidad**. – La capacidad de adaptar el modelo de comunicación hacia nuevos dispositivos o reubicación de la infraestructura existente.
- **Administración**. – Se refiere al manejo de la infraestructura de red (a niveles de operación y mantenimiento), la cual es una tarea compleja si no se poseen los conocimientos adecuados. Se dejará documentado el modelo de la presente propuesta para disminuir la complejidad de esta tarea hacia cualquier miembro del Laboratorio de Cómputo del Centro Tecnológico Aragón, el cual solo necesitará conocimientos mínimos al respecto.[5]
- **Seguridad**. - Actualmente, en las Redes de Computadoras es necesario contar con políticas de seguridad como característica fundamental, debido a

[4] Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson. P.3.
[5] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.49.

las vulnerabilidades internas o externas, a los ataques perpetrados por terceros, cuya finalidad es extraer información sensible existente en todo el tráfico. La intención de esta característica es blindar lo más posible la información e infraestructura de alguna unidad, en este caso el Centro Tecnológico Aragón.

2.1.2. Dispositivos de Red.

Para solventar las características previamente mencionadas se necesitan dispositivos electrónicos de red, algunos con funcionalidades de comunicación y otros con políticas de seguridad útiles. La presente propuesta adoptará los siguientes elementos:

Cable de Par Trenzado. – Podemos encontrar diferentes tipos y categorías en estos cables, dependiendo el contexto de uso es el tipo de cable que se elige. Para efectos de la presente propuesta, se mencionará en tipo el *Cable de Par Trenzado Sin Blindaje (UTP – Unshielded Twisted Pair)* en *Categoría 6*. Este cable de par trenzado está constituido por 4 pares conductores (hilos de cobre por lo general), el diseño ofrece resistencia mecánica, entonces la señal viaja a través del cable sin verse afectada por señales externas no deseadas, la siguiente figura muestra el diseño del cable.[6]

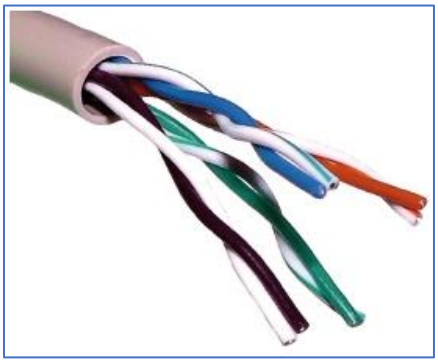


Figura 2.2 Cable de Par Trenzado Sin Blindaje (UTP). [B2]

[6] Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 35.

Los cables de par trenzado son de fácil fabricación, haciendo que el precio sea reducido. Sin embargo, las largas distancias representan una considerable desventaja al momento de realizar transmisiones, el estándar EIA *(Electronic Industries Alliance)* recomienda tener la consideración de una distancia máxima de 90m entre nodos para garantizar la transmisión y comunicación, si se supera esa distancia el cable merma en sus capacidades conductoras, volviéndose una resistencia, disminuyendo considerablemente la señal de transmisión.

En los cables de par trenzado han existido diferentes categorías desde su creación, la siguiente tabla muestra las características en cada categoría.

Nombre	Ancho de banda	Velocidad	Aplicaciones	Observaciones
Nivel 1	0.4 MHz		Líneas de teléfono y de módem.	No válido para sistemas modernos.
Nivel 2	4 MHz	4 Mbits/s	Terminales informáticos antiguos	No válido para sistemas modernos
Cat 3	16 MHz	10 Mbits/s	10Base-T y 100Baset- T4 Ethernet.	No válido para velocidades superiores a 16 Mbits/s. Hoy en día se usa principalmente en cables telefónicos.
Cat4	20 MHz	16 Mbits/s	Redes Token Ring de 16 Mbits/s.	No se emplea habitualmente
Cat5	100 MHz	1 Gbit/s	100Base-TX y 1000Base-T Ethernet	El más común hoy en día en la mayor parte de redes locales.
Cat5e	100 Mhz	10 Gbit/s	100Base-TX y 1000Base-T Ethernet	Categoría 5 mejorada.
Cat6	250 MHz	10 Gbit/s	10GBase-T Ethernet.	
Cat6a	500 MHz	10 Gbit/s	10GBase-T Ethernet.	
Clase F	600 MHz	10 Gbit/s	Teléfono, CCTV, 1000Base-TX en el mismo cable, 10GBaseT Ethernet.	Cable SFTP de cuatro pares.
Clase Fa	1000 MHz	100 Gbit/s	Teléfono, televisión por cable, 1000Base-TX en el mismo cable. 10base-T Ethenet.	Cable SFTP de cuatro pares.

Tabla 2.1 Categorías de cable de par trenzado. [TB1]

Las categorías 3 y 4 se han visto superadas por las velocidades de transmisión actuales, la categoría 5 es la más común actualmente, especialmente en entornos domésticos donde pocos nodos se ven involucrados, no obstante, en un entorno como el Centro Tecnológico Aragón la extensión de nodos demanda altas velocidades.

Se elige la categoría 6 porque ofrece una velocidad de transmisión de hasta *10 Gbit/s*, nos da la certeza de establecer transmisiones de calidad entre los nodos con un bajo impacto económico, haciendo viable la relación costo beneficio, en el capítulo 6 se mencionarán todos los efectos de esta elección.

Al ser de bajo costo hace muy factible su adquisición, se considera sin blindaje ya que se usará para el interior de las instalaciones del Centro Tecnológico Aragón.

Switch. – Conocidos como **puentes** en países de habla hispana, es un dispositivo de red (utilizado en el segundo nivel del modelo de referencia OSI) cuya característica principal es segmentar una red local de formas principalmente física (cableado y dispositivos) y lógica (mediante VLANs) en caso que el dispositivo lo permita, esto último es debido a la existencia de tipos de switch administrable (con puertos e interfaz de configuración) y no administrable (plug & play).[7] Es útil también para la diferenciación entre redes de datos y voz, o para la creación de Redes Virtuales de Área Local (VLAN) de las cuales se hará mención más adelante. Veamos gráficamente los tipos de switch existentes:

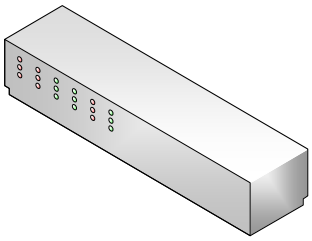


Imagen 2.1 Representación gráfica de un Switch. [A1]

Figura 2.3 Switch de tipo administrable. [B3]

[7] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.47.

Figura 2.4 Switch de tipo Plug & Play. [B4]

Router. – Conocido como **encaminador** en países de habla hispana, es un dispositivo de red (utilizado en el tercer nivel del modelo de referencia OSI) cuya característica principal es seleccionar la ruta óptima para hacer llegar los paquetes de información de un dispositivo a otro.[8] De forma similar a un switch, el router también segmenta redes en **subredes,** pero estableciendo rutas de comunicación entre las subredes mediante direccionamiento. Otra característica importante de un router es la interconexión de diferentes Redes de Área Local en diferentes protocolos de comunicación. Respecto a los tipos de routers existen los de interfaces exclusivamente alámbricos y los que incluyen interfaz inalámbrica en el ámbito físico, en el ámbito lógico depende de las características que desea incluir cada fabricante, entre más características ofrezca mayor es el costo del dispositivo. Las siguientes figuras muestran los diferentes tipos de router:

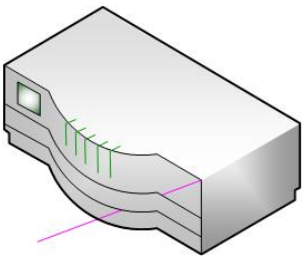


Imagen 2.2 Representación gráfica de un Router. [A2]

[8] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.48.

Figura 2.5 Router de tipo alámbrico con características especiales. [B5]

Figura 2.6 Router de tipo inalámbrico. [B6]

Access Point. – Conocidos como **puntos de acceso** o **antenas** en países de habla hispana, es un dispositivo de red (ubicado también en el tercer nivel del modelo de referencia OSI) cuya función principal es manejar el control de acceso inalámbrico de usuarios hacia redes locales alámbricas, o hacia redes con salida a internet.[9] La diferencia entre los tipos de Access Point radica en la distancia a cubrir, mientras más larga sea mayor intensidad de ondas de radiofrecuencia, los de menor intensidad comúnmente se instalan en pequeños espacios cerrados, y los de mayor intensidad se usan para exteriores. Las siguientes ilustraciones muestran el Access Point:

[9] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.48.

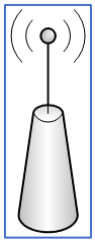


Imagen 2.3 Representación gráfica de un Access Point. [A3]

Figura 2.7 Access Point de alta intensidad. [B7]

Firewall. – Conocidos como **cortafuegos** en países de habla hispana, éste dispositivo parte del concepto de seguridad perimetral, estableciendo "muros" alrededor de una infraestructura de red, dónde todo el tráfico de información viaja por una vía "vigilada" mediante el manejo de protocolos y políticas de seguridad, estableciendo reglas para la entrada/salida de la información, tanto del exterior (Internet) hacia el interior (Redes LAN) y viceversa.[10] Hay variedad de tipos de Firewalls, algunos de ellos solo permiten establecer políticas de seguridad para redes internas, o políticas de comunicación para servidores; otros comparten características de un router, pero mejorando dichas características por las políticas de seguridad a establecer para enrutamiento. Y al igual que un router, mientras más características ofrezca el dispositivo, más elevado es el costo. Conozcamos como lucen gráficamente:

[10] ISACA. (2015). Manual de Preparación para el Examen CISA. EE. UU.: ISACA. P.396.

Imagen 2.4 Representación gráfica de un Firewall. [A4]

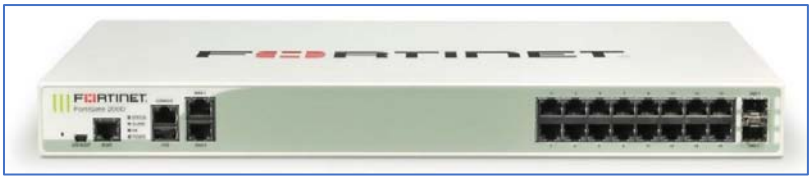


Figura 2.8 Firewall Fortinet. [B8]

2.1.3. Topología de Red.

Dentro de una infraestructura de red, los dispositivos finales (computadoras, impresoras, servidores), conocidos también como nodos, se comunican mediante enlaces físicos (cables, dispositivos de red, presentados previamente) formando un esquema geométrico el cuál de forma técnica se le conoce como **Topología**[11]. Una topología define la estructura de interconexión de la red, por lo que la forma de la estructura es variada, dependiendo principalmente del espacio físico (edificio o unidad) donde se va a implementar el diseño topológico.

Existen varios tipos de topologías, destacándose las siguientes:

- **Lineal** o **bus:** se hace la conexión de nodos con un cable corto que va del dispositivo hacia una línea troncal, la cual está delimitada por terminales en sus extremos.
- **Anillo:** cada nodo cuenta con un enlace al siguiente nodo y al anterior, creando una forma circular, entonces cada nodo funciona como repetidor para la transmisión de la información.
- **Malla:** en esta topología cada nodo se conecta con otros y una variante es la de tipo **malla completa**, donde cada nodo se conecta con los demás

[11] Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 22.

estableciendo una comunicación entre todos los nodos. La información viaja de un punto a otro a través de diferentes rutas.

En estos primeros tipos la comunicación se establece de forma directa entre los nodos, no intervienen otros dispositivos. Ahora veamos topologías en donde intervienen otros dispositivos:

- **Estrella**, los enlaces de transmisión de todos los nodos están conectados entre sí mediante un dispositivo de red como un switch o router, de forma centralizada.

Ahora bien, la presente propuesta tiene la intención de adoptar la siguiente topología, ya que su jerarquía ofrece características de estandarización, permitiendo una mejor organización al momento de diseñar un modelo de red y una gran escalabilidad.

- **Árbol**, esta estructura posee jerarquía[12], en la que los nodos se conectan a dispositivos de red dentro de su área, a su vez esos dispositivos de red se conectan a otros dispositivos de red los cuales se encuentran alojados en un espacio dedicado conocido técnicamente como **SITE**, la representación gráfica tiene la siguiente forma:

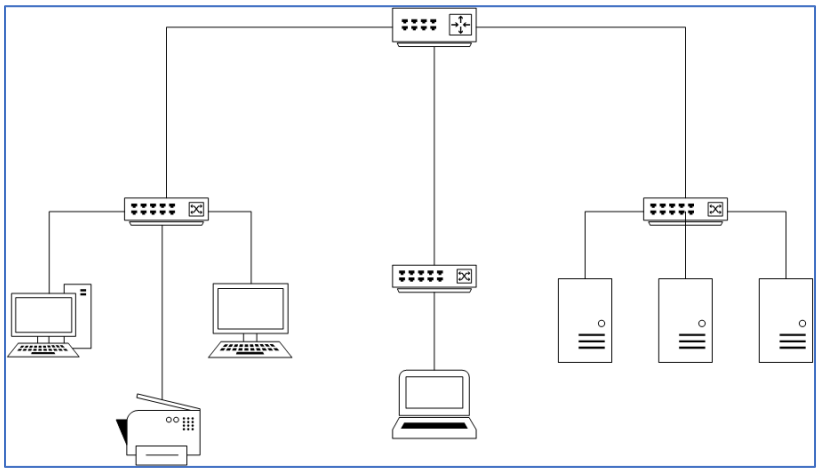


Imagen 2.5 Topología de Tipo Árbol. [A5]

[12] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.56.

2.1.4. Redes Internas y Externas.

Una Red de Computadoras posee extensión, partiendo desde un área de trabajo (cuarto, departamento), pasando por un área más amplia (casa, edificio), estableciendo comunicación con otros edificios dentro de un mismo complejo (escuela, edificios contiguos), hasta conectar con otras partes del mundo. La importancia de mencionar la extensión de una red es para tener identificadas las características entre los tipos de red.

Una **red interna** posee una extensión topológica al interior de algún edificio, donde la comunicación existe solamente entre los nodos pertenecientes a la unidad. En contraparte, una **red externa** posee una extensión que va desde una ciudad, a todo el país, hasta establecer comunicación con varias partes del mundo, donde las redes internas se comunican entre sí. Pasemos a revisar redes LAN las cuales son de carácter interno e Internet la cual tiene características de una red externa.

2.1.5. Redes LAN.

Sus siglas en inglés significan **Local Area Network** (Red de Área Local en países de habla hispana), son un tipo de red interna de propiedad privada operando al interior de algún edificio, oficina u hogar, con amplia popularidad debido a ser de fácil diseño, instalación y operabilidad[13]. Es importante tener presente que **Internet no** es una red de este tipo. Las **LAN** caracterizan por los siguientes aspectos:

<u>Características Generales</u>

- La extensión es **limitada**, al instalarse dentro de una sola unidad se conoce sus límites. Permitiendo conocer la cantidad de nodos operantes dentro de la extensión.
- Son redes **privadas**, solamente el personal perteneciente a la unidad tiene acceso a la red.

[13] Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson. P.17.

- Su topología comúnmente es **jerárquica** (tipo árbol en la mayoría de los casos).
- Los **medios de transmisión físicos** son los mismos dentro de toda la red, ya sea si es mediante cable o de forma inalámbrica. Facilitando la **identificación** de problemas de red.
- Hace uso de tecnología de difusión **broadcast** mediante un Switch.
- Permite la **interconexión** entre varias LAN mediante un router.
- La **transmisión** de datos interna suele ser elevada, con un nivel de consumo estable, dependiendo las interfaces y dispositivos que se utilicen (Mbps/Gbps) en la infraestructura.
- El **mantenimiento** preventivo y correctivo se puede realizar sin alterar drásticamente la estructura de la red en tiempos relativamente bajos.
- Es posible realizar **expansión** de nodos, mediante los dispositivos de red existentes o si se añaden nuevos dispositivos.
- Es posible **segmentar** la red LAN mediante el uso de **VLAN** (Virtual LAN, se mencionarán más adelante).

Elementos de la LAN

Es necesario conocer los principales componentes participantes al momento de diseñar este tipo de red[14], los cuáles son:

- **Medios de transmisión**, medios físicos como los cables u ondas si se trata de medios inalámbricos.
- **Dispositivos de conexión**, los dispositivos de red como Switch, Router o Access Point.
- **Computadoras (Nodos)**, la herramienta de trabajo de cada usuario de la red.
- **Interfaz de red**, para conectar un medio de transmisión, forma parte de la computadora de cada usuario.

[14] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.43.

- **Periféricos**, los elementos en la red que se consideran recursos compartidos, como impresoras, terminales, servidores.

2.1.6. Internet.

Se le considera como la "red de redes" ya que es una colección de distintas redes utilizando protocolos en común o diferentes, donde se ofrecen diferentes tipos de servicios. Esta red se concibió sin planearse, tiene una compleja operación, se dice que no se tiene control sobre la misma.[15]

Veamos la operación de Internet con el siguiente diagrama:

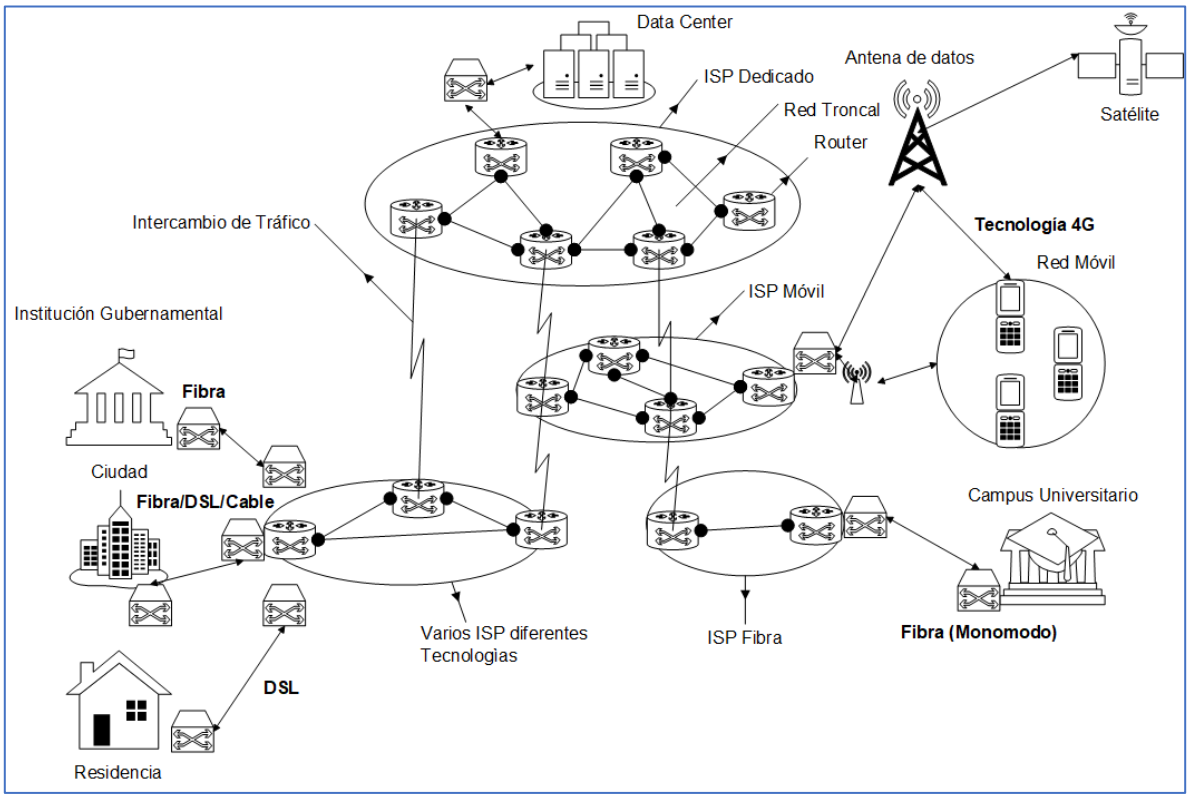


Imagen 2.6 Funcionamiento de Internet. [A6]

El diagrama muestra distintas redes operando en conjunto mediante enlaces de **Intercambio de Tráfico**, en la parte superior encontramos un **Data Center** (Centro de Datos) el cual ofrece distintos tipos de servicios, como servicios podemos considerar desde *Google* o redes sociales como *Facebook*, incluso servicios

[15] Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson. P.46.

multimedia como *Netflix*, los cuales cuentan con un **ISP** (Proveedor de Servicios de Internet) dedicado, esto es cuentan con enlaces **troncales** exclusivos donde su información corporativa se mantiene aislada de otras redes.

Del lado derecho vemos una **Red Móvil**, esta red hace uso de señales de ondas de radio originadas desde un satélite en el espacio, la cual mediante antenas llega a la infraestructura de un ISP, mediante enlaces de intercambio de tráfico es como se puede establecer comunicación con otras redes.

En la parte inferior encontramos infraestructuras de distintos tipos de ISP, cada ISP ofrece diferentes tecnologías de conectividad, entonces existe una amplia gama de posibilidades, donde la relación costo-beneficio es variable de acuerdo con el tipo de tecnología a adquirir.

Entonces la conectividad entre distintos puntos como de una ciudad a una universidad es posible mediante las infraestructuras de los ISP y los intercambios de tráfico entre las infraestructuras, a través de **dispositivos de red** y **rutas de información**.

2.1.7. Ancho de Banda.

Previamente se dijo que una Red de Computadoras es un **Sistema de Comunicación**, el cual posee un canal de transmisión. En dicho canal la información viaja en forma de ondas analógicas[16] (ya sea de radiofrecuencia, eléctricas o de luz) con determinada frecuencia o bien un rango de distintas frecuencias, esas ondas mediante procesos de discretización (conversión analógica a digital[17]) manejan la información en bits (0 o 1 del sistema binario), de un punto a otro por el canal de transmisión, en la onda los datos se transmiten mediante **modulación** (potencia de la señal representada en binario).[18] Para comprender

[16] Onda continua la cual entre dos valores cualesquiera se pueden tomar un valor o un conjunto de valores intermedios con tendencia al infinito.
[17] Proceso de codificación en ceros y unos, donde a una señal analógica se le toman sus valores en intervalos regulares, formando números enteros los cuales después se codifican en binario.
[18] Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 15.

mejor los conceptos de ondas, las siguientes figuras muestran los tipos de onda analógica y digital, además de una representación de conversión analógica a digital:

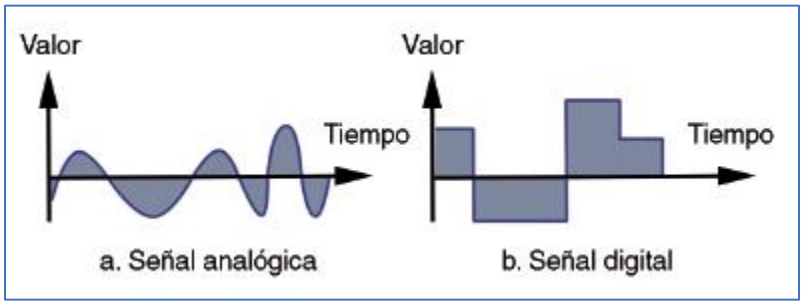


Figura 2.9. Tipos de señal. [B9]

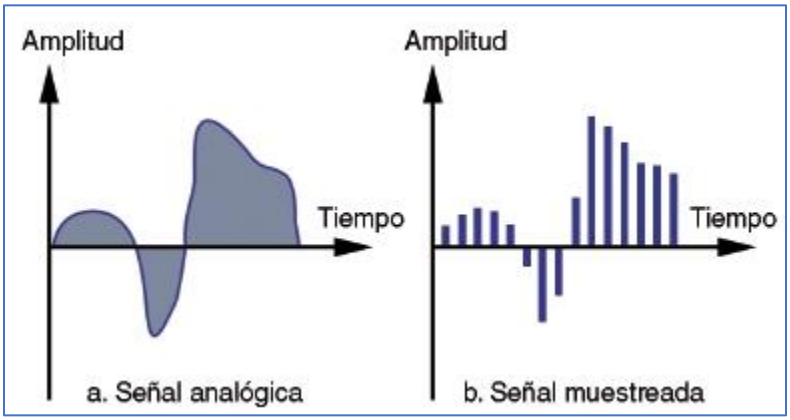


Figura 2.10. Señal analógica discretizada. [B10]

El **ancho de banda** es la capacidad de un canal de comunicaciones para la transmisión de ondas portadoras de datos[19], si el canal de comunicaciones posee mayor frecuencia, mayor será el ancho de banda.

Se utilizan dos unidades de medida para medir el ancho de banda, la tasa de *baudios* y la tasa de *bits*, los cuales no representan lo mismo. El *baudio* es el número de cambios de la señal por segundo dentro del circuito del canal de comunicación. Por otra parte, la tasa de *bits* depende de la intensidad en la modulación la cual se utiliza para incrustar los datos dentro de la onda portadora.[20] Veamos la siguiente figura:

[19] Señal donde la información viaja en formas de onda analógica y digital.
[20] Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 16.

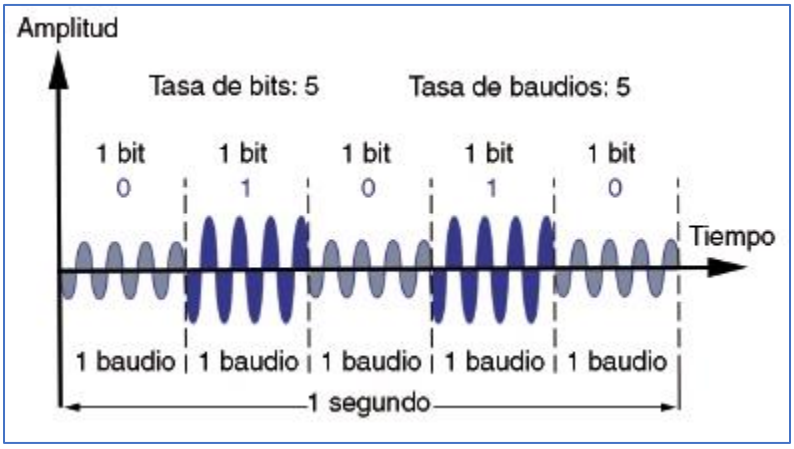


Figura 2.11. Tasa de bits y baudios. [B11]

El término *bps* (bits/baudios per second) hace referencia a la cantidad de baudios y bits transportados en la onda portadora a una cierta intensidad (amplitud) en un determinado tiempo. Los bits son la información codificada los cuales son definidos por los baudios dentro de la onda portadora.

Por lo tanto, mientras exista mayor modulación (potencia en la señal), la tasa de bits realizará más rápido la tarea de colocar los datos dentro de la onda en el canal de comunicación.

2.1.8. Protocolo de Red.

La comunicación en dispositivos informáticos es transmitida en binario o *bits*, sin embargo, no es suficiente que solo se envíen grupos de bits en canales de comunicación. Para establecer comunicación entre los elementos de una red, de manera eficaz se deben establecer un conjunto de reglas, a las cuales nombramos **Protocolo**.[21]

Un protocolo desempeña un rol análogo al idioma manejado entre dos personas en una conversación, si una persona habla español y la otra habla inglés, la comunicación entre ellas no podrá establecerse adecuadamente en primera instancia. Aquí es donde se establecen las reglas para utilizar un idioma en común.

[21] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.104.

El protocolo define lo que se va a comunicar, la manera en que se va a realizar la comunicación y el momento en que se va a realizar la comunicación a través de sus elementos de **sintaxis**, **semántica** y **temporalización**.[22]

Sintaxis define el formato de los datos dentro de la comunicación en una red, especificando la estructura ordenada en que la información es transmitida, para que los dispositivos de comunicación codifiquen tramas de datos[23] siguiendo la estructura. La **Semántica** hace referencia a cada conjunto de bits transmitidos. Y la **Temporalización** determina el momento y velocidad en que los datos deben transmitirse.

2.1.9. Redes Inalámbricas.

También conocidas como **Redes Wi-Fi**[24] se basan en los protocolos establecidos por el estándar **IEEE 802.11**. La transmisión de información se efectúa mediante ondas de radiofrecuencia, se puede hacer uso de los **Access Point** para efectuar la conectividad de los dispositivos, para que un dispositivo logre asociarse a una red Wi-Fi se requieren los siguientes elementos:

- **SSID:** Siglas que significan Identificador de conjunto de servicios, es un nombre que se le da a la red Wi-Fi.
- **Algoritmo de Seguridad:** Clave (conjunto de caracteres) cifrada para asociar a algún cliente con el punto de acceso inalámbrico.
- **Canal de radio:** es el medio donde se comparte la información.

Estas redes operan de 2 formas distintas:

Infraestructura, donde los dispositivos y su tráfico están coordinados mediante un conjunto de Router-Access Point, logrando establecer la comunicación entre dispositivos inalámbricos y alámbricos. El siguiente esquema representa esta forma de operación:

[22] Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 20.
[23] Conjuntos de 8 bits.
[24] Termino comercial el cual **no** representa un acrónimo o siglas.

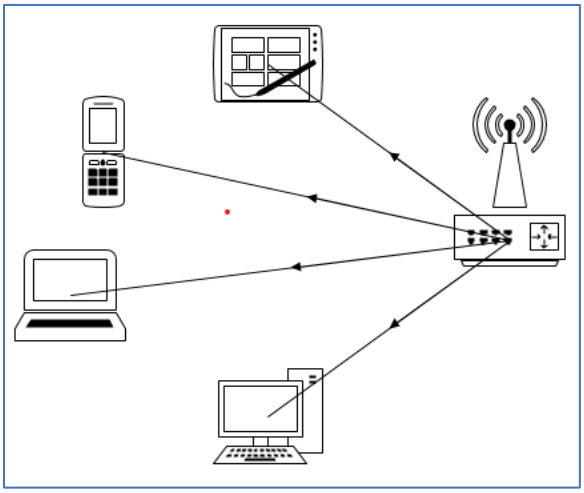


Imagen 2.7. Wi-Fi de Infraestructura. [A7]

Ad-hoc, no existen intermediarios para establecer la comunicación entre dispositivos, sin embargo, todos los dispositivos deben tener interfaz de red inalámbrica. El siguiente esquema representa esta forma de operación:[25]

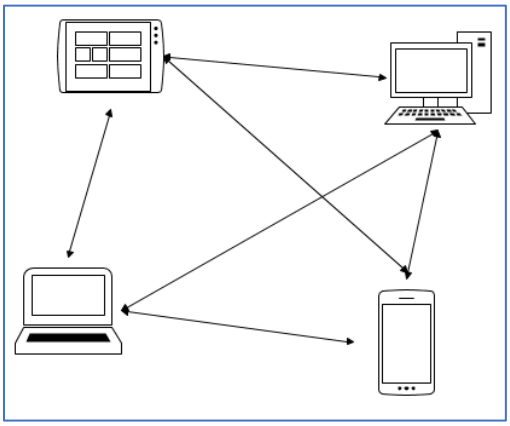


Imagen 2.8. Red Ad-hoc. [A8]

2.1.10. VLAN.

En una **LAN** el grupo de computadoras y dispositivos pertenecientes, distribuyen su información de un dispositivo a otro, mediante un **dominio de difusión** el cual

[25] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.63.

recibe todo el tráfico generado por los dispositivos miembros de la LAN, sin embargo, existen las siguientes limitantes en este tipo de redes:

- Cuando la densidad de dispositivos incrementa, el **dominio de difusión** pierde eficiencia debido a que gran parte del tráfico generado es innecesario.
- Cuando los dispositivos necesitan estar en espacios físicos diferentes, pero sin dejar de ser parte de la misma red local.

Esas limitantes logran resolverse haciendo uso de **VLAN** (Virtual LAN), este tipo de redes se configuran haciendo uso del dispositivo de red **Switch** de tipo administrable.

En una **VLAN** se establecen etiquetas las cuales separan la **LAN** de forma lógica en **dominios de difusión** más pequeños, cada VLAN tiene su propio dominio de difusión, ocasionando que el tráfico generado se reduzca y viaje únicamente en la VLAN a la que pertenece.[26]

Otra característica del etiquetado es diferenciar las Redes Locales dentro del mismo espacio físico, esto es que dispositivos colocados en el mismo espacio físico están separados en diferentes dominios lógicos (configuración) de red local. Entonces existe flexibilidad cuando la red exista tanto en el mismo espacio físico como en espacios físicos diferentes, la separación entre espacios físicos diferentes es posible mediante los **enlaces troncales** (enlaces donde viaja la información de varias VLAN). Los siguientes diagramas muestran diferencias físicas y lógicas entre una LAN y una infraestructura con VLAN:

[26] Fortinet, Inc. (2015). FortiOS Handbook System Administration. Canada: Fortinet Publications. P. 205.

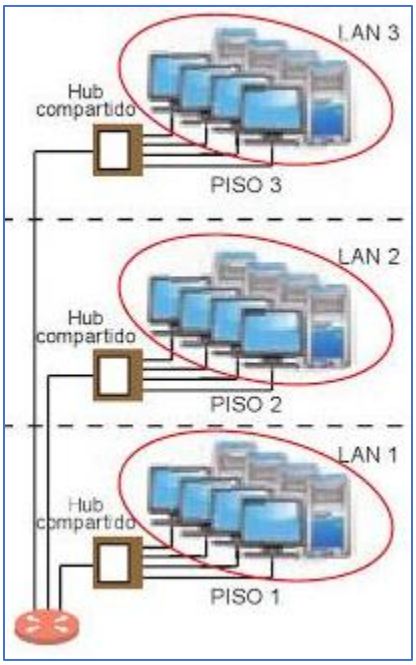


Figura 2.12. Segmentación con LAN [B12]

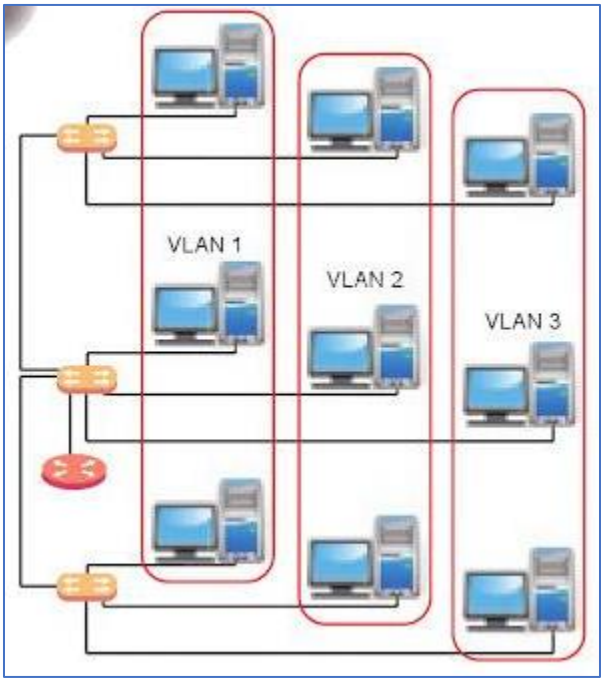


Figura 2.13. Segmentación con VLAN [B13]

En la segmentación LAN, vemos que los dispositivos están conectados entre sí mediante un dispositivo Switch, dentro del mismo espacio físico. Por otra parte, en la segmentación con VLAN, los dispositivos están conectados en espacios físicos diferentes perteneciendo al mismo dominio de red local.[27]

2.1.11. NAT.

En una **LAN** es común manejar un direccionamiento IP privado para el tráfico local, mientras que en un acceso común a internet se ocupan direcciones IP públicas.

En ocasiones es necesario que un direccionamiento privado pueda tener acceso a una red externa como internet, no obstante, se necesita contar con una dirección IP pública, en esta situación es donde se utiliza el concepto de **NAT** (Network Address

[27] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.212.

Translation – Traducción de Direcciones de Red), mecanismo que posibilita a un direccionamiento privado tener acceso a una red externa con una IP Pública.[28]

Para lograr esto es necesario contar con un dispositivo de red de capa 3 como un **Router** o un **Firewall**, el cual se encarga de realizar la traducción de forma bidireccional (solicitudes de entrada y salida). Su mecanismo de funcionamiento es de la siguiente manera: cuando se desea una solicitud hacia el interior de una red privada, la IP que origina la solicitud es de carácter pública o externa, el dispositivo de capa 3 intercepta la solicitud y sustituye la IP Pública por una IP Privada, para ello es necesario que el dispositivo cuente con las IP Privada y Pública previamente definidas en su configuración. El siguiente esquema muestra de forma general el funcionamiento:

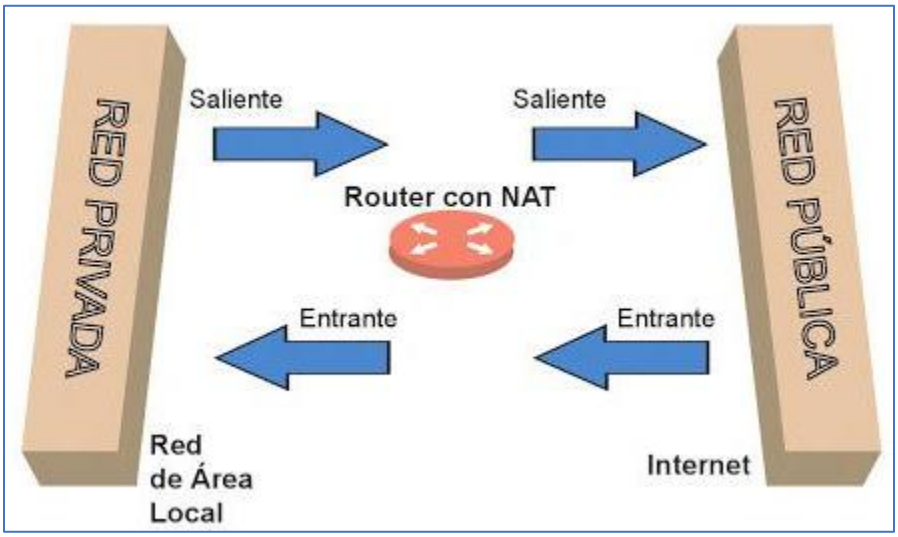


Figura 2.14. NAT en un Router. [B14]

2.1.12. Traffic Shaping.

En una red existe tráfico el cual viaja internamente en una red privada, o hacia el exterior mediante redes externas como internet, dicho tráfico viaja con cierta intensidad mediante el ancho de banda definido en sus dispositivos. No obstante, en ocasiones algunos dispositivos no requieren manejar el mismo nivel de tráfico y

[28] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.220

por ende el mismo ancho de banda disponible dentro de la infraestructura, en estos casos es dónde se puede utilizar la técnica de **Traffic Shaping** (Moldeado de Tráfico). Esta técnica consiste en definir políticas de manejo de ancho de banda para ciertos segmentos de direccionamiento, ofreciendo control en el tráfico de información dentro de la red.

En dispositivos de capa 3 como un **Router** o un **Firewall**, es posible implementar esa técnica mediante políticas dentro de la configuración del dispositivo, permitiendo flexibilidad a varios niveles dentro de la infraestructura, y con ello ajustar la cantidad de tráfico saliente para ciertos rangos de direccionamiento.[29] Posteriormente durante la propuesta se mencionará como realizar esta configuración dentro de un Firewall. La siguiente figura es una representación general de esa técnica.

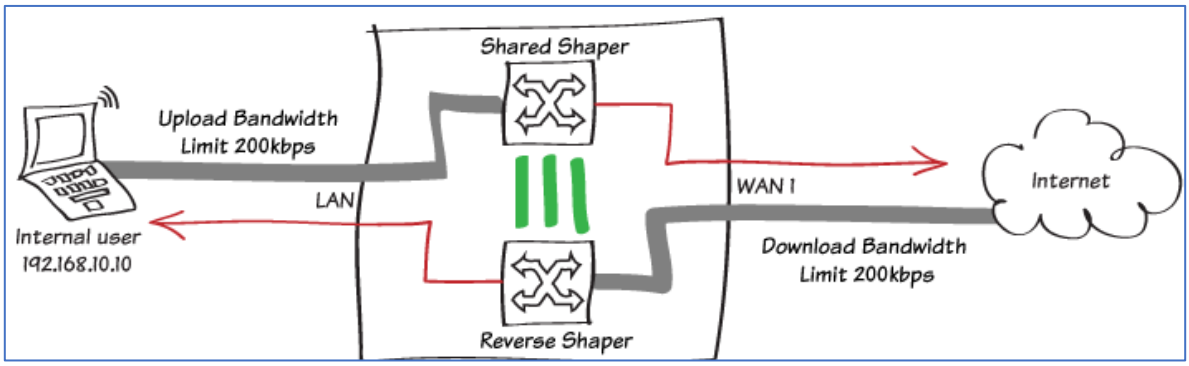


Figura 2.15. Traffic Shaping. [B15]

2.1.13. Web Filter.

Al contratar un servicio de Internet, es común que se tenga acceso a cualquier tipo de contenido o servicio existente, en un entorno privado es posible tener bajos índices de riesgo, si se cuenta con software necesario (Antivirus) o configuraciones de seguridad adecuadas. Sin embargo, en un entorno organizacional el impacto puede ser considerable, desde altos niveles de tráfico, hasta posibles puertas de entrada de atacantes.

[29] Fortinet, Inc. (2018). FortiOS 6.0. agosto 28, 2018, de Fortinet, Inc. Sitio web: http://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortiOS-HTML5-v2/Home.htm

Para mitigar en medida de lo posible esos riesgos, puede utilizarse una herramienta llamada **Web Filter** (Filtro de contenido Web)[30], presente en la mayoría de los dispositivos Firewall que cuenten con esa característica dentro de su licencia de uso. El cual establece **políticas de acceso** a los contenidos en la web, facilitando colocar restricciones a ciertos tipos de contenido. Posteriormente durante la propuesta se mencionarán algunas buenas prácticas de restricción de contenidos web.

2.2. Modelo OSI.

En los puntos anteriores, hemos visto elementos para diseñar arquitecturas de red, cada elemento cuenta con interfaces físicas (conectores o cables) e interfaces lógicas (configuración de los dispositivos). También se revisaron algunos esquemas de conexión de redes, como Internet, ahora bien, para realizar conexiones (ya sea a nivel local o a grandes distancias) es necesario seguir buenas prácticas, definidas en estándares internacionales con el fin de garantizar una arquitectura funcional y organizada, tomando en cuenta lo anterior, la presente propuesta adoptará los principios del **Modelo OSI**.

2.2.1. Características Generales.

El **Modelo OSI** (Open Systems Interconnection – Interconexión de Sistemas Abiertos) es un modelo de referencia, el cual funge como guía al momento de diseñar una arquitectura de red[31], ya que indica mediante una jerarquía de capas lo que la arquitectura de red debe realizar.

Este modelo fue desarrollado por la Organización Internacional de Normas (ISO – International Standards Organization), con el fin de establecer estándares entre los diversos protocolos existentes en el mercado. Está constituido en una jerarquía de

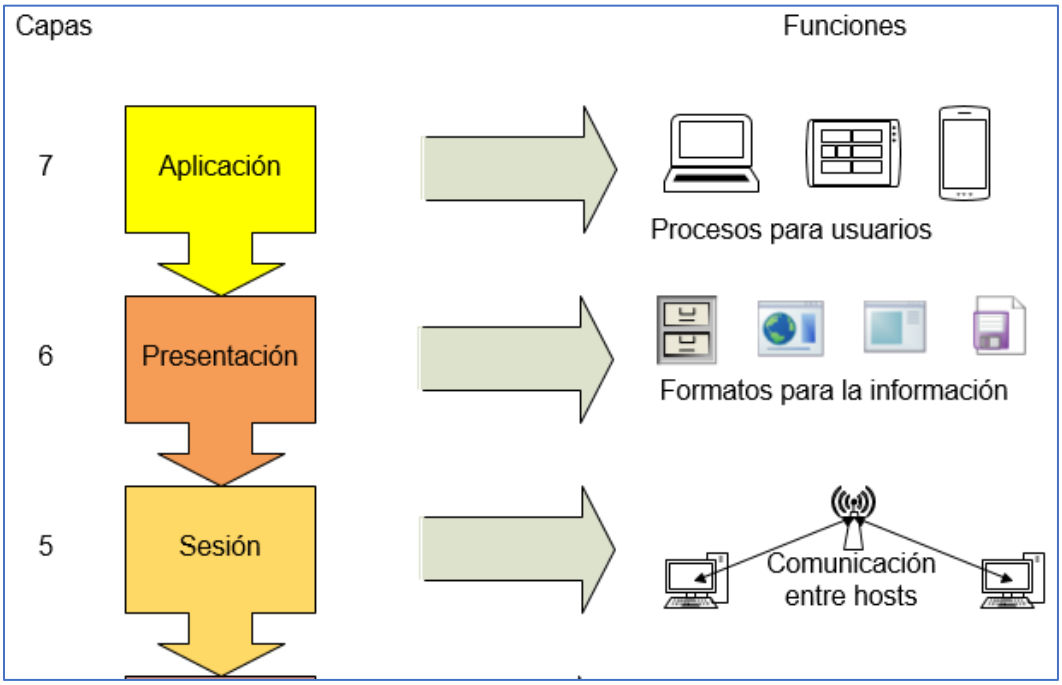
[30] Fortinet, Inc. (2018). FortiOS 6.0. agosto 28, 2018, de Fortinet, Inc. Sitio web: http://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortiOS-HTML5-v2/Home.htm
[31] No es una arquitectura de red, solo indica los pasos a realizar al momento de diseñar una arquitectura de red.

7 capas, mismas que deben seguir los siguientes principios, o también consideradas sus buenas prácticas[32]:

- Las capas deben tener diferentes niveles de abstracción.
- En cada capa existen funciones definidas.
- Las funciones en las capas se eligen teniendo en cuenta los protocolos estandarizados internacionalmente.
- Se requiere definir límites en las capas para la reducción del flujo de información en las interfaces físicas y lógicas.
- Se definen 7 capas para evitar funciones distintas a las establecidas en cada una, evitando que la arquitectura a diseñar se vuelva difícil de manejar.

2.2.2. Funcionamiento de cada Capa.

Previamente se hizo mención de 7 capas existentes en el Modelo de referencia **OSI**, éstas son: *Física, Enlace de Datos, Red, Transporte, Sesión, Presentación, y Aplicación*. La siguiente imagen muestra la jerarquía de capas y la función de cada capa:



[32] Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson. P.36.

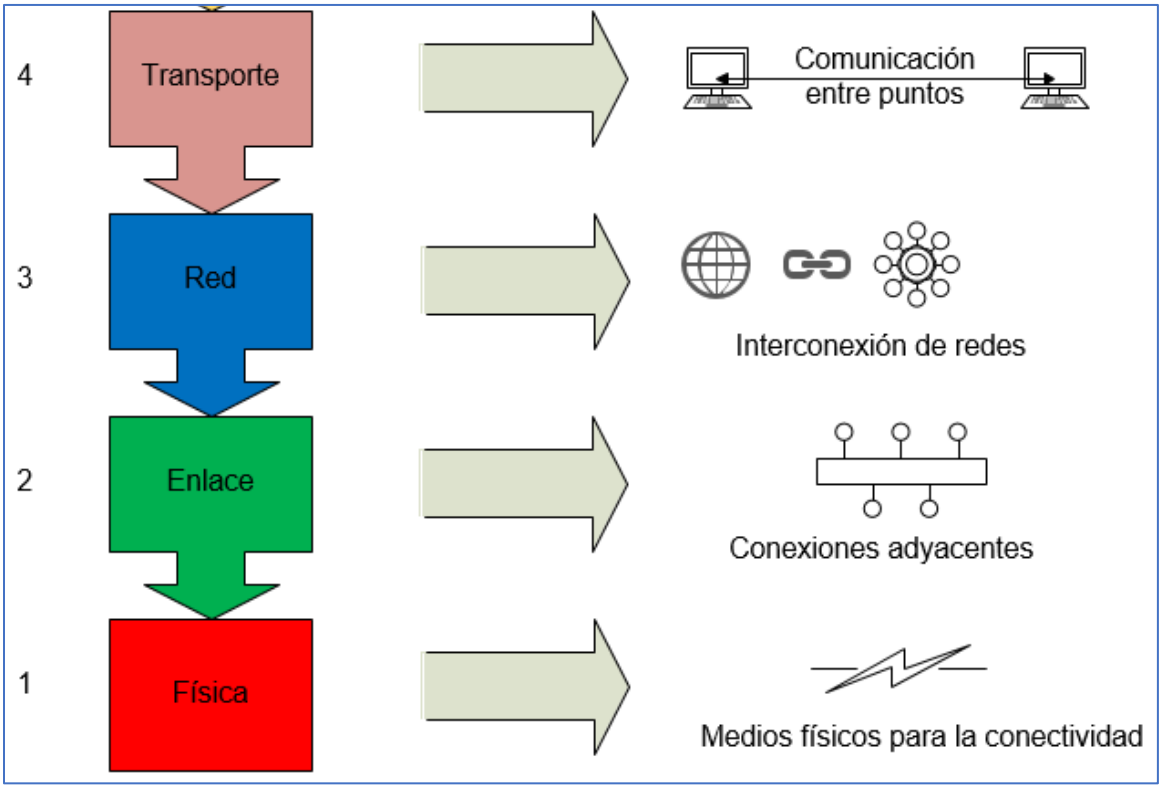


Imagen 2.9. Modelo OSI, funciones en capas. [A9]

La imagen muestra el funcionamiento general del Modelo OSI, partiendo del usuario en su interacción con una la interfaz gráfica de la **Aplicación**, como un correo electrónico o un gestor de transferencia de archivos generando información, dicha información adopta un formato compatible de **Presentación** para ser enviado a un destino esperado, después la información adquiere un control de flujo moderado para que viaje dentro de alguna **Sesión** a través de algún protocolo, en la siguiente fase la información se segmenta en paquetes para ser **Transportada** en rutas de transmisión encaminadas hacia la **Red** destino, posteriormente esos paquetes se dividen en tramas de datos evitando errores de transmisión para establecer **Enlace de Datos** dentro de la red destino, finalmente las tramas se dividen en bits los cuales viajan en el medio de transmisión **Físico** (cables u ondas de radio) empleado en la comunicación para hacer llegar la secuencia de bits al destino esperado.

Cada capa cuenta con funciones definidas, revisemos un poco más a detalle las capas del Modelo OSI, comenzando de la capa **Física** hacia la capa de **Aplicación**,

revisando también algunos elementos de interacción entre las capas, destacando las partes más esenciales de las capas.

Capa Física

Se encarga de realizar la transmisión de secuencia de *Bits* a través de un medio físico (canal), manejando señales eléctricas en caso de que el medio físico sea un cable de cobre, señales de luz en los casos de que el medio físico sean cables de fibra óptica, o bien ondas de radiofrecuencia cuando se trate de conexiones inalámbricas.

En esta capa se hace uso estándares definidos por instituciones como **IEEE** (Institute of Electrical and Electronic Engineers – Instituto de Ingenieros Eléctricos y Electrónicos), **ISO** (International Organization for Standardization – Organización Internacional para la Estandarización), **EIA/TIA** (Electronic Industries Association / Telecommunications Industry Association – Asociación de Industrias Electrónicas / Asociación de Industrias en Telecomunicaciones) para el diseño estandarizado de los medios físicos (cables), conectores, con el propósito de garantizar la transmisión de las señales.[33]

Capa de Enlace de Datos

Se encarga de agrupar los *Bits* en **tramas**, para ser enviadas de forma secuencial en enlaces directos, cada trama cuenta con cabecera y cola, los cuales contienen el mensaje a transmitir, así como la información sobre remitente y destinatario, además la cabecera y cola fungen como mecanismos para detección y corrección de errores de transmisión. Otra función de esta capa es el control de acceso al medio mediante identificadores **MAC** (el cual se encuentra en los dispositivos de hardware de comunicaciones), por lo que se deciden las acciones a realizar cuando dos dispositivos desean acceder de forma simultánea al medio de transmisión, utilizando **CRC** (Cyclic Redundant Check - Verificación de Redundancia Cíclica) dentro de una red local.

[33] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.10

En esta capa se puede hacer uso de los protocolos definidos por la interfaz física a utilizar, los más comunes son DSL (comunicación vía cable de par trenzado con conector RJ-11), 802.11 (comunicaciones inalámbricas), Ethernet (comunicación vía cable de par trenzado con conector RJ-45), TIA 492 (comunicación vía cable de fibra óptica).[34]

Capa de Red

El propósito de esta capa es darle una ruta óptima a la información, donde las tramas se empaquetan desde el punto de origen hacia el destino, mediante el uso de tablas de ruta, de carácter estático (direccionamiento definido) o dinámico, mismas que se forman con **direcciones IP** la cual funge una función similar a la de un remitente en un sistema de servicio postal. Otra función importante de esta capa es manejar la congestión generada por el envío de paquetes, con la intención de evitar saturación de paquetes en el medio de transmisión, para preservar la calidad del servicio de la red.

En la práctica, se hace uso de los protocolos **IP** (Internet Protocol – Protocolo de Internet) e **ICMP** (Internet Control Message Protocol – Protocolo de Mensajes de Control de Internet).

Capa de Transporte

Esta capa tiene varias responsabilidades importantes como el manejo de segmentos, determinar los servicios a utilizar para las capas superiores, aislar a las capas superiores en situaciones de cambios tecnológicos en su hardware de las capas inferiores.[35]

Ahora bien, dependiendo del rol establecido en un proceso de comunicación en la red (emisor o receptor), esta capa se encarga de ensamblar los segmentos del lado del receptor o bien de segmentar los datos de las capas superiores para su envío del lado del emisor, tareas que debe desempeñar de forma eficaz (sin pérdida de

[34] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.11
[35] Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson. P.38.

segmentos y manteniendo el control de envío de los mismos) y eficiente (asegurando que los segmentos vayan al destino indicado en la ruta trazada por la capa de red), con el propósito de lograr la recepción de los segmentos, y en caso de que no se confirme la recepción de algún segmento, entonces se solicita el reenvío del segmento en cuestión.

Además, previamente vimos que la información viaja tanto en redes locales o en redes externas como **Internet**, dicho esto, la capa de transporte lleva los datos de extremo a extremo, tanto de forma local o externa (esto último siendo determinado por una ruta en la capa de red).

Los servicios que solicita a las capas superiores siguen los protocolos **TCP** (Transmission Control Protocol – Protocolo de Control de la Transmisión) donde la entrega de información se hace de forma controlada sin importar la ocasión en que se haga la petición o entrega de información. Y **UDP** (User Datagram Protocol – Protocolo de Datagrama de Usuario) el cual no posee control de flujo para entrega de la información, sin embargo, la entrega de información se hace forma oportuna e inmediata, debido a que la interacción cliente-servidor ocurre en tiempo real, este protocolo es muy utilizado en servicios *Streaming* como *Netflix* o *Youtube*.[36]

Capa de Sesión

La capa de sesión toma el rol similar al de un moderador en algún proceso de comunicación, debido a que mantiene el control del flujo de la comunicación ya que controla el “dialogo”, en términos técnicos establece, administra y cierra las conexiones en el intercambio de información entre origen y destino, dichas funciones las realiza de forma controlada evitando que ambas partes realicen operaciones al mismo tiempo, además se asegura de cerrar una transmisión de información de forma adecuada y si hay interrupciones busca reanudar la transmisión en algún punto manteniendo sincronía.

[36] Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson. P.40.

Para establecer el tipo de comunicación se hace uso de los protocolos **TCP** o **UDP** solicitados por la capa de transporte al momento de levantar una sesión para determinar cómo será el flujo de la información.

Capa de Presentación

Define el formato que deben tomar los datos mediante sintaxis y semántica (establecidos por lenguajes de programación con los cuales se crean las aplicaciones), para garantizar la comunicación entre dispositivos sin importar el sistema operativo empleado, entonces, la capa de presentación implementa los mecanismos de traducción necesarios para asegurar compatibilidad entre los sistemas, ya que cada sistema representa los datos de forma diferente. Otros mecanismos que ofrece como servicios esta capa son el cifrado de la información (si se requiere establecer seguridad), compresión (agilizando su transporte y consumiendo menos ancho de banda). En su interacción con la capa de sesión encontramos otra de sus funciones la conversión de los datos, por un lado, prepara la información para el flujo hacia las capas inferiores, de forma inversa también da formato a los datos para su flujo hacia la capa de aplicación.[37]

Capa de Aplicación

Esta capa es la que se encarga de la interacción directa del usuario con el proceso de comunicación, mediante el uso del protocolo más popular **HTTP** (HyperText Transfer Protocol – Protocolo de Transferencia de Hipertexto) para las aplicaciones que se comunican con los recursos de un equipo de cómputo, o con los recursos alojados de forma remota en algún servidor. Cabe aclarar que esta capa no es sinónimo de software de aplicación, ya que el software de aplicación es quien se sirve del protocolo HTTP de la capa de aplicación para tener acceso a los recursos de la red. [38]

Las interfaces más comunes que se pueden utilizar en esta capa son **SMTP** (Simple Mail Transfer Protocol – Protocolo para Transferencia Simple de Correo) para correo

[37] ISACA. (2015). Manual de Preparación para el Examen CISA. EE. UU.: ISACA. P.296.
[38] Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson. P.38.

electrónico, **FTP** (File Transfer Protocol – Protocolo para Transferencia de Archivos) para transferencia de archivos, **DNS** (Domain Name Server – Servidor de Nombres de Dominio) para nombres de dominio (nombres de los sitios web).

La siguiente imagen sintetiza el Modelo OSI mostrando el flujo completo en su esquema de comunicación, donde la información parte de forma privada hacia entornos públicos para su transporte hacia su destino de carácter privado:

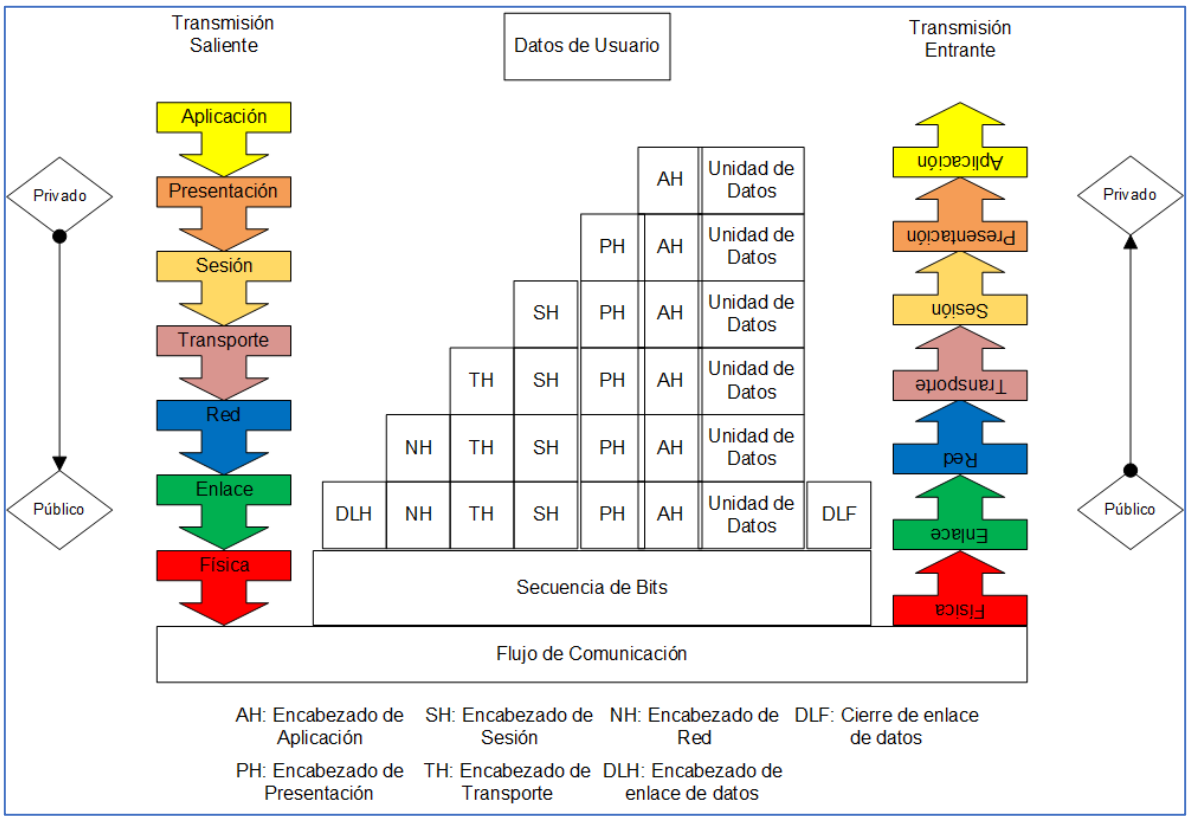


Imagen 2.10. Modelo OSI, flujo de comunicación. [A10]

2.3. Seguridad en Infraestructura de Red.

A lo largo de este capítulo se han mencionado conceptos, términos y elementos involucrados en una Infraestructura de Red, representando la base teórica de la presente propuesta. No obstante, es importante reconocer la existencia de **vulnerabilidades**, **amenazas** y **riesgos**, los cuales tienen los propósitos desde mermar algún sistema y su infraestructura, hasta sacar ventaja de las

vulnerabilidades existentes dentro de los sistemas e infraestructura con diversos fines, o incluso secuestrar información existente dentro de la infraestructura.

Por tanto, resulta imperativo adoptar medidas básicas de seguridad a través de **conceptos**, **políticas** y **dispositivos de seguridad**, en formas tanto teórica como operativa. Dicho lo anterior, este apartado tiene la intención de sentar algunas bases teóricas elementales para fundamentar las medidas de seguridad operativas presentadas más adelante en la presente propuesta.

2.3.1. Conceptos básicos y buenas prácticas generales de Seguridad en Red.

A continuación, veremos algunos términos básicos que debemos de considerar en materia de Seguridad en una Red:

- **Vulnerabilidad.** Son puntos débiles los cuales pueden ser aprovechados como entradas para los atacantes, comprometiendo la disponibilidad, confidencialidad e integridad de la infraestructura de red.
- **Amenaza.** Acciones que aprovechan las vulnerabilidades existentes en la infraestructura, atentando contra los elementos existentes dentro de la red, ejerciendo impacto negativo sobre los mismos. Cabe señalar que las acciones pueden ser perpetradas por atacantes, por factores físicos externos como algún desastre natural, o incluso por la negligencia de los recursos humanos pertenecientes a la organización que opera en la infraestructura de red.
- **Riesgo.** Es la posibilidad que algún incidente se manifieste en forma ataque, o evento natural, incidente en el cual se materializa en pérdidas de información o daños tanto en los elementos de la red como en la infraestructura en general.[39]

[39] INCIBE. (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?, diciembre 10, 2018, de INCIBE Sitio web: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Ahora consideremos los siguientes factores y sus daños potenciales tanto para la infraestructura de red como para la unidad donde opera:

- **Usuarios:** son los elementos humanos que realizan operaciones dentro de la infraestructura de red, es importante considerar el peor de los casos, esto es asumir que la persona desconoce conceptos en temas de seguridad, ignorando que las consecuencias de sus operaciones realizadas dentro de la infraestructura se pueden tornar en vulnerabilidades para la organización.
- **Atacantes:** son aquellos elementos (ya sea humanos o software) que aprovechan alguna vulnerabilidad encontrada, para perpetrar acciones que comprometen la información residente en algún sistema dentro de la infraestructura.
- **Negligencia Operativa:** son los vicios o malos hábitos de los elementos operativos dentro de la organización, considerando como malos hábitos acciones operativas reincidentes negativas que pueden comprometer su equipo o información dentro del equipo, ejerciendo un impacto negativo para la infraestructura.
- **Ingeniería Social:** hace alusión a las técnicas de persuasión perpetradas por atacantes que aprovechan la falta de precaución de los usuarios operativos (tornándose en víctimas), para la obtención de información sensible implicando una vulnerabilidad para la organización.
- **Desastres Naturales:** este factor es impredecible tanto en su aparición como en el impacto que puede generar, por lo que es recomendable tenerlo presente de forma constante teniendo medidas preventivas premeditadas como respaldo periódico de información, un mayor blindaje físico para los dispositivos, un diseño de los espacios físicos del edificio adaptados a mitigar lo mayor posible este riesgo.
- **Software Malicioso:** son los programas o aplicaciones que realizan ataques directos o silenciosos aprovechando alguna vulnerabilidad, como las

acciones de algún operador de los sistemas o algún punto débil existente en la infraestructura.

- **Software Cazarrecompensas:** son programas o aplicaciones que secuestran la información existente dentro del equipo donde llegan a hospedarse, los cuales solicitan una recompensa de bienes ya sea de una transferencia de dinero o de *bitcoins*[40], para la liberación de la información abducida, este software entra en operación al aprovechar alguna vulnerabilidad creada por algún usuario.
- **Botnets:** son equipos que se encuentran infectados con algún software malicioso para perpetrar ataques a terceros.

Veamos la siguiente imagen sintetizando los factores de riesgo y su daño potencial:

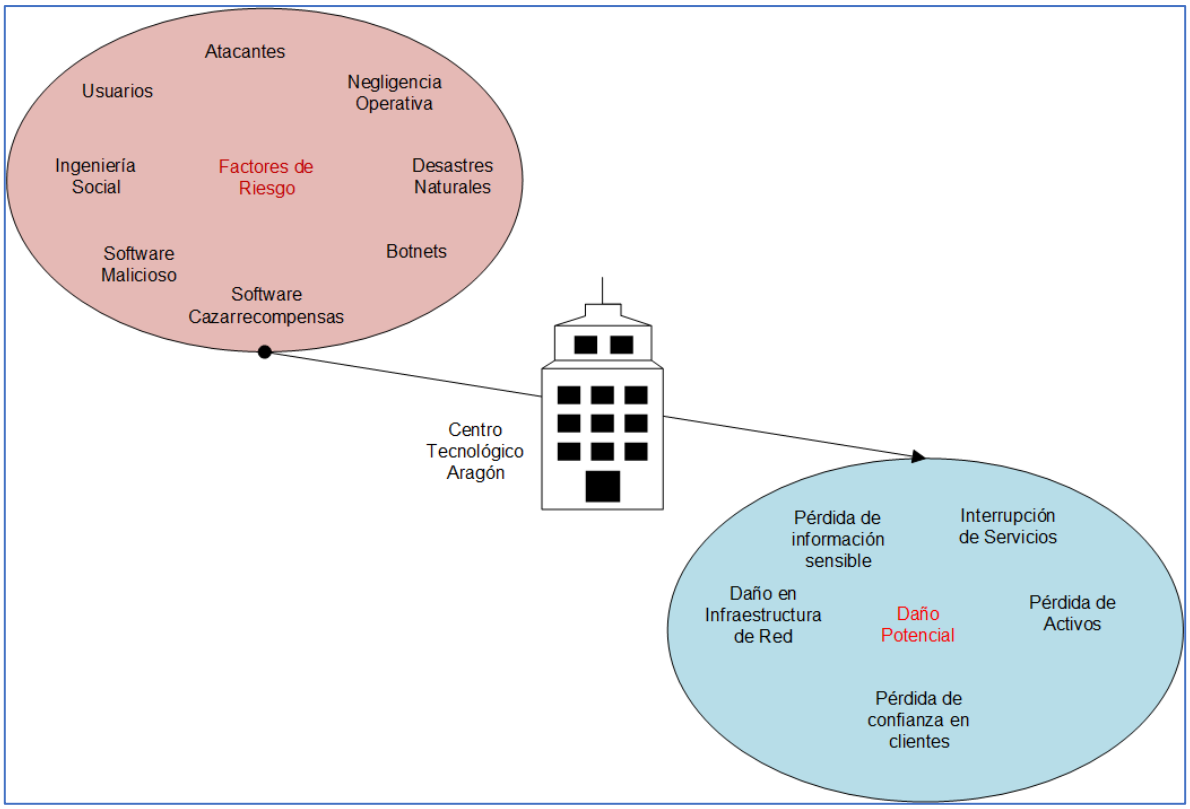


Imagen 2.11. Factores de Riesgo y Daño Potencial. [A11]

[40] Divisa electrónica, la cual se utiliza para el intercambio de bienes y servicios, con la diferencia que no depende de una entidad bancaria.

Ahora veamos los daños potenciales ocasionados por los factores mencionados[41]:

- **Pérdida de información sensible:** conjunto de datos con información privada o confidencial residente dentro de algún sistema perteneciente a la infraestructura, la cual fue eliminada, abducida, alterada o peor aún utilizada por algún atacante para sus propios fines.
- **Interrupción de Servicios:** es el paro de actividades de algún servicio como un gestor de correos o un gestor de hospedaje de datos para la información de usuarios internos o externos, el cual puede tener un impacto negativo para la confianza de los usuarios o representar pérdidas económicas.
- **Daño en Infraestructura de Red:** con daño se hace referencia a impactos en equipos pertenecientes a la infraestructura, desde dispositivos de red específicos o computadoras, donde a niveles de hardware o software se hayan visto comprometidos, desde un mal funcionamiento, aperturas a vulnerabilidades, incluso hasta la baja operativa definitiva de algún equipo o dispositivo.
- **Pérdida de Activos:** es la baja operativa de equipos existentes en la infraestructura, donde se realizan las tareas cotidianas por la organización, ocasionando merma en la operación de la organización, e impactos negativos en cuestiones económicas para la organización.
- **Pérdida de Confianza en Clientes:** ofrecer servicios electrónicos implica que existen clientes consumidores, entonces la organización se hace de dominio público (incluso reservando derechos de admisión), ahora bien, si la organización es víctima de ataques se va a reflejar en un desempeño mermado, el cual no pasa inadvertido para el consumidor, esto genera duda e incertidumbre en si debe continuar con sus operaciones, al grado de abandonar los servicios adquiridos en aras de proteger su información. Una vez perdida la confianza se torna complicado recuperar a esos clientes.

[41] Thomas, T. & Stoddard, D. (2012). Network Security First-Step. Indianapolis, EE. UU.: Cisco Press. P.86.

Los riesgos y sus daños nos ofrecen un panorama para acciones preventivas o correctivas, a través del uso de políticas, dispositivos especializados o configuraciones adecuadas para mitigar lo más posible esos riesgos (de los que se hará mención más adelante).

Sin embargo, es importante comenzar **aceptando** que los riesgos existen, con el fin de **compartir** este hecho con los miembros operativos, administrativos y directivos de la organización, para tomar **medidas** las cuales apoyen en **evitar** los riesgos en medida de lo posible.[42]

Objetivos de la Seguridad aplicados en la Infraestructura de Red

La seguridad informática cuenta con objetivos a cumplir, veamos la adaptación de estos en una infraestructura de red[43]:

- **Integridad.** Los elementos en la infraestructura de red no deben presentar alteraciones, a menos que se realicen modificaciones solicitadas previamente por usuarios autorizados.
- **Disponibilidad.** Los elementos de la infraestructura de red deben estar disponibles para la realización de las tareas diarias de los usuarios cuando ellos lo soliciten.
- **Privacidad.** Los elementos de la infraestructura de red solo son visibles y accesibles para los usuarios previamente autorizados.
- **Control.** Solo los administradores de red, o usuarios autorizados determinan los accesos a los elementos de la infraestructura de red.
- **Autenticidad.** Es la verificación que la información transportada de un punto origen hacia un destino haya llegado sin alteraciones durante el tránsito por la infraestructura de red.

[42] INCIBE. (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?, diciembre 10, 2018, de INCIBE Sitio web: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
[43] ISACA. (2015). Manual de Preparación para el Examen CISA. EE. UU.: ISACA. P.393.

- **No repudio.** Si un mensaje fue alterado, se debe tener la evidencia contundente de la acción infractora, para que cualquier entidad dentro de la infraestructura de red no se deslinde de sus acciones perpetradas.
- **Auditoría.** Es la revisión de la aplicación de controles para cumplir las políticas establecidas de seguridad, revisión de las acciones realizadas, quienes las realizaron y en qué fecha se realizaron dichas acciones dentro de la infraestructura de red mediante un procedimiento de revisión periódica y constante.

Controles y buenas prácticas de Seguridad en la Infraestructura de Red

Comencemos revisando algunos controles de **carácter general** para toda la infraestructura de la red[44]:

- ✓ El control de la red debe ser realizada por administradores u operadores con capacitación previa y de preferencia con experiencia operativa.
- ✓ El control de la red debe estar aislado de otras funciones operativas.
- ✓ El control de la red debe tener jerarquía de operaciones, dejando el control de la bitácora operativa (archivos Log) en manos de los administradores de red de forma exclusiva.
- ✓ El control de la red debe facilitar las auditorías a través de rastros de operación.
- ✓ Los rastros de operación se deben revisar de forma periódica para detectar actividades no autorizadas.
- ✓ Tanto protocolos como los estándares de red predefinidos por la organización deben estar documentados y a disposición tanto de los altos mandos, administradores, operadores especializados o auditores.
- ✓ Los protocolos y estándares de red deben tener una revisión periódica para garantizar la aplicación de estos dentro de la infraestructura.
- ✓ El acceso a los administradores u operadores especializados debe estar previamente agendado, además de mantener monitoreo durante el evento para evitar accesos no autorizados.

[44] ISACA. (2015). Manual de Preparación para el Examen CISA. EE. UU.: ISACA. P.390.

- ✓ Se deben mantener archivos de configuración general de todos los elementos administrables, con el fin de tener identificado cada dispositivo y sus funciones que realiza para facilitar la detección de eventos no esperados.

Estos controles aplican para toda la unidad, aunque, también es necesario revisar controles para las **Redes Locales**, las cuales se encuentran en cada área o laboratorio perteneciente a la unidad[45]:

- ✓ Guardar una relación de propiedad – dispositivo del software, archivos y accesos a servicios, en un archivo con impresiones periódicas el cual solo el responsable de área puede tener acceso.
- ✓ Limitar el acceso de contenidos a los usuarios operativos, para que solo utilicen lo que realmente necesitan para desempeñar sus funciones.
- ✓ Bloquear funciones administrativas en los sistemas operativos, para evitar cambios en configuraciones, a menos que toda el área cuente con operadores capacitados para esas funciones.
- ✓ Prevenir actualización simultánea de los sistemas operativos de los usuarios para evitar alto consumo de recursos innecesarios de red, y evitar mermar el desempeño del área.
- ✓ Definir un protocolo para la creación de credenciales de inicio de sesión a los equipos de cómputo.
- ✓ Utilizar dispositivos de red administrables, con puertos etiquetados para evitar accesos no autorizados a dispositivos no registrados.

Algunas áreas pueden llegar a hacer uso de **Redes Inalámbricas**, los siguientes controles se consideran fundamentales[46]:

- ✓ Ocultar el SSID de las redes emisoras.
- ✓ Manejar un nivel de seguridad WPA2, el cual presenta menores vulnerabilidades.
- ✓ Mantener una frecuencia de ondas de radio acorde con el espacio físico.

[45] ISACA. (2015). Manual de Preparación para el Examen CISA. EE. UU.: ISACA. P.391.
[46] Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson. P.708.

- ✓ Limitar el número de clientes inalámbricos acorde con el número de operadores alámbricos.
- ✓ Establecer red de invitados, algunos dispositivos ofrecen esta característica, la cual permite aislar los dispositivos pertenecientes a la red inalámbrica operativa del grupo de invitados.
- ✓ Mantener controles operativos similares a los de una Red LAN vista en el apartado anterior.

2.3.2. Políticas de Seguridad.

En una infraestructura de red participan elementos tecnológicos, información, y recursos humanos. Además, anteriormente vimos que existen riesgos y amenazas en materia de seguridad, entonces resulta recomendable revisar algunas **Políticas** elementales para definir reglas, límites y funciones a desempeñar por parte de los recursos humanos, dentro de la infraestructura de red.

Primeramente, revisemos algunos puntos que resaltan la importancia de establecer políticas[47]:

- Se establecen expectativas para procedimientos, estándares y manuales a seguir.
- Define conductas adecuadas por los diferentes roles en la red.
- Establece consenso operacional y de negocio.
- Provee de mecanismos de respuesta ante situaciones de conductas inesperadas.
- Define tanto roles como responsabilidades para cada integrante de la infraestructura de red.
- Define conceptos e ideas cruciales al momento de asegurar la infraestructura de red.
- Permite establecer el uso de herramientas o dispositivos para justificar inversiones en la seguridad de la infraestructura de red.

[47] Thomas, T. & Stoddard, D. (2012). Network Security First-Step. Indianapolis, EE. UU.: Cisco Press. P.45.

Tener políticas de seguridad facilita resaltar la importancia de adquirir buenos hábitos preventivos y operacionales para todas las áreas de la organización, para tener un control adecuado de roles, responsabilidades y límites de cada área, usuario, líder, administrador. Esa serie de hábitos incluso se pueden lograr adaptar a la vida cotidiana, en aspectos fuera de lo tecnológico.

Revisemos la siguiente tabla, la cual contiene políticas seleccionadas para un control básico de una infraestructura de red:

Nombre de la Política	Descripción
Procesos de Antivirus	Definir procedimientos a seguir para la reducción de amenazas de códigos maliciosos en la red.
Auditoría en Escaneo de Vulnerabilidades	Proveer de autoridad a la organización para crear un grupo de gente capacitada, el cual tiene la tarea de realizar auditoría bajo las premisas de buenas prácticas
Seguridad DMZ	Proveer de reglas definibles para todas las redes involucradas en la infraestructura y los equipos servidores conectados a internet dentro de la zona desmilitarizada.
Uso aceptable	Delimitar quienes pueden usar equipos de cómputo y redes de la organización.
Política de evaluación de adquisiciones	Definir responsabilidades respecto a adquisiciones corporativas, y definir los requerimientos mínimos para que una adquisición a evaluar sea completada por el grupo de seguridad de la información.
Extranet	Definir los requisitos de las organizaciones de terceros para que el acceso a la red de la organización se dé mediante un acuerdo de conectividad firmado por el tercero. Como ejemplos está algún socio o un proveedor de servicios.
Sensibilidad de la Información activa	Ayudar a los empleados a determinar qué información es de carácter privado para los invitados o a los que no sean empleados de la organización, para que la información sensible no sea mostrada sin previa autorización.
Uso de Internet	Proveer reglas sobre que sí y que no se considera apropiado acceder en internet, esto se puede mitigar con un filtro de contenidos web.
Dispositivos de Comunicación Personal	Definir los requisitos para dispositivos personales como Smartphones, Tablets, o Laptops y cómo se permiten usar esos dispositivos.

Acceso Remoto	Definir las reglas o software permitidos para la conectividad a la red organizacional desde cualquier dispositivo fuera de la organización.
Evaluación de Riesgos	Exhortar a que el grupo encargado de la seguridad de la información realice evaluaciones periódicas de los riesgos en la organización, con el propósito de encontrar y solventar vulnerabilidades.
Seguridad en Routers y Switches	Definir una configuración de seguridad mínima para routers y switches de la infraestructura de red, misma que debe ser realizada y controlada por los administradores de red.
Seguridad en Servidores	Establecer configuraciones básicas para los servidores internos, los cuales son operados bajo las premisas establecidas por la organización.
Comunicación Inalámbrica	Establecer reglas para el acceso a la red inalámbrica.

Tabla 2.2. Políticas de Seguridad Básicas. [TA1]

2.3.3. Seguridad en Internet.

Si los riesgos existen en las redes locales ejerciendo en ocasiones alto impacto, en internet dichos riesgos se potencian por la naturaleza global de la red de redes. Al estar basado en el protocolo **TCP/IP** permite que tanto redes privadas como públicas tengan comunicación, incrementando la cantidad de factores de riesgo, ya que alrededor del 40 al 50% de la población mundial cuenta con acceso a internet.[48]

Teniendo en cuenta ese preámbulo es importante identificar los tipos de ataque existentes en Internet:

Ataques Pasivos. El propósito de éstos es recabar información sobre el objetivo a atacar, ya sea un equipo, una infraestructura o un sitio web, las acciones que realiza este tipo de ataque es analizar el entorno donde reside la víctima, revisar de forma no autorizada el tráfico circulante, poner software que esté revisando las actividades realizadas, todo ello en carácter exploratorio, sin intenciones de alterar (aún) algún elemento de la víctima, no obstante, su intrusión es capaz de obtener datos sensibles a través del análisis de tráfico de la infraestructura de red.

[48] ISACA. (2015). Manual de Preparación para el Examen CISA. EE. UU.: ISACA. P.394.

Ataques Activos. En algunas ocasiones éste ataque viene precedido de un ataque pasivo, los objetivos son variados, desde tener el control de un sistema, ocasionar ataques desde ese sistema, secuestrar la información de ese sistema, infectar a la infraestructura con código malicioso, o cualquier otro de las siguientes formas más comunes[49]:

- Ataque de Fuerza Bruta.
- Enmascaramiento.
- Reenvío de paquetes.
- Phishing (suplantación de identidad).
- Modificación de mensajes.
- Acceso no autorizado mediante Internet.
- Denegación de Servicio (DoS).
- Bombardeo y correo basura en los gestores de correo electrónico.
- Suplantación de correo electrónico (spoofing).

Para que estos tipos de ataque se presenten, las siguientes causas intervienen en su punto de partida:

- Variedad y fácil disponibilidad de herramientas en internet para perpetrar los dos tipos de ataque.
- La falta de cultura sobre seguridad y por consiguiente falta de capacitación en los empleados de una organización.
- Nula configuración de seguridad en los dispositivos de red, asimismo en los equipos de cómputo existentes en la infraestructura de red.
- Mantenimiento nulo en los dispositivos de red, mientras más pasa el tiempo más ventanas de vulnerabilidad se desarrollan sin que la organización lo considere.
- Nula implementación de dispositivos firewalls dentro de la infraestructura de red.

[49] ISACA. (2015). Manual de Preparación para el Examen CISA. EE. UU.: ISACA. P.395.

- Mala configuración de los firewalls en los sistemas operativos de los equipos de cómputo pertenecientes a la infraestructura de red.

Todas esas causas representan vulnerabilidades para la infraestructura de red y sus elementos, no obstante, como en el caso de la Red Local, es posible establecer controles de seguridad para mitigar lo mayor posible esas vulnerabilidades, revisemos algunas recomendaciones generales:

- ✓ Realizar evaluaciones de riesgos periódicamente sobre desarrollo de sistemas web.
- ✓ Realizar investigación de herramientas existentes en internet para la realización de los tipos de ataque, con la intención de conocer los alcances y las amenazas que representan.
- ✓ Incentivar la cultura de seguridad mediante capacitación a los empleados, con la finalidad de realizar mejoras en sus responsabilidades.
- ✓ Implementar configuraciones actualizadas en dispositivos de red, tomando capacitaciones de ser necesario.
- ✓ Implementar dispositivos como firewalls, para reducir la ventana de vulnerabilidades de la infraestructura de red.
- ✓ Implementar técnicas de detección de intrusos, para ello proponer la creación de un grupo encargado de la seguridad de la infraestructura de red capacitándose de forma continua en dichas técnicas.
- ✓ Mecanismos de gestión de incidentes, mecanismos de respuesta ante detección de amenazas, contención de amenazas, o recuperación ante ataques perpetrados.
- ✓ Gestionar cambios de configuración preservando los niveles mínimos de seguridad.
- ✓ Implementar técnicas de encriptación para los archivos residentes en los equipos pertenecientes a la infraestructura de red.
- ✓ Formar un equipo CERT (Computer Emergency Response Team – Equipo de Respuesta ante Emergencias en Cómputo), quienes monitorean la infraestructura y mandan avisos oportunos en caso de incidente.

Vemos que en la actualidad internet ya tomó un lugar importante en los modelos de negocio, por lo que resulta imprescindible tomar este tipo de medidas para alcanzar al menos estabilidad en la organización, sin importar si es pública o privada.

2.3.4. Firewall.

En los apartados anteriores se hizo mención de este concepto de forma material, esto es, hablando del dispositivo, sin embargo, no solo cuenta con una representación material, también es un concepto abstracto partiendo de una idea hasta una representación en software el cual reside en un sistema operativo.

La idea se basa en los antiguos castillos medievales, donde se hacían excavaciones profundas alrededor del castillo, las murallas protegían el interior del castillo y solo existía un único acceso, un puente levadizo el cual estaba controlado por centinelas pudiendo observar con precisión quienes ingresaban o salían del castillo. En una infraestructura se parte de ese concepto, se pueden tener muchas redes LAN interconectadas dentro de la unidad, entonces el Firewall guarda una función similar a la del puente levadizo del castillo, se tiene un acceso controlado de los paquetes hacia las redes internas de la infraestructura.[50]

En otras palabras, un firewall representa el punto donde a las conexiones de la red se le aplican políticas para tener controles de tráfico de las redes externas hacia las redes internas (de afuera hacia adentro) como de las redes internas hacia las redes externas (de adentro hacia afuera).

La efectividad de un Firewall radica en que permite a los usuarios tener acceso a Internet, con las limitaciones que los administradores de red o un grupo CERT consideren pertinentes, y a su vez impedir paso a intrusos lo mayor posible, además de mantener tráfico controlado tanto en la red interna, como en su salida hacia las redes externas.

[50] Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson. P.704.

Características Generales de un Firewall

Un firewall puede ser un dispositivo de red el cual pretende blindar toda una infraestructura de red, o un software para blindar el sistema operativo de un equipo de cómputo, en cualquiera de las formas de este concepto, se cuenta con las siguientes características[51]:

- Bloquea accesos a sitios de internet preseleccionados por la organización.
- Limita el tráfico en los diferentes segmentos de la organización.
- Controla el acceso a usuarios a determinados servidores o servicios tanto de la red interna como en internet.
- Monitorea las interacciones entre las redes internas con las redes externas.
- Encripta paquetes cuando se estén utilizando VPN (Virtual Private Network – Red Privada Virtual).

Pero, un Firewall no solo adjudica ventajas, si no se tiene conocimiento básico de su operación, pueden presentarse las siguientes desventajas:

- Nula salida a Internet, o a servicios en Internet los cuales se comunican a través de puertos de comunicación comunes.
- Nula comunicación entre los dispositivos de red conectados al Firewall.
- Dejar sin comunicación a los dispositivos de la red virtual de voz.
- Dejar sin ningún tipo de acceso de red (tanto local como externa) a ciertas áreas de la organización.
- Incrementar vulnerabilidades al establecer políticas de acceso permisivo a todo el tráfico existente en la infraestructura de red.

2.3.5. DMZ.

En algunas organizaciones como el Centro Tecnológico Aragón, existen servidores, los cuales muchas veces son de carácter público ya que los servicios ofrecidos son para los usuarios de las redes exteriores e internet, por consiguiente, necesitan tener apertura en su tráfico de información. Aunque, si esos servidores comparten

[51] ISACA. (2015). Manual de Preparación para el Examen CISA. EE. UU.: ISACA. P.396.

la misma infraestructura de red de todas las unidades existentes dentro de la organización, existe la situación en que, si se desea dar blindaje a la infraestructura, se limitaría el tráfico teniendo impacto en el acceso hacia los servidores y la salida de los servicios a Internet.

Ante esta situación existe el concepto de **Zona Desmilitarizada (DMZ)**, esta zona funciona como una red aislada sin dejar de tener conectividad con la red que se tenga la intención de proteger, en la cual se pueden dejar los servidores de carácter público, en los cuales el manejo de los riesgos se delega en la configuración de sus firewall integrados en los sistemas operativos, o del dispositivo de red que les ofrezca la salida a Internet, representando una segunda línea de defensa para la red que se mantenga privada[52]. Veamos su funcionamiento a través de la siguiente imagen:

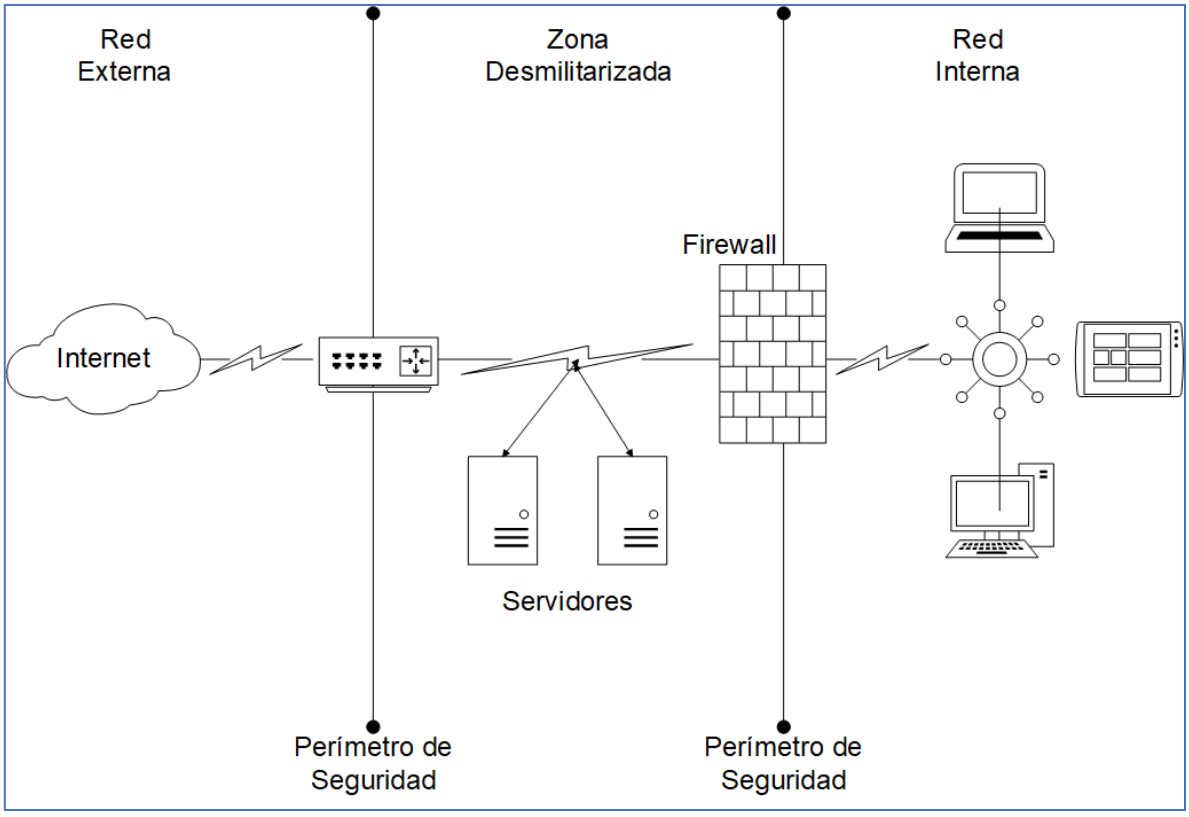


Imagen 2.12. Zona Desmilitarizada. [A12]

[52] ISACA. (2015). Manual de Preparación para el Examen CISA. EE. UU.: ISACA. P.398.

A lo largo del capítulo se revisaron algunos conceptos básicos en temas de redes, dispositivos de red, algunas buenas prácticas de red a implementar, e incluso políticas fundamentales de seguridad informática, el propósito de estos temas fue establecer la base de conocimiento para la propuesta. La finalidad es comprender con mayor precisión los elementos que se mencionarán en la propuesta, impulsando la implementación técnica para cualquier miembro del laboratorio de cómputo, o para cualquier estudiante de ingeniería en computación, o disciplina relacionada.

3. Red Actual.

Previo a realizar la propuesta, es pertinente hacer un análisis del estado actual de la Infraestructura de Red del Centro Tecnológico Aragón, por tanto, este capítulo mostrará el diseño de Red Actual, la operación de esta, además del funcionamiento basado en los testimonios recabados en un estudio previamente realizado.

3.1. Estado actual de la red basado en diseño.

El Centro Tecnológico Aragón es una unidad multidisciplinaria, la cual consta de 3 pisos, donde se encuentran 10 áreas para las diferentes disciplinas ubicadas en laboratorios y oficinas, 2 áreas administrativas, 3 áreas audiovisuales, 1 auditorio para eventos académicos o culturales de todas las disciplinas impartidas en la Facultad de Estudios Superiores Aragón y 1 jardín botánico para la realización de prácticas multidisciplinarias.

Desde el momento de la planeación del edificio se establecieron requisitos de dimensiones para las diferentes áreas y disciplinas, además se consideraron espacios para establecer todos los dispositivos de comunicación, y a su vez la distribución de los nodos de comunicación alámbrica para todas las áreas.

Dicho esto, la unidad cuenta con 3 espacios dedicados para la ubicación de los dispositivos de comunicación, 1 espacio que funge como sitio principal donde llega el servicio de Internet, se establecen las configuraciones de enrutamiento, direccionamiento y nodos para cada área o laboratorio (capas 2 y 3 de OSI), dicho espacio se ubica en el ala norte de la planta baja de la unidad. Los otros 2 espacios están ubicados en el ala sur del primer y segundo piso, esos 2 espacios sirven para la distribución de nodos de cada piso, por lo que solo cuentan con dispositivos switch y paneles de distribución para realizar esa tarea.

Las siguientes fotografías muestran esos 3 espacios físicos de comunicación, así como su diseño actual:

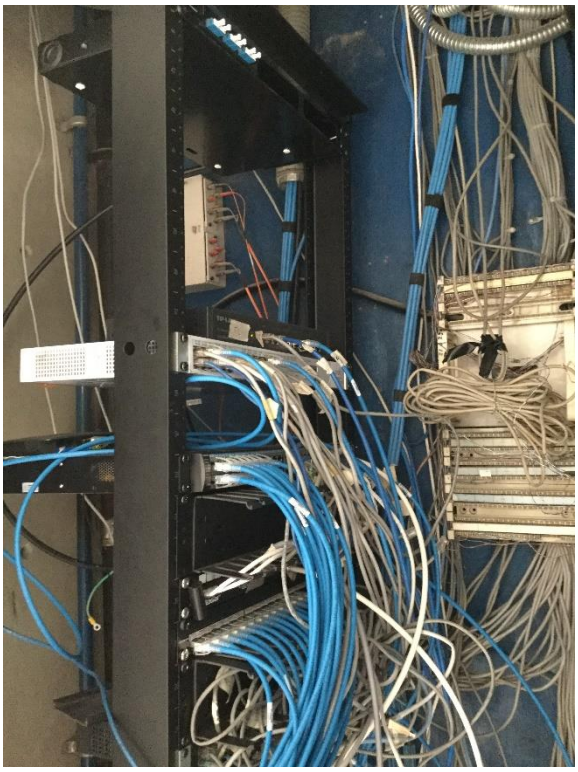


Imagen 3.1. Site Principal. [A13]

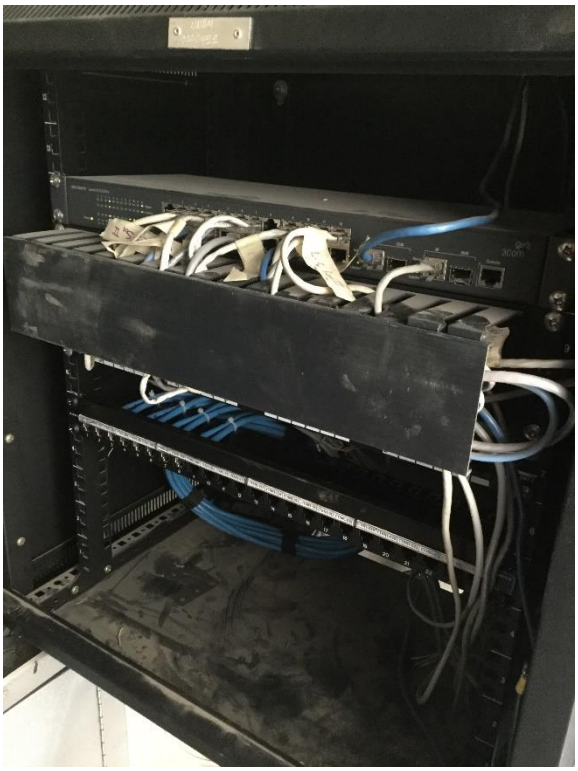


Imagen 3.2. Espacio de Comunicación en el primer piso. [A14]

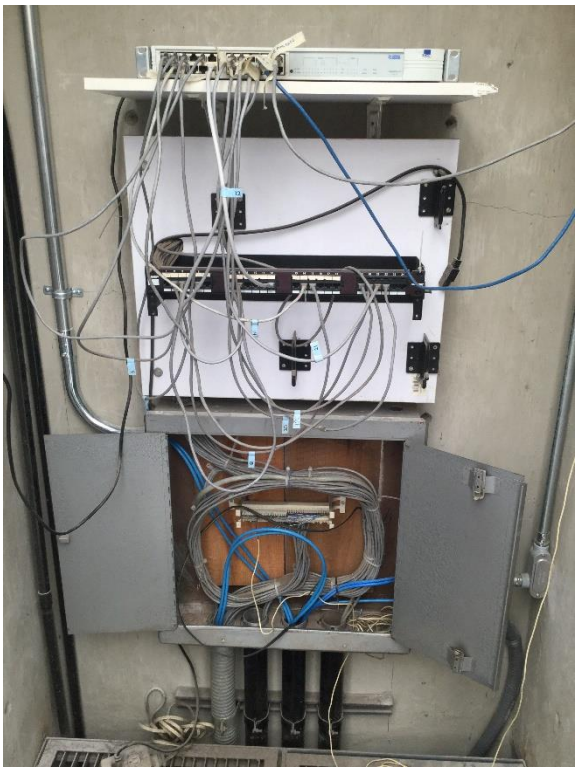


Imagen 3.3. Espacio de Comunicación en el segundo piso. [A15]

Ahora bien, dentro del diseño de red actual la distribución de nodos para todas las áreas y laboratorios del Centro Tecnológico Aragón, se indica con la siguiente tabla, dicha tabla se obtuvo del estudio realizado dentro de la unidad:

Área/Laboratorio	Número de Nodos
Ingeniería Ambiental	4
Ingeniería Mecánica	4

Medición, Instrumentación y Control	4
Estudios Ambientales	4
Seguridad Informática	4
Cómputo	6
INNOVA UNAM	3
Jardín Botánico	0
Auditorio y Espacios Audiovisuales	4
Administración	4
Coordinación	3

Tabla 3.1. Lista de Nodos. [TA2]

Los siguientes planos muestran la distribución física de los nodos por piso, áreas y laboratorios dentro del Centro Tecnológico Aragón (se muestran a partir de la siguiente página):

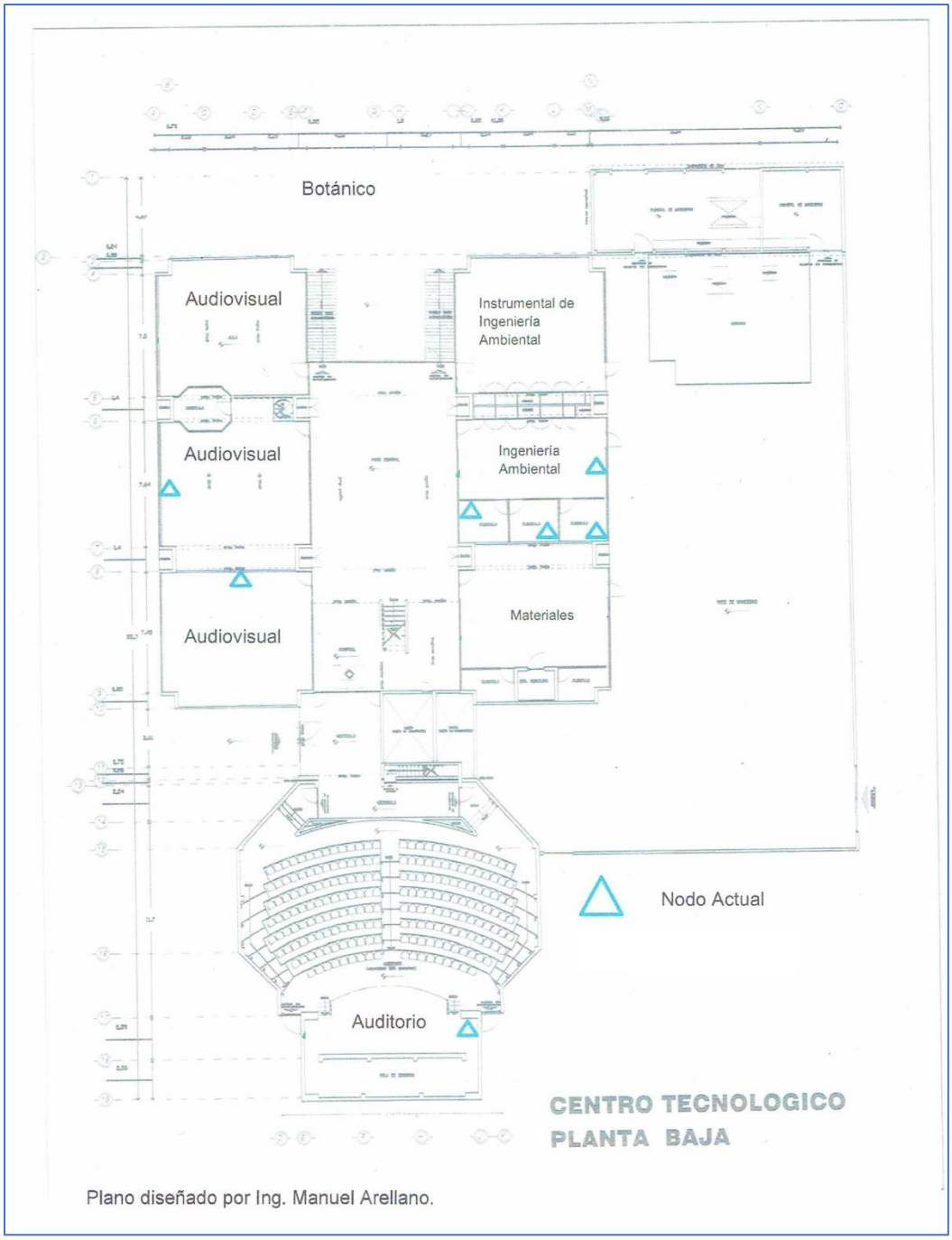


Imagen 3.4. Distribución Actual PB. [A16]

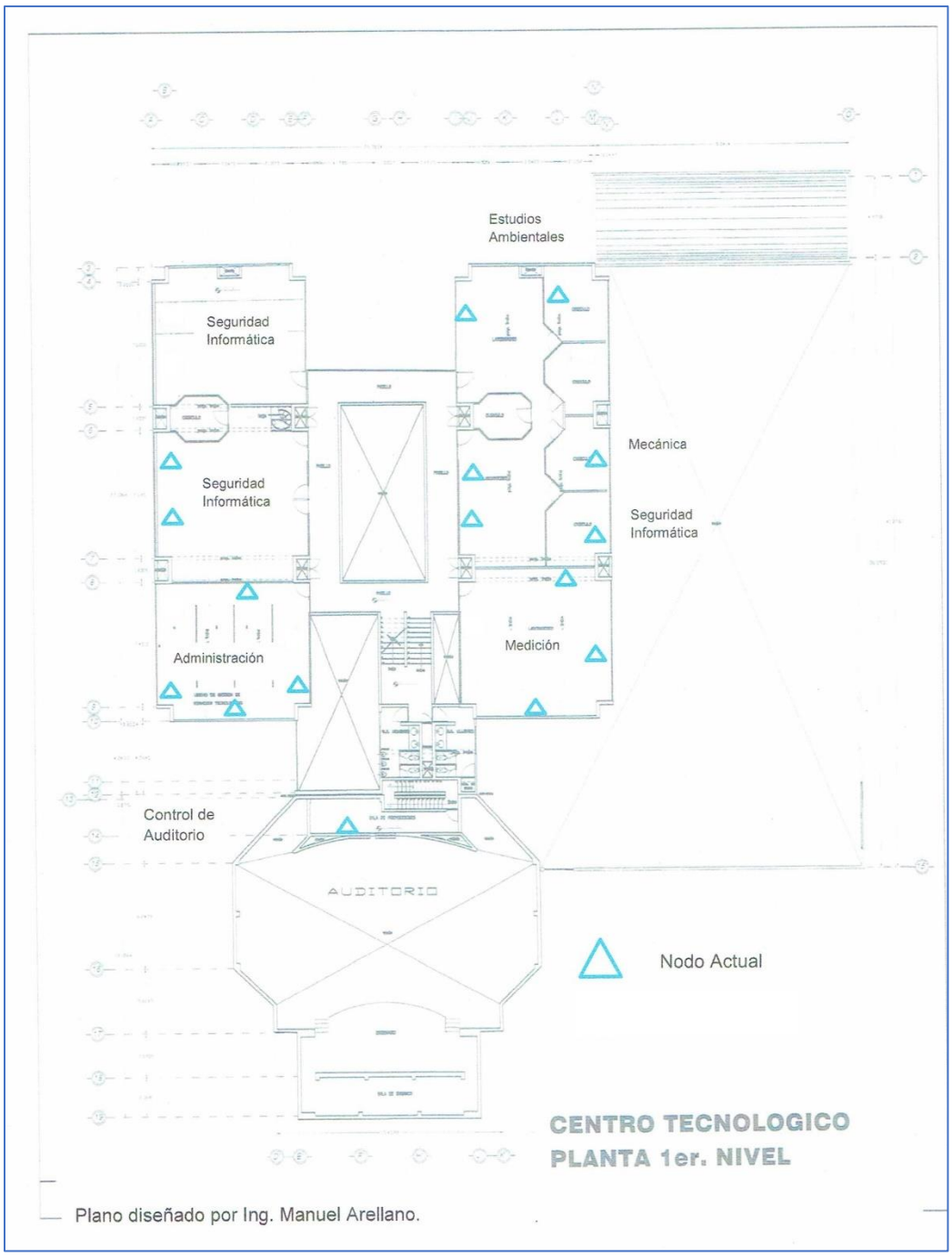


Imagen 3.5. Distribución Actual P1. [A17]

Imagen 3.6. Distribución Actual P2. [A18]

Para cerrar la exposición del diseño actual en el Centro Tecnológico Aragón revisemos el siguiente diagrama de red donde se muestra de forma general la distribución física de toda la red:

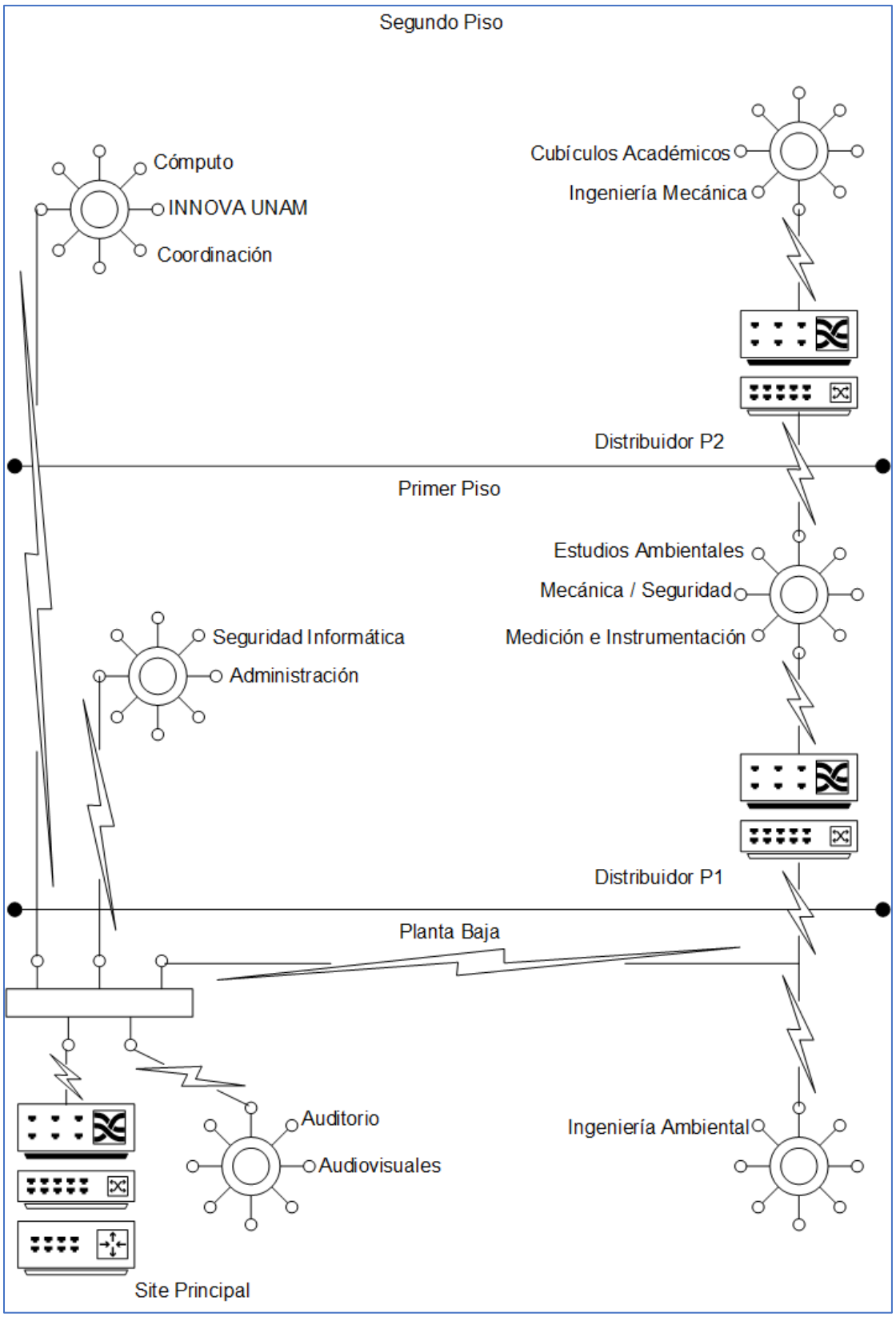


Imagen 3.7. Modelo de Red Actual. [A19]

3.2. Estado actual de la red basado en funcionamiento.

Con funcionamiento se hace referencia a la operación de la red a nivel lógico, en otras palabras, a las configuraciones existentes dentro de los dispositivos de red en el diseño físico general de la red.

Los dispositivos de red alojados en el sitio principal, reserva las direcciones IP (capa 3 del Modelo OSI), para que todos los nodos existentes en cada área/laboratorio puedan establecer comunicación interna y salida a internet a través del router principal, dicho router también posee una dirección IP para la ruta de salida a internet.

La distribución física de los nodos se logra mediante los switches conectados en el sitio principal, como en los sitios de distribución de los pisos superiores, los switches no poseen una configuración lógica, debido a que solo se encargan de distribuir los nodos.

Dicho lo anterior, los diversos dispositivos (computadoras, impresoras, o equipo de red personal) pertenecientes a las diferentes áreas, cuentan con una dirección IP definida por el administrador de la red, las cuales están contenidas en la siguiente tabla (solo se muestran los últimos 2 octetos por seguridad, puede consultar esa información con el administrador de la red local o el administrador de red de toda la Facultad):

Área/Laboratorio	Dirección IP
Coordinación	***.***.173.8
Secretaria coordinación	***.***.0.102
Secretaria coordinación	***.***.0.101
Secretaria coordinación	***.***.173.6
Lab. de cómputo	***.***.173.30
Lab. de cómputo	
Lab. de cómputo	***.***.173.19
Lab. de cómputo	***.***.173.29
Lab. de cómputo	***.***.173.58
Lab. de cómputo	***.***.173.31
Lab. de cómputo	***.***.173.39

Lab. de cómputo	***.***.173.44
Lab. de cómputo	***.***.173.35
Administración	***.***.173.14
Cubículo 4 Mel (comparte red)	***.***.173.60
Cubículo 4 Mel (comparte red)	***.***.173.60
Lab. Computo	***.***.173.21
Lab. seguridad	***.***.173.15
Vinculación	***.***.173.13
INNOVAUNAM	***.***.173.11
Mecánica	***.***.173.49
Materiales	***.***.173.43
Estudios Ambientales	***.***.173.55
Cómputo	***.***.173.7
Laboratorio de cómputo	***.***.173.17
Laboratorio de cómputo	***.***.173.16
Laboratorio de cómputo	***.***.173.22
Proyecto Antena CTA	***.***.173.32
Cámara de vigilancia	***.***.173.33

Tabla 3.2. Direccionamiento actual. [TA3]

La mayoría de las direcciones IP son de tipo público, este tipo de direccionamiento es flexible al momento de ofrecer servicios en línea, sin embargo, también puede representar una desventaja en términos de seguridad, más adelante durante la propuesta se hará un análisis sobre ese tipo de direccionamiento.

Sin embargo, otro detalle por notar es la existencia de un mayor número de nodos disponibles respecto al número de direcciones, esto se debe a que con el paso del tiempo ha crecido la demanda de direcciones, en las cuales no se ha tenido un control adecuado.

Finalmente, no existen políticas de manejo de control de tráfico, o de control de contenido, además, no se cuenta con un firewall como dispositivo, por consiguiente, no se manejan políticas de seguridad **globales** dentro de la red.

3.3. Estado actual de la red basado en testimonios.

En un período de 6 meses, se realizó una encuesta a todas las áreas/laboratorios del Centro Tecnológico Aragón, con el fin de recabar información sobre su experiencia de uso de la red actual, a continuación, se exponen algunas preguntas (las cuales no preservan el orden) concretas para mostrar tendencia estadística de uso y experiencia, el propósito es obtener respuestas concretas para evaluar la viabilidad de la propuesta, la cual se presentará en un capítulo posterior:

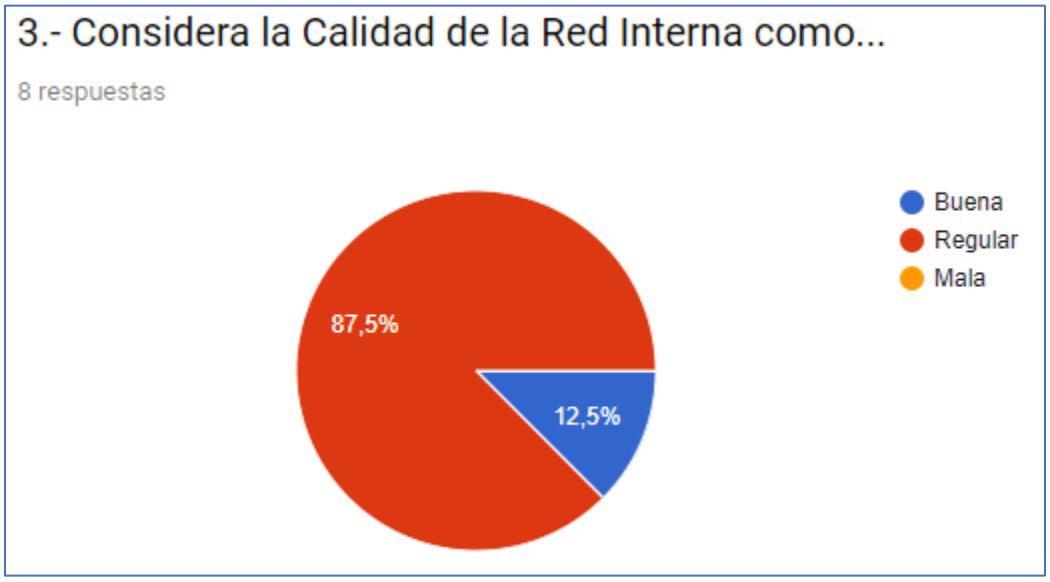


Imagen 3.8. Pregunta 3. [A20]

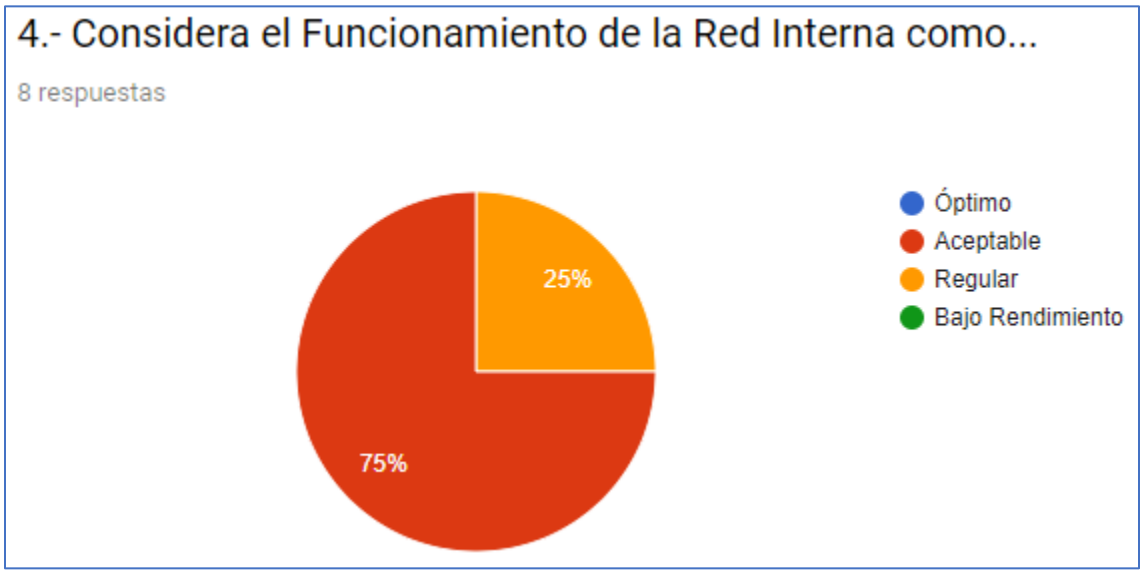


Imagen 3.9. Pregunta 4. [A21]

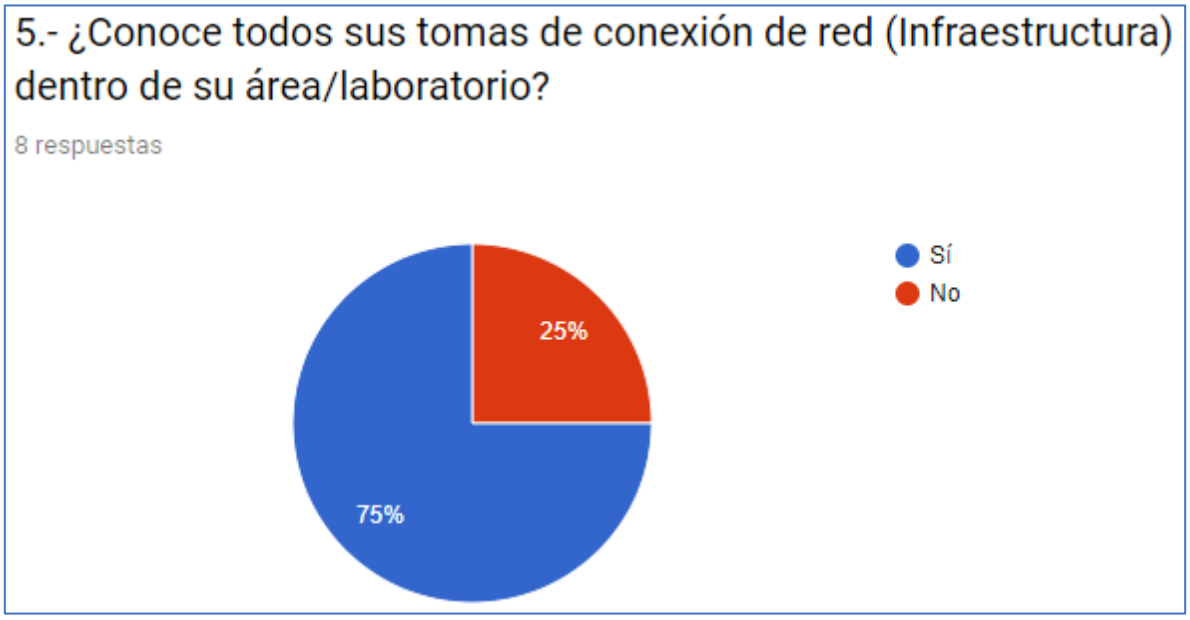


Imagen 3.10. Pregunta 5. [A22]

Imagen 3.11. Pregunta 6. [A23]

Las respuestas proporcionadas, fungen como testimonios de cada área/laboratorio sobre su experiencia con la red. La mayoría coincide que la calidad del servicio de la red es regular, ¾ partes consideran que el funcionamiento es aceptable sin llegar a ser óptimo, ¼ parte de las áreas/laboratorios no conocen los nodos que poseen

en su espacio, y en unanimidad consideran necesario actualizar los dispositivos de red del Centro Tecnológico Aragón.

La intención de este capítulo fue mostrar un análisis breve y concreto sobre el funcionamiento de la red, vimos el diseño físico y lógico, el contexto actual de la red, con el propósito que la propuesta ofrezca algunas soluciones a los detalles por mejorar.

Durante la exposición de los aspectos de diseño, funcionamiento y testimonios surgen áreas de oportunidad para mejorar el desempeño de la red, destacando detalles importantes, como la ausencia de políticas básicas de seguridad, las cuales se consideran urgentes por atender.

4. Necesidades por Área.

En los testimonios recabados durante el análisis del estado de la red actual del Centro Tecnológico Aragón, se solicitó a las áreas/laboratorios, destacar las oportunidades de mejora que detectan para tener un desempeño eficiente, dicho lo anterior, este capítulo tiene la intención de exponer lo que algunas áreas/laboratorios consideran necesario para mejorar su desempeño, dicha exposición se realizará por cada piso.

4.1. Planta Baja.

Audiovisuales

En las áreas audiovisuales, las cuales son el Auditorio Merfield Castro y las aulas audiovisuales, sus necesidades son:

- Videoconferencias a distancia, por parte de algunos profesores para impartir sus asignaturas.
- Constante actualización de su itinerario de eventos para el auditorio.
- Ancho de banda fluido (*al menos 50Mbps*) para la transmisión simultánea de eventos principales en el auditorio José Vasconcelos.

Sus oportunidades de mejora que detectan son:

- Extensión de nodos de comunicación para la conexión de dispositivos multimedia.
- Control de tráfico del ancho de banda para garantizar sus funciones de forma óptima.

Laboratorio de Ingeniería Ambiental

En el laboratorio de Ingeniería Ambiental expresan las siguientes necesidades en sus funciones:

- Búsqueda constante de información en bases de datos especializadas en los sistemas de la UNAM.
- Envío masivo de información vía correo electrónico.
- Actualización constante de datos a los sistemas de información por parte de los miembros del laboratorio.

Las oportunidades de mejora detectadas por parte del laboratorio son:

- Extensión de nodos de comunicación para la conexión de más dispositivos.
- Ancho de banda disponible para evitar pérdidas de información.
- Políticas de seguridad para evitar comprometer la información compartida y la información consumida.

4.2. Primer Piso.

Laboratorio de Mecánica

En este laboratorio presentan las siguientes necesidades:

- Búsqueda constante de información mediante contenido multimedia, manuales, bancos de información.

Las oportunidades de mejora detectadas por parte de este laboratorio son:

- Ancho de banda disponible para el acceso al contenido deseado por los miembros del laboratorio.

Administración

En el área administrativa exponen las siguientes necesidades:

- Consumo constante de información proveniente de otras áreas de la Facultad de Estudios Superiores Aragón, o de unidades pertenecientes a la UNAM.
- Búsqueda constante de información en bases de datos especializadas.
- Consulta de información de parte de otras áreas de la UNAM.

Las oportunidades de mejora señaladas por parte del área son:

- Extensión de nodos de comunicación para la instalación de dispositivos.
- Control de tráfico del ancho de banda para una operación óptima en sus funciones.
- Políticas de seguridad para evitar comprometer los equipos pertenecientes al área.

Laboratorio de Seguridad Informática

Las necesidades que presenta el laboratorio son las siguientes:

- Consulta constante de información sobre temas de seguridad, contenido documental, contenido multimedia.
- Uso de herramientas de seguridad para realizar prácticas o pruebas.
- Búsqueda constante de información en bases de datos especializadas.
- Comunicación constante con dispositivos de cómputo o de red para monitoreo o prácticas desde fuera del laboratorio.

Las oportunidades de mejora que señala el laboratorio son:

- Extensión de nodos de comunicación para la instalación de dispositivos.
- Control de tráfico y contenido en internet, para mejorar la operación en sus actividades.
- Políticas de seguridad que no interfieran con las actividades que realizan los miembros del laboratorio.

Laboratorio de Estudios Ambientales

El laboratorio tiene las siguientes necesidades:

- Consulta constante de información con contenido variable.

Para mejorar su desempeño el laboratorio recomienda:

- Control de tráfico para que el ancho de banda no cause merma en sus actividades realizadas.

4.3. Segundo Piso.

Laboratorio de Medición e Instrumentación

El laboratorio expone las siguientes necesidades:

- Manejo de dispositivos, algunos de ellos con salida a internet para un desempeño expandido.
- Consulta constante de información en bases de datos especializadas.
- Búsqueda de todo tipo de contenido para retroalimentar sus actividades.

El laboratorio menciona que las oportunidades de mejora son:

- Extensión de nodos de comunicación para la instalación de dispositivos.
- Control de tráfico para que las búsquedas de información no ocasionen merma en el desempeño de sus actividades.

INNOVA UNAM

Esta área presenta las siguientes necesidades a cubrir:

- Comunicación constante con alumnos, emprendedores, empresas, mediante medios electrónicos para la organización de eventos.
- Consulta constante de información de contenido variable.
- Envío masivo de información a través de medios electrónicos.

Las mejoras propuestas por el área son:

- Extensión de nodos de comunicación para la instalación de dispositivos.
- Políticas de control de tráfico para realizar sus actividades de manera fluida.

Laboratorio de Cómputo

Este laboratorio expone las siguientes necesidades:

- Consulta constante de información de contenido variable.
- Descargas constantes de software para la realización de prácticas o proyectos.

- Consumo de servicios remotos a través de internet para la realización de proyectos.
- Conexiones remotas para monitoreo de servicios proporcionados.
- Conexión constante de servidores.
- Videoconferencias con clientes.
- Envío masivo de información a través de medios electrónicos.

Para tener un desempeño óptimo, el laboratorio destaca las siguientes áreas de oportunidad de mejora:

- Extensión de nodos de comunicación para la instalación de dispositivos.
- Control de tráfico y de contenido web para evitar cuellos de botella al momento de utilizar internet.
- Políticas de seguridad que no impidan las actividades realizadas.
- Establecimiento de una Zona Desmilitarizada para los servidores residentes en el laboratorio.

Coordinación

El área expone las siguientes necesidades:

- Envío masivo de información a través de medios electrónicos.
- Consulta constante de información de contenido variable.
- Conferencias electrónicas con colaboradores de proyectos.

La coordinación menciona las siguientes oportunidades para mejorar:

- Extensión de nodos de comunicación para la instalación de dispositivos.
- Control de tráfico para contar con ancho de banda para la realización de sus actividades.

El propósito de las oportunidades expuestas, señalan la importancia de realizar una actualización a la red, destacando que todas las áreas/laboratorios coinciden en la necesidad de proponer mejoras para tener un desempeño eficiente. Dichas áreas de oportunidad dan lugar a la propuesta la cual veremos en el capítulo siguiente.

5. Propuesta de Actualización.

En los capítulos previos se revisaron conceptos básicos en temas de redes, dispositivos de red y seguridad informática. También se realizó un análisis del estado actual de la red, el diseño físico que posee, y la configuración lógica dentro de los dispositivos del sitio principal. Finalmente, se mencionaron las necesidades de cada una de las áreas/laboratorios.

Tanto la revisión de temas, el análisis y las necesidades han tenido el propósito de sentar bases teóricas e incentivar la búsqueda de áreas de oportunidad de mejora. Entonces, el presente capítulo propondrá 2 alternativas de mejora, las cuales se denominarán como **Propuesta A** y **Propuesta B**.

En la **Propuesta A**, se propone la inclusión de un dispositivo *Firewall* dentro del sitio principal, en el cual se establecen configuraciones de funcionamiento y sobre todo políticas de seguridad, además de establecer opciones como el filtro de contenido web, o la posibilidad de incluir un servicio de **VPN** (Virtual Private Network – Red Privada Virtual) estable y seguro, o también la posibilidad de tener un mejor manejo de direccionamiento con IP públicas (para aquellas áreas/laboratorios que lo deseen adoptar), ejerciendo impacto de mejora de moderado a alto, no obstante, es importante señalar que se requiere realizar una inversión económica para poder incluir el dispositivo.

En la **Propuesta B**, se contempla realizar mejoras con los dispositivos existentes dentro del sitio principal, ejerciendo un menor impacto económico, pero se prescinde de establecer políticas de seguridad generales, o la inclusión de servicios adicionales, en otras palabras, el impacto de mejora sería de bajo a moderado.

Finalmente, otro propósito, es el de mostrar los pasos a realizar para las instalaciones, o configuraciones que se propondrán, con el fin de facilitar la implementación para cualquier miembro del laboratorio de cómputo, o estudiante de ingeniería en computación, sin importar si maneja el área de redes (ya que puede

apoyarse del marco teórico de la presente propuesta para una mejor retroalimentación), e incluso poder adaptar la presente propuesta a otras áreas académicas o administrativas de la Facultad de Estudios Superiores Aragón.

En términos de diseño físico ambas propuestas se adaptan a todo lo que se propondrá en ese apartado, comencemos con esa parte.

5.1. Actualización de Diseño.

En este apartado se documentará el estado actual de la red del Centro Tecnológico Aragón mediante un diseño topológico, incluyendo un par de diseños para las propuestas **A** y **B**, ya que, al contar con ese registro, a fututo nos facilitará hacer cambios o actualizaciones en el diseño. También se mencionarán los dispositivos a incluir en las áreas/laboratorios con el fin de mejorar la eficiencia, al final del apartado se propone una actualización del cableado estructurado para todo el centro, para prolongar la vida útil de esas vías de comunicación.

5.1.1. Topología Actualizada.

Partamos con el diseño topológico actual, el Centro Tecnológico Aragón está distribuido de la siguiente forma:

- 1 sitio principal, ubicado en la planta baja en el ala norte, donde se conecta con el sitio central de la Facultad de Estudios Aragón, a su vez ese sitio distribuye el servicio de Internet con el que cuenta la Facultad.
- 2 sitios de distribución, ubicados en el primer y segundo piso en el ala sur ambos sitios están conectados al sitio principal, la función de estos es repartir los nodos para todas las áreas/laboratorios. La conexión está dada por cable Ethernet.
- Nodos de conexión para cada área/laboratorio.
- En los casos del laboratorio de cómputo y el laboratorio de seguridad informática, cuentan con dispositivos de red particulares para sus actividades.

Gráficamente el diseño topológico actual está organizado de la siguiente forma:

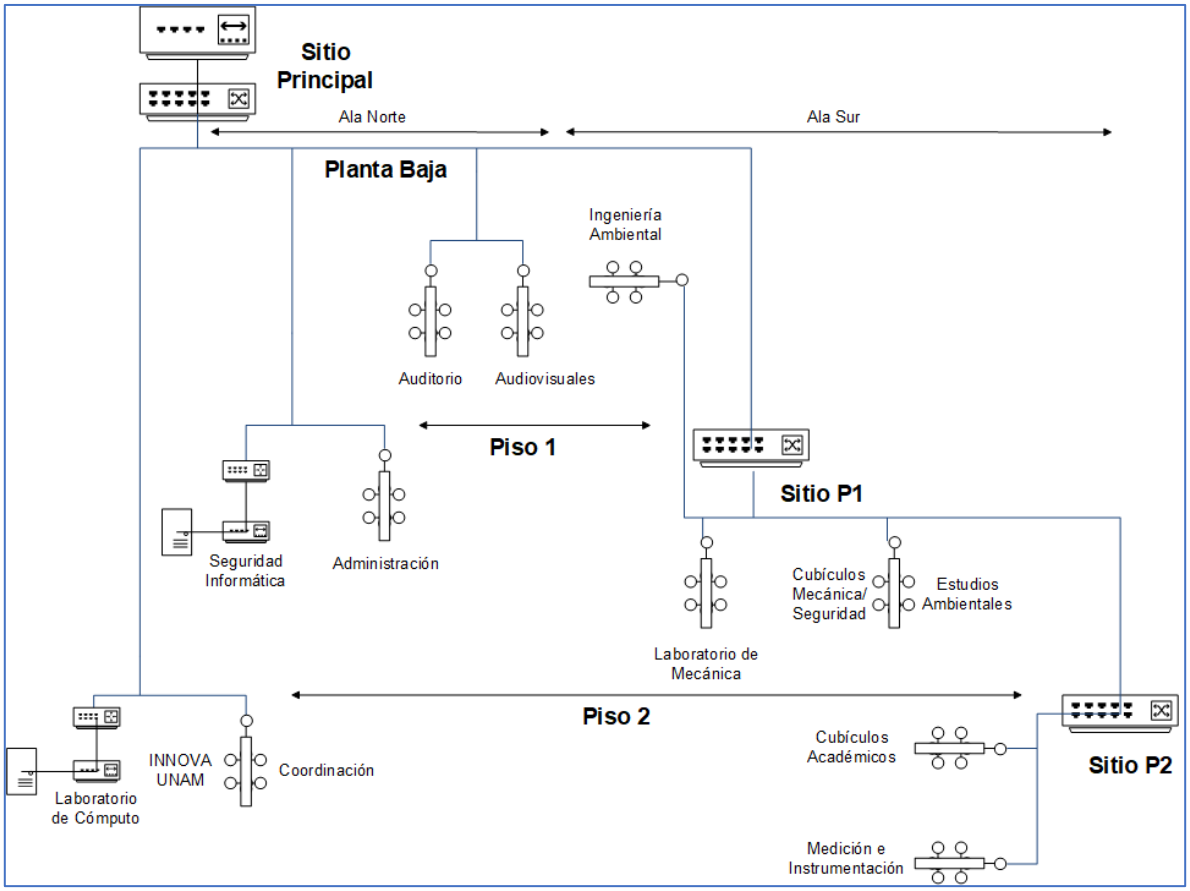


Imagen 5.1. Topografía Actual. [A24]

Como resultado del levantamiento de la presente topología, se detectaron áreas de oportunidad las cuáles se plantea aprovechar para mejorar el diseño físico, a través de las **Propuestas A** y **B**.

Para el caso de la **Propuesta A**, se recomienda estructurar la topología con los siguientes elementos:

- Realizar expansión de nodos.
- Integrar un dispositivo Firewall en el sitio principal, delante del Switch principal, en el cual llegará el enlace de Internet, y se establecen las políticas de comunicación y seguridad.
- Instalar dispositivos Router con Access Point para la mayoría de las áreas/laboratorios, con excepción de la oficina principal de la Coordinación, el Auditorio, y alguno de los espacios audiovisuales.

- Establecer un dispositivo Switch, o configurar alguno disponible en el sitio principal, para establecer la Zona Desmilitarizada para la instalación de los servidores de todas las áreas/laboratorios en ese espacio.

Veamos la representación gráfica:

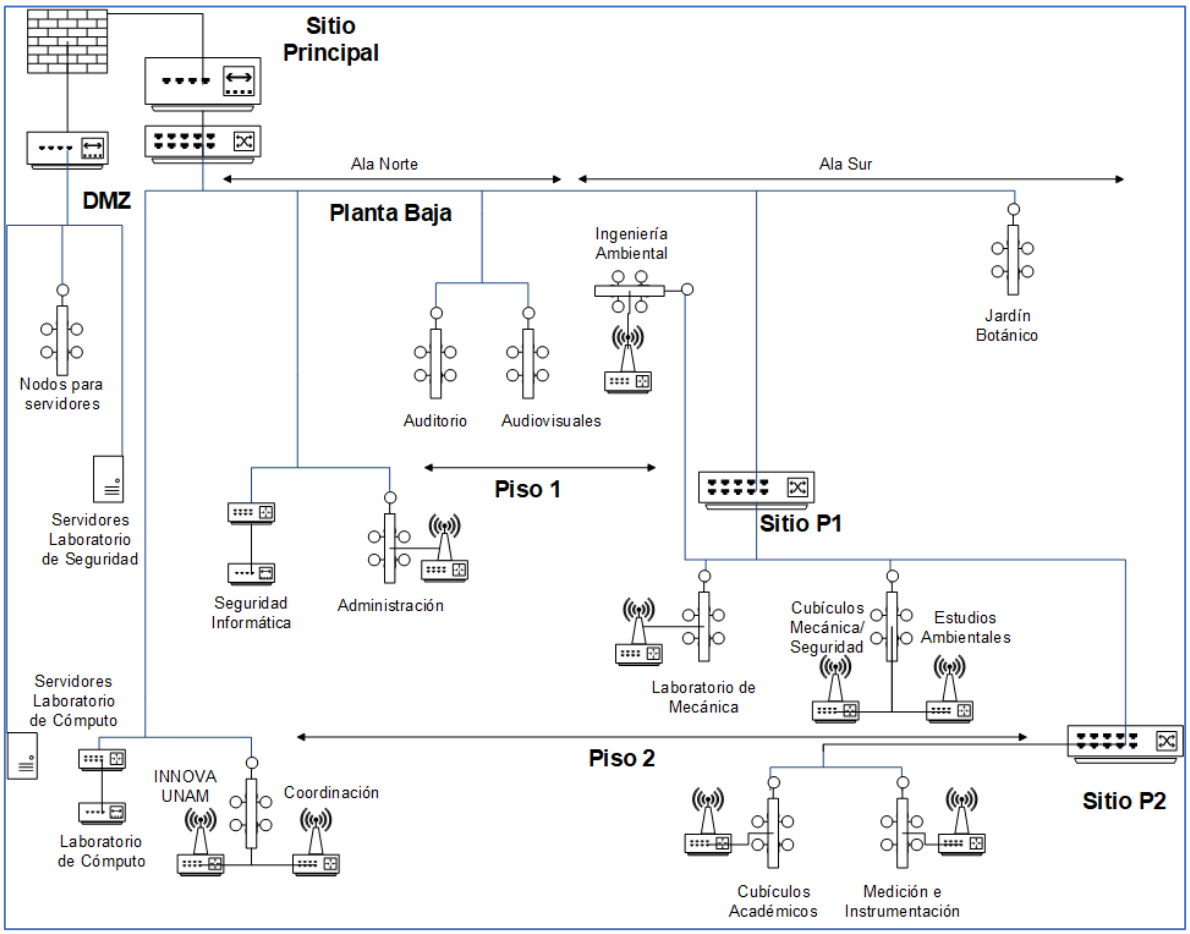


Imagen 5.2. Topología Propuesta A. [A25]

Por otra parte, para la **Propuesta B**, se plantea la siguiente estructura:

- Realizar la expansión de nodos.
- Instalar dispositivos Router con Access Point para la mayoría de las áreas/laboratorios, con excepción de la oficina principal de la Coordinación, el Auditorio, y alguno de los espacios audiovisuales.

Su representación gráfica es de la siguiente manera:

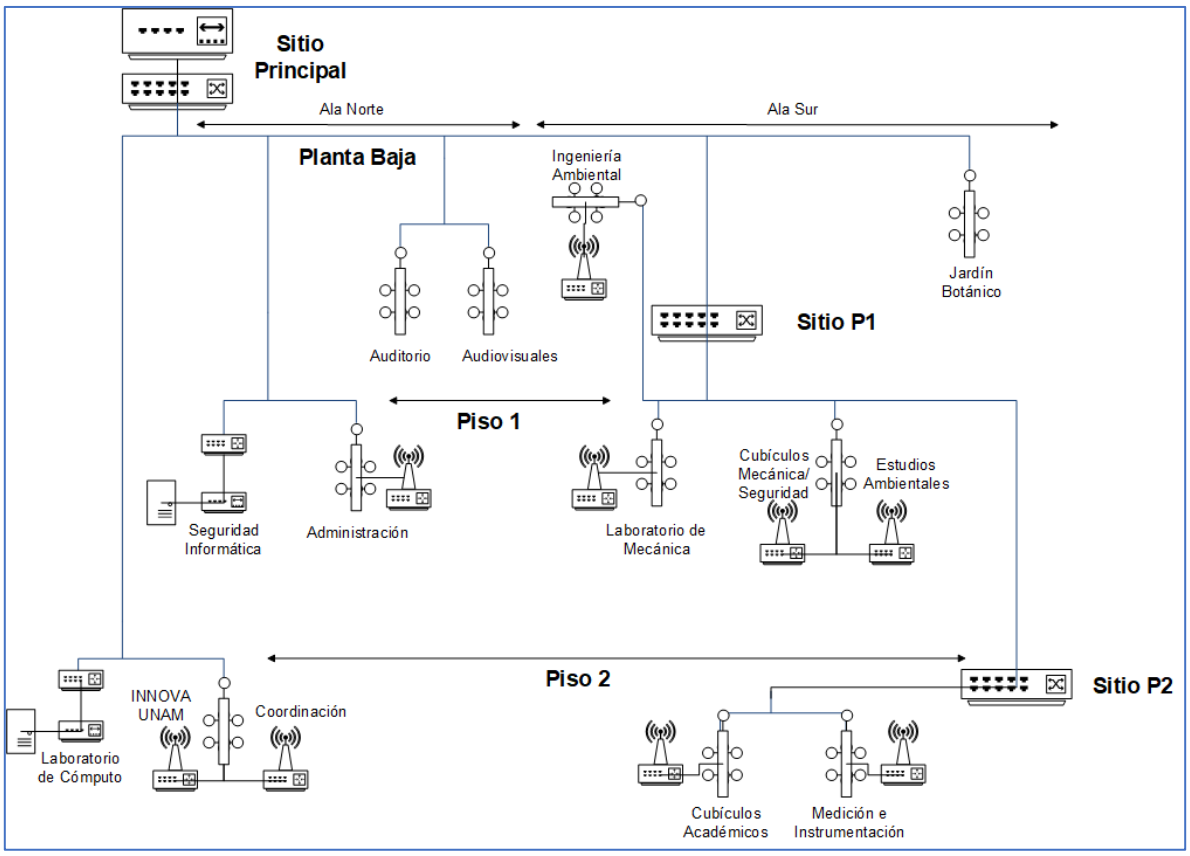


Imagen 5.3. Topología Propuesta B. [A26]

En ambas propuestas se observa la inclusión de dispositivos de red, se presentan de forma general, pasemos al siguiente tema dónde se revisa con mayor detalle los dispositivos que se proponen.

5.1.2. Dispositivos de Red.

En el caso particular de la **Propuesta A**, el dispositivo clave a incluir es un Firewall *Fortigate Serie 60E* en su versión básica, el dispositivo cuenta con un sistema operativo para su administración, el dispositivo luce de la siguiente forma:

Figura 5.1. Fortigate 60E frente. [B16]

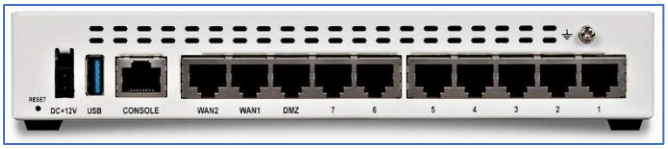


Figura 5.2. Fortigate 60E puertos. [B17]

Físicamente cuenta con:

- 7 puertos Gigabit Ethernet, para conexiones mayores a 100 Mbps.
- 1 puerto dedicado para Zona Desmilitarizada (DMZ).
- 2 puertos WAN para la salida a Internet, permitiendo tener 2 Proveedores de Servicios de Internet (ISP), ofreciendo flexibilidad en combinar los servicios, para evitar problemas de conectividad.
- 1 puerto de consola para administración sin interfaz gráfica.
- 1 puerto USB para conexión de dispositivos externos como almacenamiento, o impresora compartida para la red.

Respecto a características lógicas generales, el dispositivo ofrece lo siguiente[53]:

- Detecta ataques dirigidos, mitigando de forma automática la detención de los ataques.
- Ofrece capacidades de enrutamiento, conmutación, servicio VPN, servicio de Virtual IP para políticas de seguridad con direccionamiento público.
- Permite establecer políticas de seguridad o comunicación flexibles a las necesidades de la organización.
- Interfaz de usuario simple e intuitiva.

Otra particularidad en la **Propuesta A**, es la posibilidad de incluir un Switch dedicado para la Zona Desmilitarizada (DMZ), dicho dispositivo basta que pueda suministrar nodos para las áreas interesadas en instalar servidores, por lo que uno de carácter plug & play es suficiente para cubrir la proyección.

[53] Quanti. (2018). FortiGate 60E Datos técnicos. febrero, 7, 2019, de Solutions S.A. de C.V. Sitio web: https://www.quanti.com.mx/fortigate-60e-datos-tecnicos/

El modelo que se propone es un *TP-LINK TL-SG1024D*, el cual cuenta con 24 puertos, físicamente luce de la siguiente manera:

Figura 5.3. TP-LINK TL-SG1024D. [B18]

Al ser un dispositivo de tipo Plug & Play, solo se necesita suministrarle energía eléctrica, y las conexiones de red necesarias hacia los nodos que vayan a ser dedicados a servidores.

Sin embargo, pese a que se puede omitir este dispositivo, debido a que se pueden configurar algunos puertos de los switch, es mejor considerarlo para aislar la DMZ del resto de la infraestructura. Se propone uno no administrable debido a que no es necesario configurar VLAN en la DMZ.

Ahora de forma general, para **ambas** propuestas, se propone incluir Routers con Access Point integrados, con el objetivo de lograr expansión en las redes privadas de cada área/laboratorio, ya que se toma en consideración que algunos miembros de las áreas/laboratorios cuentan con varios dispositivos electrónicos, entonces el adoptar esos routers facilitará algunas tareas o proyectos que requieren conectividad compartida.

Entonces, con base en lo anterior, los routers a proponer son los *TP-LINK TL-WR840N*, los cuales físicamente lucen como sigue:

Figura 5.4. Router con Access Point. [B19]

Figura 5.5. Router con Access Point puertos. [B20]

Estos dispositivos ofrecen las siguientes características físicas y lógicas:

- 1 puerto WAN, para establecer la salida a Internet.
- 4 puertos Fast Ethernet, para conectividad alámbrica hasta 100 Mbps.
- Alcance de radio de 2.4 Ghz para conectividad inalámbrica.
- Posibilidad de limitar el ancho de banda.
- Instalación de una red de invitados, la cual separa la red inalámbrica/alámbrica principal.
- Establecer políticas elementales de seguridad para redes inalámbricas.

Finalmente, se considera prioridad la adquisición de *Fuentes de Alimentación Continua*, tanto para el sitio principal, como para los sitios de los pisos 1 y 2, para la protección eléctrica de los dispositivos, evitando fallas de los equipos por cortes de energía inesperados.

El dispositivo por sugerir es la *Fuente de Alimentación APC Back-UPS BR1300G*, físicamente tiene el siguiente aspecto:

Figura 5.6. Fuente APC. [B21]

La fuente ofrece las siguientes características:

- Puertos dedicados a protección de energía con batería de reserva.
- Puertos regulados para evitar cambios drásticos de energía.
- Puertos Gigabit Ethernet, para la protección de dispositivos electrónicos conectados con esa interfaz.
- Pantalla led para mostrar estado del dispositivo.
- Alarma para indicar problemas que tenga el dispositivo en su operación.

5.1.3. Cableado Estructurado.

Partamos con proponer una expansión de nodos, mismos que contendrán un cableado estructurado nuevo, asegurando calidad en las conexiones, alargando la vida útil de las vías de comunicación.

Es importante destacar que en este punto existe la flexibilidad los dos tipos de propuesta, debido a que en los dos casos se considera necesario extender los nodos existentes para todas las áreas/laboratorios.

Para las **Propuestas A** y **B**, la siguiente tabla sugiere reorganizar los nodos de la siguiente manera:

Área/Laboratorio	Nodos Actuales	➔ Nodos con Expansión
Ingeniería Ambiental	4	➔ 6
Ingeniería Mecánica	4	➔ 6
Medición e Instrumentación	4	➔ 7
Estudios Ambientales	4	➔ 6
Seguridad Informática	4	➔ 6
Cómputo	6	➔ 9
INNOVA UNAM	3	➔ 4
Jardín Botánico	0	➔ 2
Auditorio y Espacios Audiovisuales	4	➔ 6
Administración	4	➔ 6
Coordinación	3	➔ 4

Tabla 5.1. Lista de nodos con expansión. [TA4]

Gráficamente organizados de la siguiente manera:

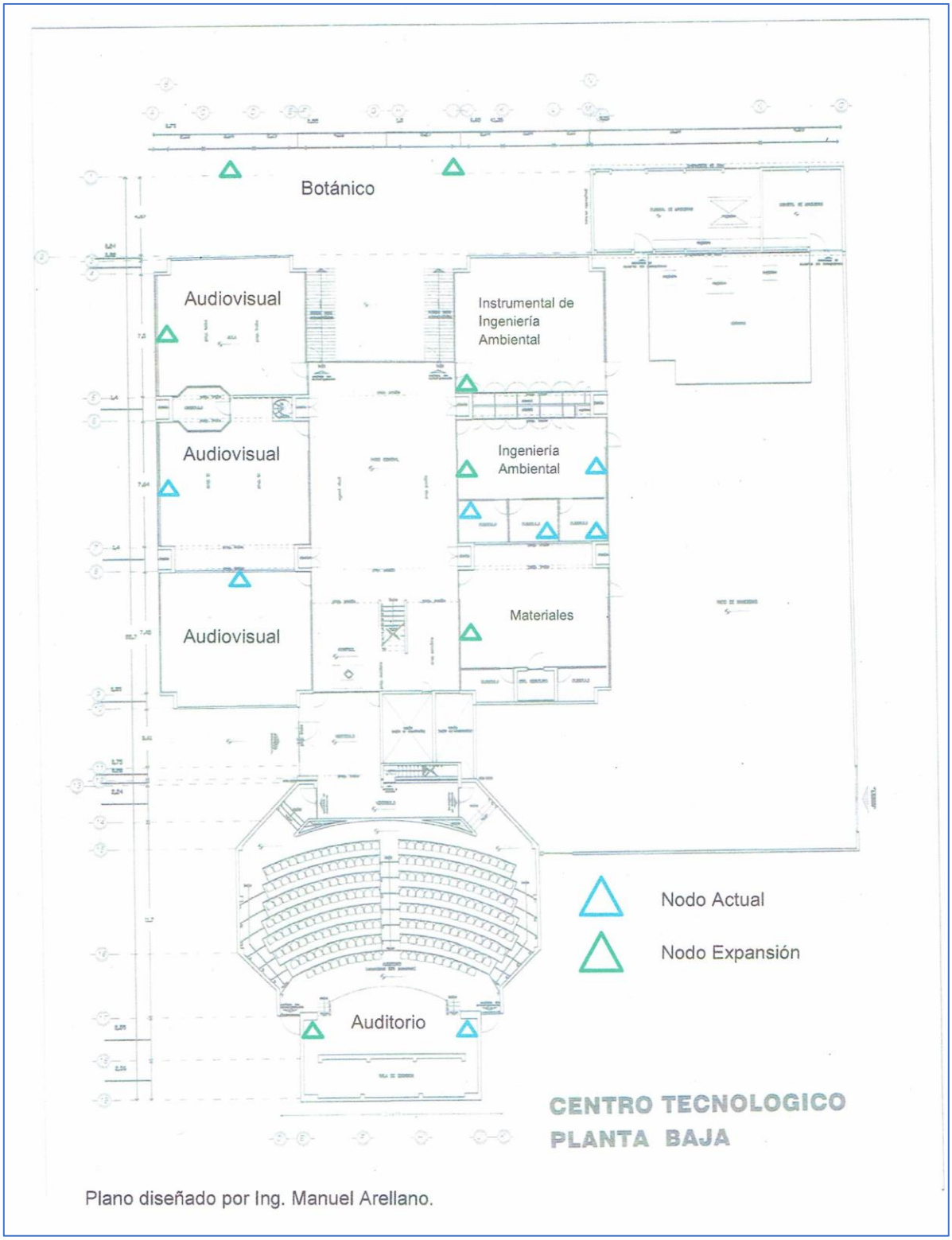


Imagen 5.4. Planta Baja. [A27]

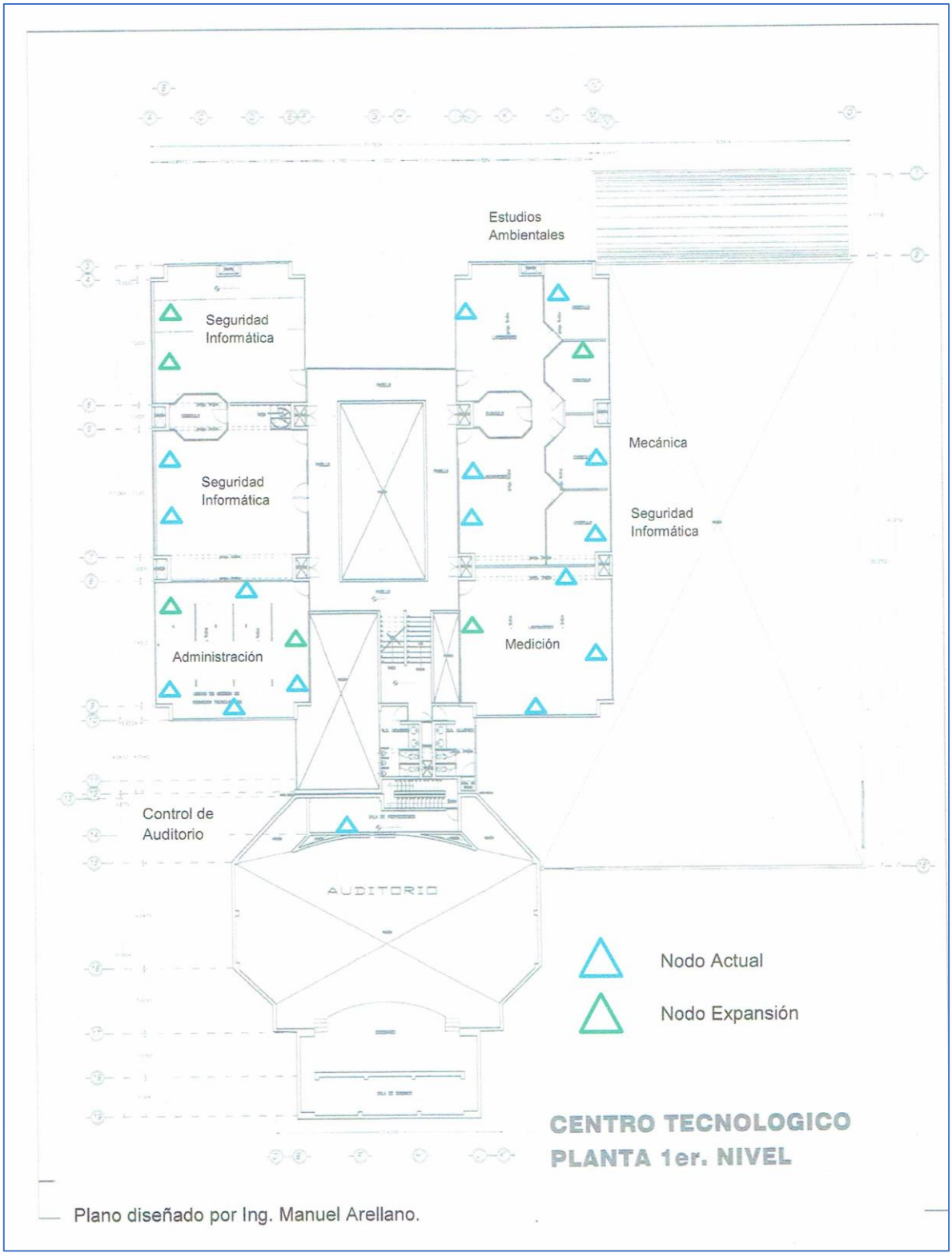


Imagen 5.5. Primer Piso. [A28]

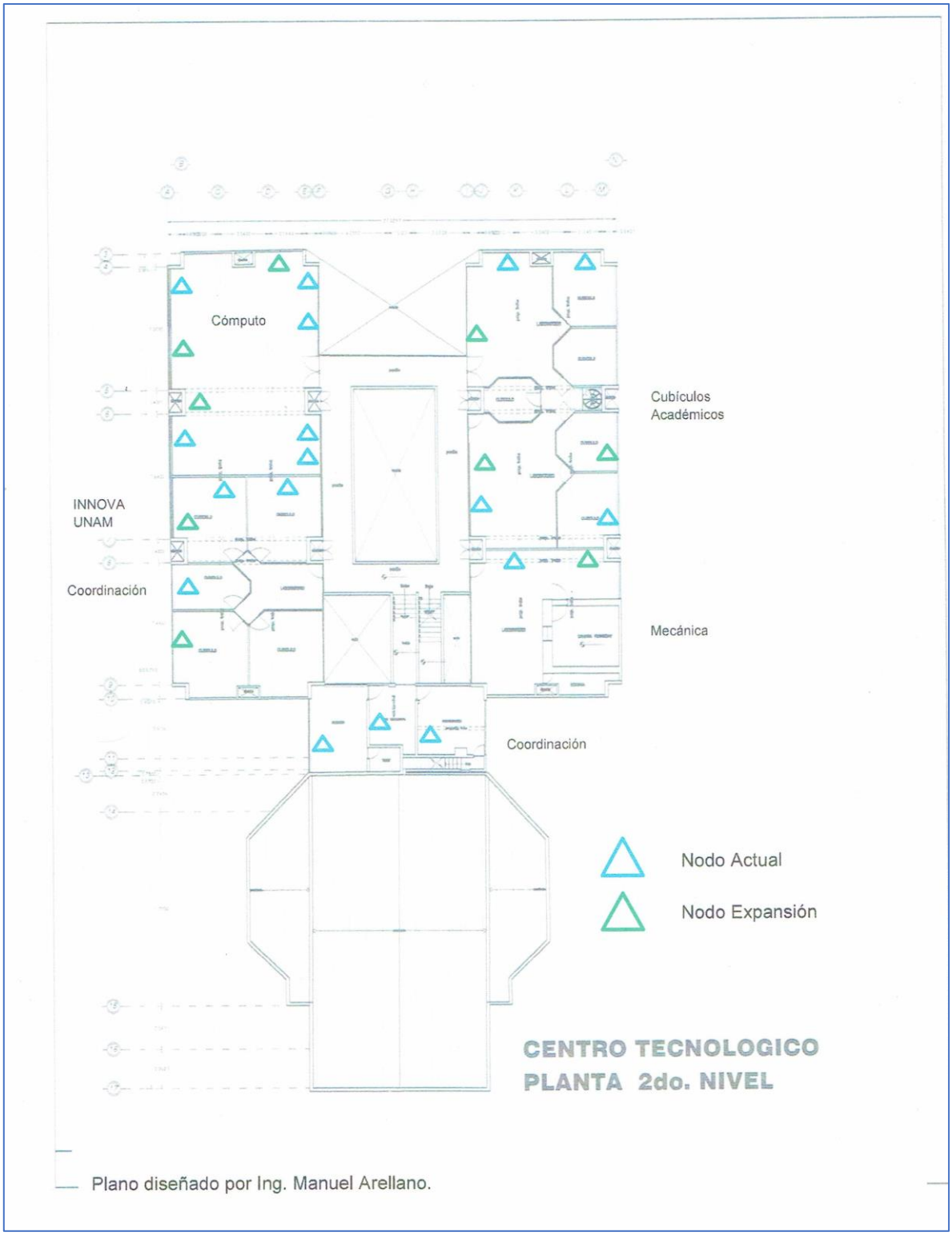


Imagen 5.6. Segundo Piso. [A29]

El tipo de cable a proponer para cubrir esta característica es un *Cable UTP Categoría 6*, el cuál podemos encontrar en el mercado con la siguiente forma física:

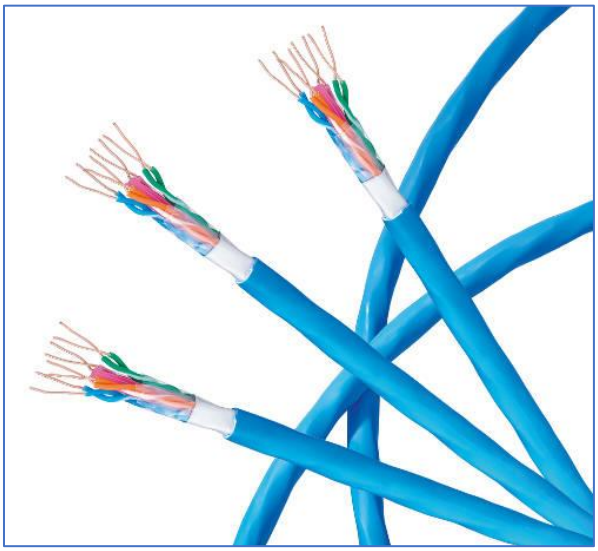


Figura 5.7. Cable UTP Cat-6. [B22]

Se elige este cable debido a que cuenta con las siguientes cualidades:

- Recubrimiento plastificado de alta densidad, dotando de flexibilidad en su manejo.
- Doble forro interno, uno de ellos de aluminio, para ampliar sus capacidades conductoras, otorgando estabilidad para largas distancias.
- Tiras de cobre de mayor densidad, para facilitar el ensamblaje con los conectores RJ-45.
- Alcanza velocidades de hasta 10 Gbps.

Tanto el cable como la distribución propuesta son el complemento adecuado al nuevo diseño que se puede alcanzar, hasta aquí se proponen elementos en su mayoría físicos, ahora pasemos a las primeras propuestas de funcionamiento.

5.2. Actualización de Funcionamiento.

En este apartado se sugieren algunas ideas de actualización de funcionamiento de la red, esto es a nivel lógico, se hace énfasis en que, a partir de este punto las ideas

presentadas aplican en mayor medida para la **Propuesta A**, la razón es la flexibilidad en las configuraciones que el *Firewall* planteado previamente ofrece.

Los puntos por tratar en este tema son la segmentación de la red en VLAN por área/laboratorio, la revisión de los tipos de direccionamiento público y privado, añadiendo una comparativa de ventajas y desventajas entre los tipos de direccionamiento, además de ideas de configuración generales para los Router con Access Point planteados en el apartado anterior.

5.2.1. Red Interna segmentada en VLAN.

Es importante aclarar que el siguiente planteamiento solo es posible dentro de la **Propuesta A**, en el caso de la **Propuesta B** como se prescinde del Firewall complica establecer direccionamiento para las VLAN, no obstante, más adelante se mencionarán algunas configuraciones aplicables en ambas propuestas.

Se propone segmentar la red en VLAN por área/laboratorio, el propósito de distribuir la red de esa manera es encapsular el transporte de información, disminuyendo el tráfico innecesario en la infraestructura. También se "etiqueta" de manera lógica a cada área/laboratorio, permitiendo identificar el tráfico generado, esto es particularmente útil para los miembros del Laboratorio de Seguridad Informática.

Otro objetivo de organizar la red en VLAN es la flexibilidad de colocar equipos fuera de su espacio designado, actualmente ya ocurre que el área de Coordinación tuvo que ocupar otro espacio físico para sus miembros de trabajo, no obstante, se ignora que dispositivos pertenecen a esa área.

La siguiente tabla propone las jerarquías VLAN para cada área/laboratorio:

Área/Laboratorio	VLAN
Coordinación	10
Administración	20
Laboratorio de Cómputo	30
Laboratorio de Seguridad Informática	40

INNOVA UNAM	50
Medición, Instrumentación y Control	60
Ingeniería Mecánica	70
Estudios Ambientales	80
Ingeniería Ambiental	90
Auditorio y Espacios Audiovisuales	100
Jardín Botánico	110
Administrador de Red	200

Tabla 5.2. Jerarquía de VLAN. [TA5]

Gráficamente la distribución queda etiquetada de la siguiente manera:

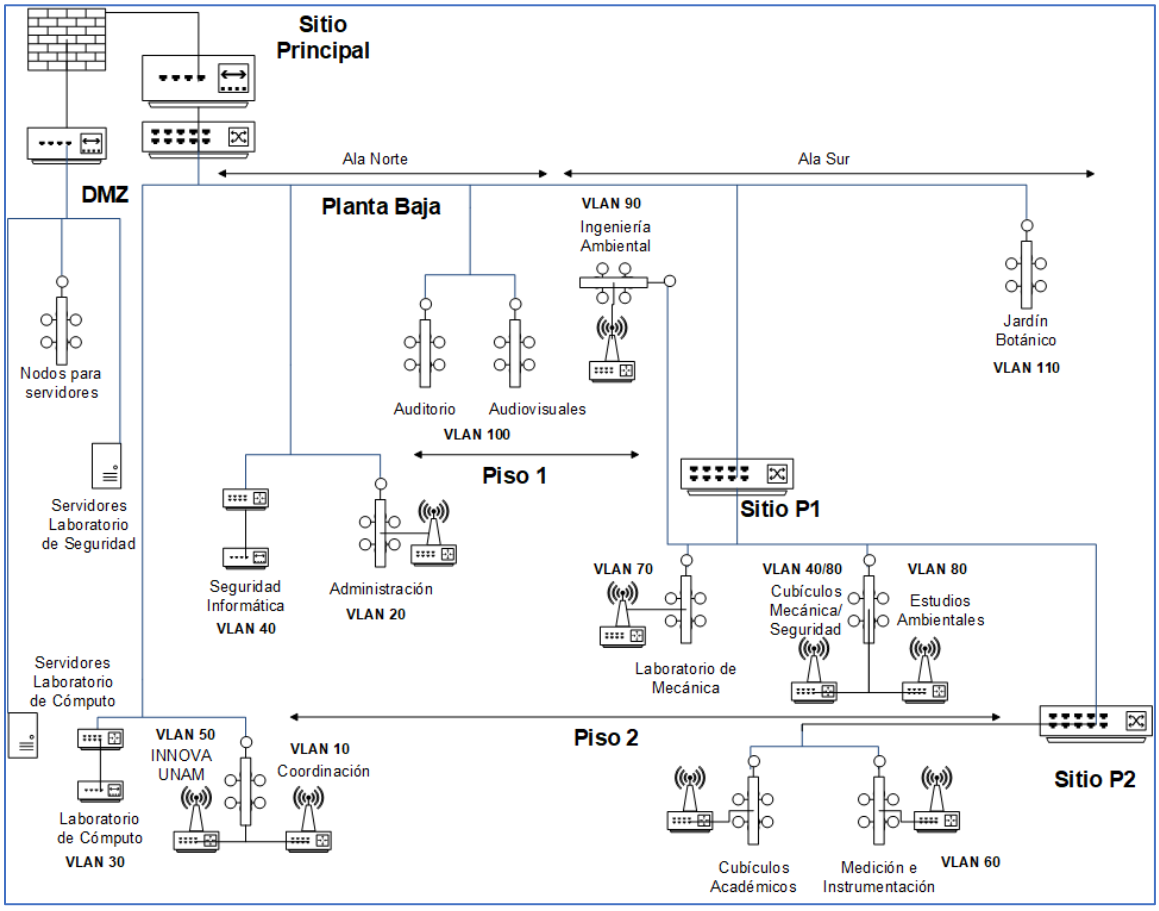


Imagen 5.7. VLAN en Topología A. [A30]

La distribución necesita que los nodos físicos estén etiquetados, esto es, se tenga certeza de las áreas a las que pertenecen, la intención es facilitar la configuración lógica en los dispositivos, con ello se puede establecer un direccionamiento preciso para las áreas/laboratorios.

5.2.2. Direccionamiento.

Antes de ver las propuestas en materia de direccionamiento, primero revisemos algunos conceptos generales de direccionamiento, los tipos existentes: **Direccionamiento Público** y **Direccionamiento Privado**. Sumado a lo anterior, revisaremos sus características, ventajas, desventajas de cada tipo, y posteriormente se pasará a revisar las ideas a plantear en las **Propuestas A** y **B**.

Comencemos viendo la constitución de una dirección **IP** en su **Versión 4** con la siguiente figura 5.8:

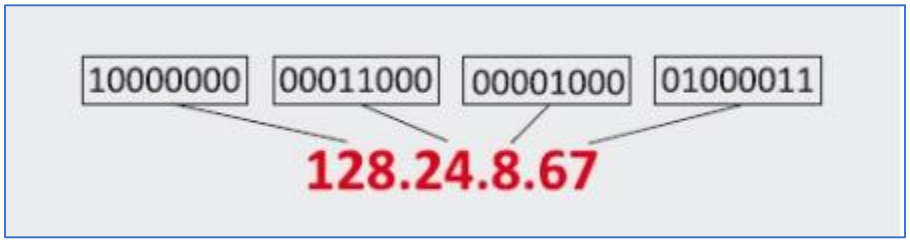


Figura 5.8. Dirección IP en notaciones Binaria y Decimal. [B23]

Podemos ver que las notaciones guardan una relación estrecha, puesto que son valores equivalentes entre una y otra, por tanto, los valores máximos en sus intervalos van de 00000000 a 11111111 (0 a 255), exceptuando en el último valor (ubicado en el extremo derecho). El diseño comprende 4 octetos de bits (32 bits en total[54]), los cuales en su momento se les considero suficientes para cubrir las comunicaciones. No obstante, ese planteamiento se empieza a ver superado por el número de redes y dispositivos existentes en la infraestructura de internet.

[54] En la concepción de diseño existían limitaciones físicas (circuitos) por eso se estableció ese límite.

Actualmente se planteó el diseño de un direccionamiento **IP Versión 6**, en el cual la notación pasa a ser hexadecimal, expandiendo drásticamente la cantidad de redes y dispositivos que puedan conectarse.

Ahora revisemos las clases de direccionamiento **IPV4** existentes en general con la siguiente tabla[55]:

Clase	Rango de Direcciones	Número de Redes	Número de direcciones por Red
A	1.x.x.x – 126.x.x.x[56]	$2^7 - 2 = 126$*	$2^{24} - 2$* = 16,777,214
B	128.x.x.x – 191.x.x.x	2^{14} = 16,384	$2^{16} - 2$* = 65,534
C	192.x.x.x – 223.x.x.x	2^{21} = 2,097,152	$2^8 - 2$* = 254

Tabla 5.3. Clases de direccionamiento IPV4. [TA6]

En la Clase A existen 2 direcciones reservadas la 0.x.x.x y 127.x.x.x las cuales se utilizan para realizar pruebas, en el caso particular de la 127.x.x.x funge como dirección "local", los routers envían los paquetes del dispositivo hacia él mismo creando un bucle. Se dice que es de prueba, porque se pueden testear el comportamiento de algunos servicios que se deseen proveer, previo a darles salida a Internet.[57]

El resto de las direcciones en la Clase A se utilizan comúnmente para establecer nexos muy lejanos, por ello el número de redes a establecer es limitado.

Las direcciones de la Clase B su uso común es para las Redes de Área Amplia (Wide Area Network – WAN), esto es la interconexión de ciudades de un país, o de unidades de una gran industria.

[55] Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 101.
[56] Entiéndase **x** como un número comprendido en intervalo de 0 a 255, excepto en el último valor (extremo derecho véase la Figura 5.8) donde el intervalo es de 1 a 254, en ese valor se le está pidiendo un valor al inicio 00000001 y cuando se llega al final ya está en 11111111 entonces por diseño no se puede superar ese valor, por ese motivo el último valor cuenta con esa particularidad.
[57] Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P. 113.

Y las direcciones de la Clase C se utiliza mayormente para las Redes de Área Local (LAN) siendo de carácter privado, para espacios industriales, académicos o empresariales, no obstante, es posible utilizar esta clase de direccionamiento para redes WAN en los casos en que se requiera un número limitado de nodos.

Respecto al número de nodos disponibles por red, se destaca el descuento de 2^{58} direcciones, las cuales corresponden al ID de red (para difusión) y a la puerta de enlace (Gateway), una sirve para conocer el destino, mientras que la otra sirve como salida para la información.

En la *Tabla 5.3* se puede notar el alcance de redes a establecer, el número de dispositivos a cubrir dependiendo el tipo de red a diseñar o implementar, entonces aquí se ve una primera diferencia entre los tipos de direccionamiento, en el **direccionamiento público** tiene un alcance muy amplio, mientras que en el **direccionamiento privado** ocurre lo inverso, su distancia se limita al espacio de trabajo (industria, empresa o escuela) donde se haya establecido la red.

Dicho lo anterior pasemos a revisar algunas características del **direccionamiento público**:

Características del Direccionamiento Público

- Son direcciones de Clases A o B comúnmente, dependiendo la distancia a cubrir, en casos particulares adaptan la Clase C.
- Puede tener Dirección Fija (utilizada principalmente para servidores) o Dinámica (donde la dirección cambia en un tiempo determinado), depende del servicio a contratar a un ISP.
- El uso común de este tipo de direcciones es establecer servicios como páginas web, correo electrónico, almacenar archivos, e-commerce, entretenimiento multimedia.
- Se puede acceder a servicios alojados (privados o públicos) a través de Internet.

[58] Por ello en la Tabla 5.3 en la columna de Número de direcciones se restan 2 al valor total.

- Las direcciones fijas poseen un costo elevado, debido a que el ISP contratado reserva la dirección, notificando a la **IANA** (Internet Assigned Numbers Authority – Autoridad de Asignación de Números de Internet) la reservación.

La principal **desventaja** de este tipo de direccionamiento es en materia de seguridad, ya que como son de acceso público, suele estar expuesto a atacantes; entonces si algún dispositivo está detrás de ese tipo de dirección y no cuenta con controles para mitigar amenazas, puede quedar comprometido ante los atacantes.

Por otra parte, el **direccionamiento privado** frecuentemente suele utilizar direcciones de la Clase C, además de emplear **NAT** en los casos que se desee traducir de un tipo de dirección público a uno privado.

Mencionemos algunas características de este tipo de direccionamiento:

Características del Direccionamiento Privado

- Usualmente son direcciones de Clase C.
- Contienen pocos nodos.
- Su mayor uso es para establecer Redes LAN.
- Se pueden establecer servicios para consumo interno.
- Los recursos compartidos son para uso interno.
- Pueden tener salida a Internet a través de un enlace WAN.

Entre algunas **desventajas** de este tipo de direccionamiento encontramos:

- Los servidores no son para el acceso o consumo público.
- Limitación de acceso a recursos privados.
- Limitaciones para algunas herramientas de software de propósito específico.

Sin embargo, en materia de seguridad, hace más complicado la perpetración de ataques en este tipo de direcciones, debido al encapsulamiento de los dispositivos detrás de este tipo de red.

Planteamientos para Propuestas A y B

Ahora bien, para la **Propuesta A**, se sugiere utilizar direccionamiento público directo para el caso de los servidores alojados dentro de las áreas/laboratorios, ubicados dentro de la **DMZ**.

Para casos ajenos a servidores se sugiere adoptar un direccionamiento privado, con la particularidad de configurar **IP Pool** (Grupo de Direcciones IP) dentro del Firewall, para traducir directamente de direcciones privadas hacia direcciones públicas (direccionamiento público indirecto) con medidas de seguridad, en los casos en que se necesite el acceso remoto a algún dispositivo o recurso, sin necesidad de uso de software de terceros.

Con base en lo anterior, se sugiere la siguiente tabla de direcciones para las áreas/laboratorios:

Área/Laboratorio	ID de Red	Gateway
Coordinación	200.128.10.0	200.128.10.64
Administración	200.128.20.0	200.128.20.64
Laboratorio de Cómputo	200.128.30.0	200.128.30.128
Seguridad Informática	200.128.40.0	200.128.40.128
INNOVA UNAM	200.128.50.0	200.128.50.32
Medición, Instrumentación y Control	200.128.60.0	200.128.60.64
Ingeniería Mecánica	200.128.70.0	200.128.70.64
Estudios Ambientales	200.128.80.0	200.128.80.64
Ingeniería Ambiental	200.128.90.0	200.128.90.64
Auditorio y Espacios Audiovisuales	200.128.100.0	200.128.100.128
Jardín Botánico	200.128.110.0	200.128.110.32

Tabla 5.4. Direccionamiento CTA. [TA7]

Podemos observar que los ID de Red propuestos forman parte de la Clase C no privada, utilizando rangos poco convencionales como medida de seguridad, puesto que existen rangos comunes establecidos (192.168…), esto se considera así para

facilitar la configuración de IP Pool que más adelante se mencionará. Además de adoptar las etiquetas propuestas para las VLAN planteadas previamente en el tercer octeto de la dirección.

También se puede observar que el Gateway establece un número implícito sugerido de dispositivos a conectar, con la intención de limitar el acceso a dispositivos.

En el caso de la **Propuesta B**, se puede adaptar la *Tabla 5.4.* para los Router con Access Point propuestos para cada área/laboratorio, no obstante, solo limitaría a extender la red a dispositivos para los usuarios del área/laboratorio, dejando de lado características de seguridad.

Hasta aquí se plantean las ideas conceptuales, pasemos a aterrizar algunas de las ideas propuestas, dándoles forma en las interfaces de configuración de los dispositivos, el siguiente apartado comenzará a abordar la materialización de las ideas.

5.2.3. Configuraciones Iniciales en Dispositivos de Red y Seguridad.

En este apartado se realiza la configuración en los dispositivos de red proyectados, comencemos preparando los elementos para la **Propuesta A**.

Firewall

Pasemos con las configuraciones iniciales para el Firewall, previamente se presentó el modelo Fortigate 60E, para llevar a cabo la implementación de las ideas propuestas, el dispositivo cuenta con una interfaz web intuitiva.

Es importante señalar que las siguientes ilustraciones mostradas se toman de un modelo superior el **FortiGate 200D**, sin embargo, los dispositivos de Fortinet presentan una interfaz homogénea, la diferencia viene en algunas características, en ese sentido, ambos modelos cuentan con los mismos atributos anteriormente propuestos, no habrá problemas de precisión en ese sentido.

Comencemos con las configuraciones iniciales del Firewall recién tomado del embalaje, existen varias maneras de ingresar a la interfaz gráfica de usuario GUI (o Sistema Operativo):

- Interfaz Ethernet, ya sea por puerto de Administración (Management), o por puerto de Consola (Console) usando una Computadora con Sistemas Windows, Linux, Mac OS X.
- Interfaz USB, para administrar mediante una Computadora con Sistemas Operativos Windows o Mac OS X, o un dispositivo móvil con Sistema Operativo iOS (iPad, iPhone).

Veamos las configuraciones a través de la interfaz Ethernet:

MGMT/Port1

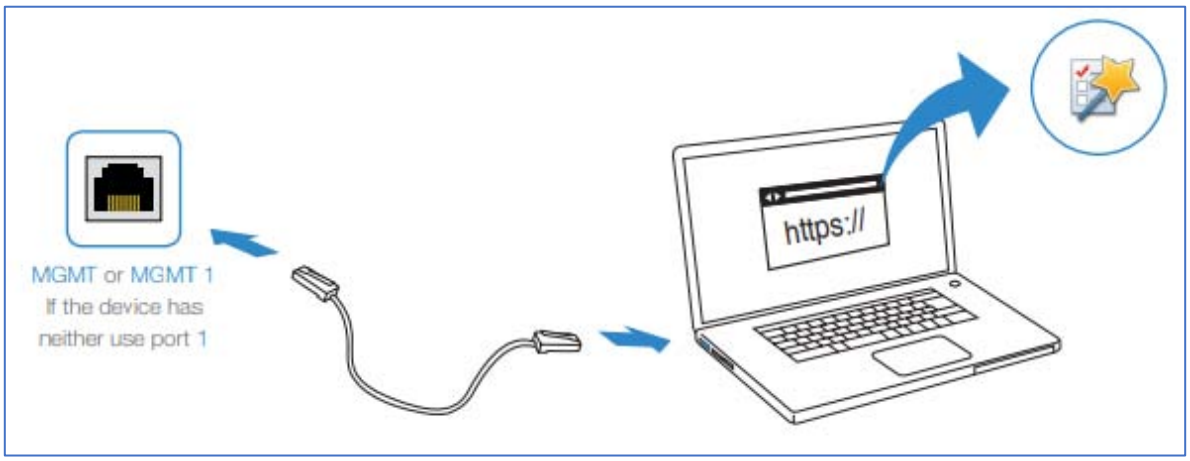


Figura 5.9. Interfaz Ethernet Management. [B24]

El modelo Fortigate 60E no tiene indicado el puerto MGMT1, el puerto 1 cumple con esa función. Para ingresar a la interfaz gráfica se requiere configurar la tarjeta de red de la computadora dentro del mismo segmento de red que viene por defecto dentro del Firewall.

En plataforma **Windows 10** se puede realizar desde el Panel de Control, en el apartado Redes e Internet, eligiendo la opción de Ver el estado y las tareas de red, en Cambiar configuración del adaptador, haciendo clic derecho en la interfaz

Ethernet para seleccionar Propiedades mostrando las siguientes opciones en la ventana:

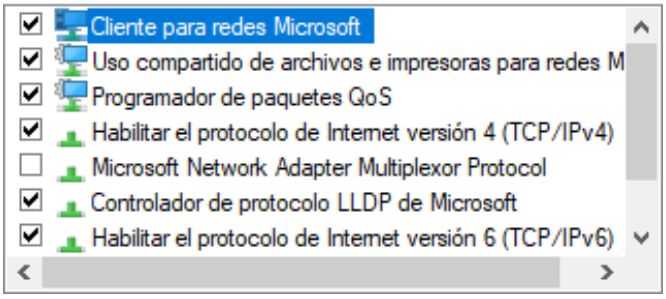


Imagen 5.8. Opciones en interfaz Ethernet. [A31]

Se señala la opción Habilitar el protocolo de Internet versión 4, hacemos clic en el botón Propiedades, para mostrar la siguiente ventana en la cual se colocan los datos mostrados en la imagen:

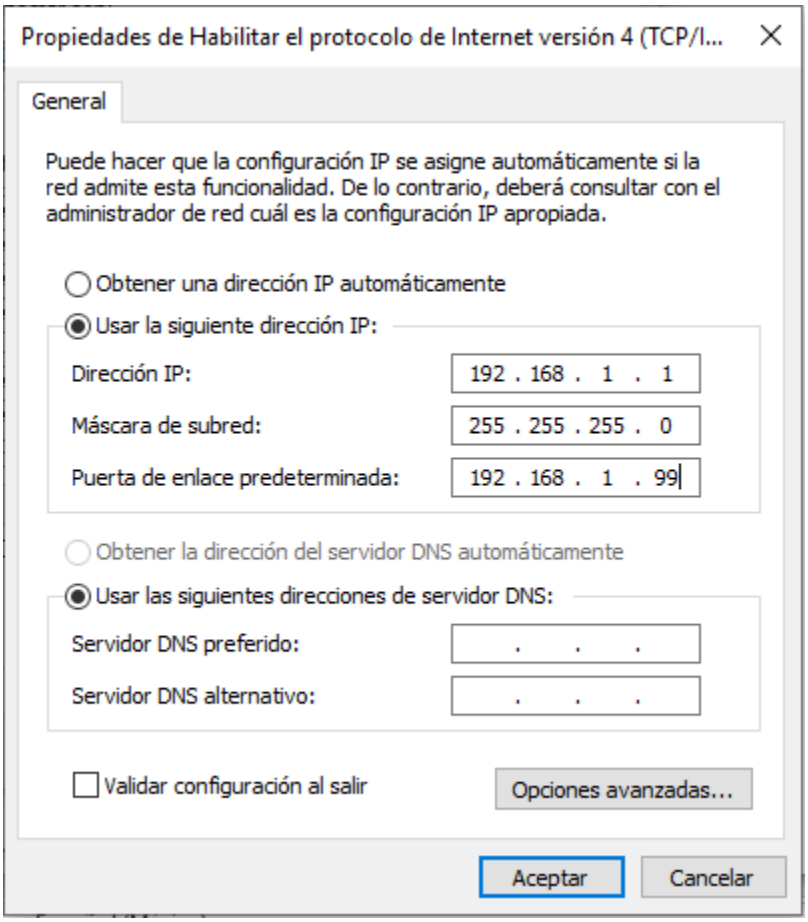


Imagen 5.9. Asignación IP. [A32]

Ahora desde un navegador de Internet, en la barra de direcciones se coloca 192.168.1.99, al indicar que vaya a esa dirección, la interfaz gráfica del Firewall mostrará el espacio para credenciales de inicio de sesión. Por defecto el dispositivo solo cuenta con el usuario **admin** y **no tiene contraseña**, por seguridad se recomienda cambiar esas configuraciones, más adelante se dirán los pasos para realizar ese cambio.

En plataformas **Linux** (con interfaz gráfica) o **Mac OS X**, desde las opciones de Red en su Panel Central de Configuración, se tiene acceso a configuraciones similares a las presentadas en **Windows 10**, se tiene que hacer un proceso análogo para tener acceso a la interfaz del Firewall.

Console Port

Por otra parte, está el puerto Ethernet etiquetado como Console, el cual sirve como otra forma de acceder al Firewall, aunque sin tener acceso a la interfaz gráfica, en su lugar se visualiza una terminal de comandos lineal CLI. La siguiente figura muestra la forma de conectar el dispositivo al puerto:

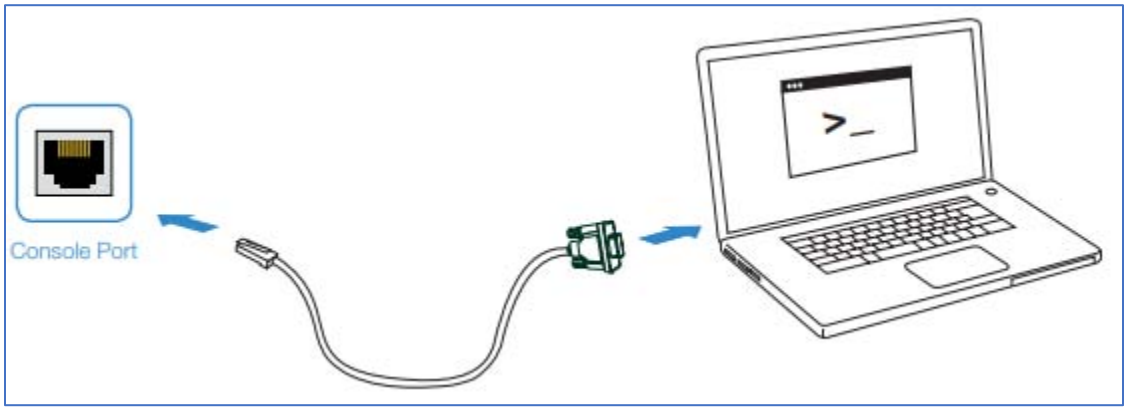


Figura 5.10. Interfaz Console. [B25]

Para acceder por dicho puerto a la interfaz de comandos, se requiere un cable de Ethernet a Serial RS-232 de 9 pines, o un cable de Ethernet a USB, y un software cliente para puerto COM como **PuttY** (emulador de terminal de comandos abierto) en caso de plataforma **Windows 10**, para las plataformas **Linux** o **Mac OS X** se puede acceder desde terminal de comandos incluido en cada sistema.

En cualquiera de los casos se tiene que establecer la siguiente configuración ya sea en el software emulador o en las opciones del controlador Serial COM, para asegurar la conexión[59]:

- **Baud rate**: 9600.
- **Data bits**: 8.
- **Parity**: None.
- **Stop bits**: 1.
- **Flow control**: None.

Una vez realizados los pasos anteriores desde la terminal de comandos, se presiona la tecla Enter del teclado, y en este caso particular la interfaz que muestra es semejante a la siguiente figura:

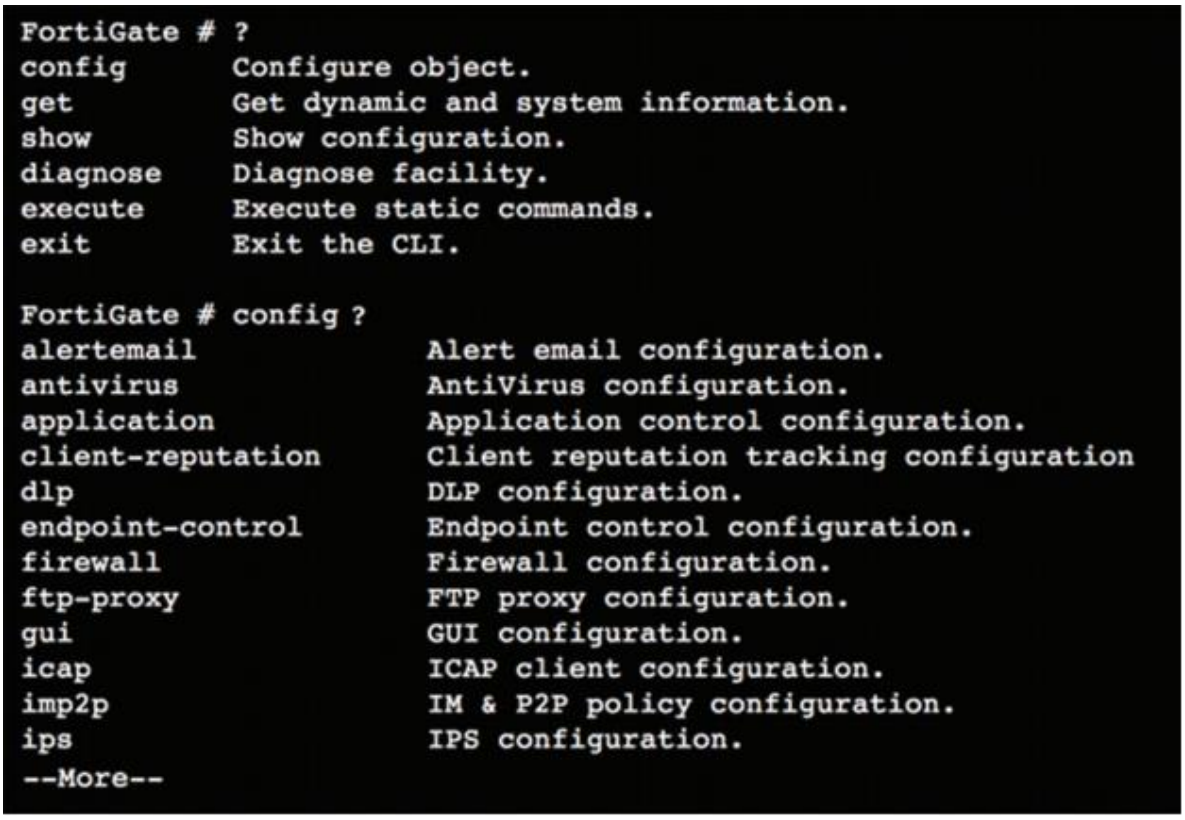


Figura 5.11. Terminal CLI FortiGate. [B26]

[59] Fortinet, Inc. (2018). FortiOS 6.0. agosto 28, 2018, de Fortinet, Inc. Sitio web: http://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortiOS-HTML5-v2/Home.htm

Desde esta interfaz lineal se puede obtener información de los comandos existentes dentro del sistema ingresando el símbolo "**?**" y presionando la tecla Enter después de ingresar el símbolo. Sin embargo, la **Propuesta A** no hará más mención de esta forma de interacción con la interfaz CLI, pero es importante aclarar que todas las configuraciones que se harán más adelante, son posibles de realizar en esta interfaz, para mayor información se puede acceder al siguiente repositorio de documentación para terminal CLI: http://forti.net/cli.

Pasemos ahora a revisar las formas de acceso mediante interfaz USB:

USB MGMT

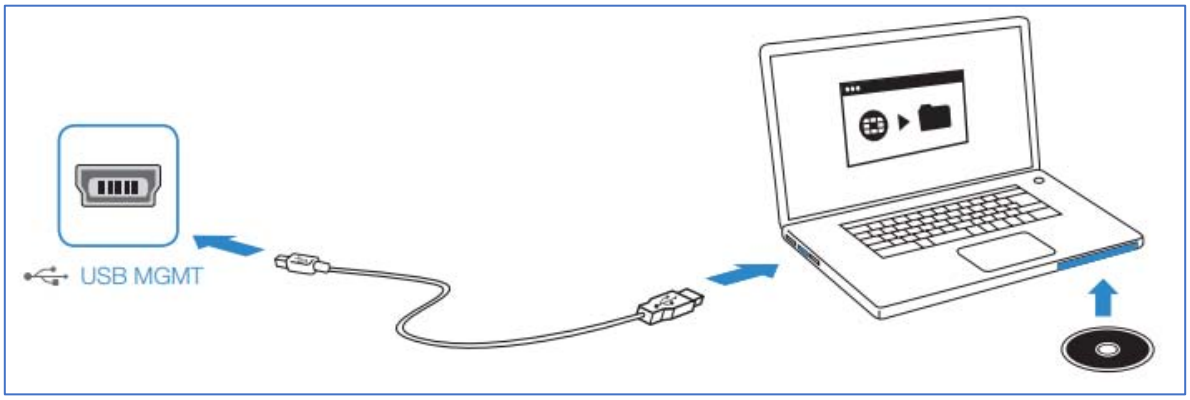


Figura 5.12. USB MGMT. [B27]

El Firewall Fortigate 60E no tiene indicado su puerto USB como Management, no obstante, el puerto funciona de la misma manera, y para tener acceso por este puerto se requiere instalar el software **FortiExplorer**, muchas veces incluido en el embalaje del equipo, es importante señalar que el software solo opera en plataformas **Windows** y **Mac OS X**.

Posterior a instalar el software, de forma análoga a su interfaz gráfica para navegador web, lo primero a mostrar será el espacio para ingresar las credenciales, y de igual manera los datos a ingresar por defecto son usuario **admin** y **sin contraseña**.

Finalmente existe la opción de configurar el Firewall utilizando un dispositivo con Sistema Operativo iOS.

USB con dispositivo iOS

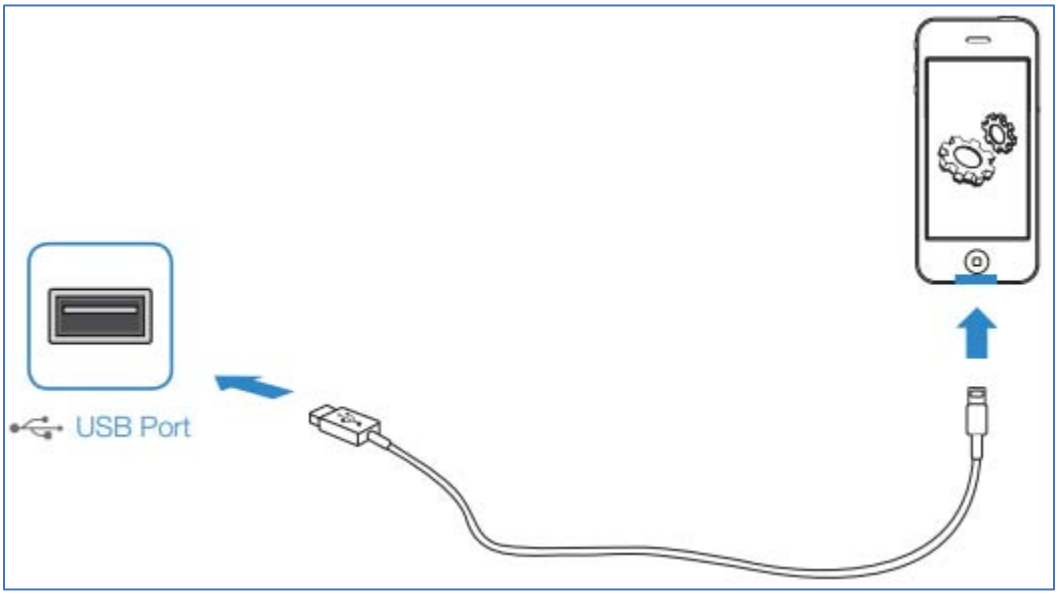


Figura 5.13. USB por iOS. [B28]

Haciendo uso del puerto USB del Firewall, es posible acceder a la interfaz gráfica a través de un dispositivo iOS como iPad o iPhone, para lograr la conectividad es necesario el cable USB incluido con el dispositivo iOS, y la aplicación **FortiExplorer App** disponible en la **AppStore**.

De forma parecida a los casos del navegador web o el software de escritorio FortiExplorer, lo primero a ingresar dentro de la interfaz gráfica son las credenciales, análogamente el usuario por defecto es **admin** y **no se ingresa contraseña**.

Ahora revisemos algunas características generales de la interfaz gráfica de usuario del Firewall.

Características de la Interfaz GUI de FortiGate 60E.

En cualquiera de los casos presentados para el acceso a la interfaz gráfica de usuario, después de ingresar las credenciales, la interfaz muestra un tablero (dashboard) similar al siguiente:

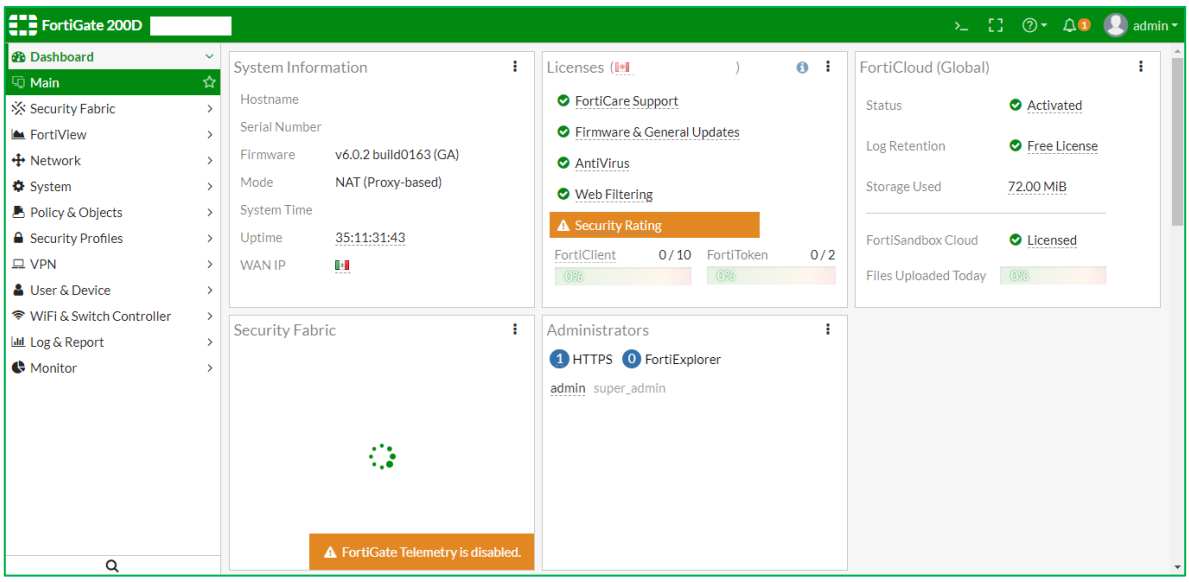


Imagen 5.10. Tablero principal FortiGate. [A33]

En la esquina superior izquierda, se puede notar el modelo en operación y el nombre asignado al dispositivo, en la esquina superior derecha, pueden verse los elementos de apertura de terminal de comandos mediante una subinterfaz (sin salir del tablero principal), un botón para asignar el tamaño con el que se desea mostrar los elementos, un botón de ayuda con preguntas frecuentes, un indicador de alertas por parte del sistema, y un botón de opciones de usuario para cerrar la sesión dentro de la interfaz.

Debajo del número de modelo se encuentran las opciones principales del tablero de operaciones, de nueva cuenta se reitera que el modelo presentado corresponde a la serie FortiGate 200D la cual tiene más características con respecto al modelo 60E una de ellas es Security Fabric, por consiguiente, no se mencionará el contenido de esa característica al verse ausente en del modelo 60E.

Las opciones principales del tablero de operaciones presentan las siguientes funciones generales:

Main

- System Information: Muestra el estado actual del dispositivo.

- Licenses: Muestra el estado de la licencia de uso del Sistema Operativo (interfaz gráfica/consola).
- FortiCloud: Muestra el estado de los servicios en la nube ofrecidos con la licencia de uso.
- Administrators: Muestra las formas activadas de acceso para administración del dispositivo.

FortiView

- Presenta en forma de diagrama la infraestructura que existe delante del Firewall, los dispositivos, sistemas operativos y el tráfico (en Megabytes) generado por cada dispositivo final.

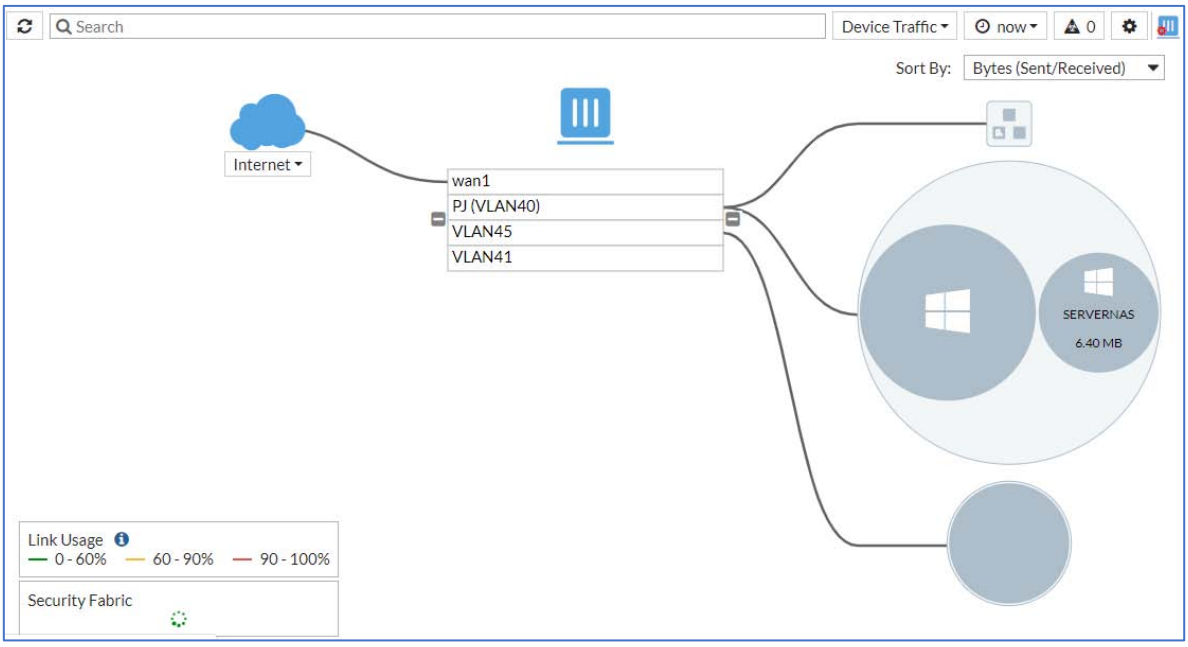


Imagen 5.11. Tablero de FortiView. [A34]

- También tiene la opción de solo mostrar la infraestructura en una tabla con datos similares al diagrama.

Network

- Muestra las interfaces físicas del dispositivo, además de presentar qué puertos se encuentran activos, y que configuración tiene cada puerto.
- Permite mitigar riesgos con servicios DNS.

- Se puede establecer política de “captura” de paquetes dentro del tráfico que viaja por el dispositivo.
- Ofrece la posibilidad de balancear la carga cuando se tenga más de un ISP contratado.
- Cuenta con opciones de configuración de rutas estáticas o dinámicas.
- Tiene opciones para establecer enlaces multicast.

System

En esta opción se tiene que acceder para hacer el **cambio de las credenciales** de administración del dispositivo. Para realizarlo, bajo la opción **Administrators** seleccionamos el botón **Create New**, el cual nos mostrará un formulario para la creación de un usuario administrador:

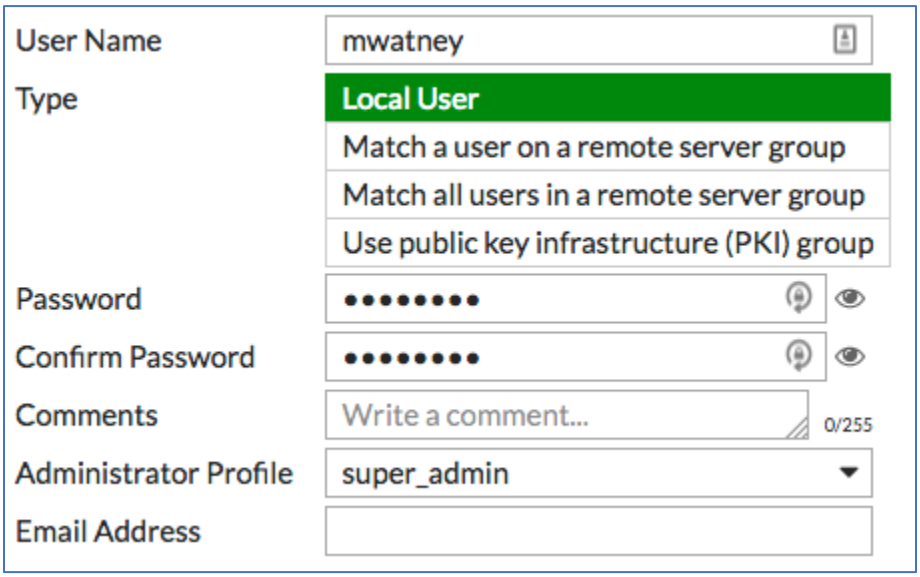


Figura 5.14. Configurando usuario en Firewall. [B29]

Es importante que al crearlo se documenten los datos a ingresar además del perfil que tiene ese usuario, para evitar problemas posteriores al desear hacer cambios, o en casos en que se tengan que reiniciar los dispositivos a sus configuraciones de fábrica.

Además, aquí pueden existir variantes de opciones entre modelos, pero las siguientes características están disponibles para los modelos 200D y 60E:

- Permite la creación de usuarios y perfiles de uso.
- Establece reglas para administración del dispositivo.
- Facilita la actualización del Firmware del dispositivo.
- Pueden instalarse certificados de seguridad específicos.

Policy & Objects

- Se pueden establecer políticas de direccionamiento.
- Políticas de direccionamiento para mitigar Denegación de Servicios (DoS).
- Establecer políticas NAT.
- Establecer políticas para administración de VLAN.
- Establecer rangos de direcciones con propósitos específicos.
- Establecer tareas programadas para políticas.
- Cuenta con opciones para conexiones Proxy.
- Opciones para establecimiento de políticas para servicios dentro de la infraestructura.
- Opciones para establecer políticas de Grupo de Direcciones Virtual (Virtual IP Pool).
- Políticas para control de tráfico mediante Traffic Shapers.

Security Profiles

Permite establecer perfiles de configuración de seguridad, de propósito específico o general, a través de seleccionar opciones de las otras características previamente mencionadas.

VPN

Ofrece opciones de configuración de políticas para servicios VPN, con la posibilidad de crear túneles VPN privados mediante el uso del software **FortiClient** (multiplataforma), siempre y cuando se tenga alguna dirección pública a disposición.

User & Device

Cuenta con configuraciones para el dispositivo, como fecha y hora, opciones para el usuario en su interacción con la interfaz gráfica.

WiFi& Switch Controller

Presenta opciones de configuración para crear una red inalámbrica dentro del Firewall, políticas de seguridad para el acceso inalámbrico. Por otra parte, cuenta con opciones para darles comportamiento de Switch a los puertos Ethernet disponibles en el dispositivo, cuando se trate de una red muy corta.

Log & Report

Esta característica ofrece la posibilidad de monitorear las actividades realizadas en el dispositivo, presenta estadísticas históricas de tráfico, un historial de configuraciones realizadas por los usuarios registrados en el sistema, e incluso un historial de incidentes mitigados, y de igual manera, la posibilidad de reportar errores al fabricante facilitando las políticas de garantía del dispositivo.

Se recomienda estar pendiente de esta característica de forma constante, ya que resulta muy útil al momento de estar controlando incidentes ocurridos dentro de la infraestructura de red. Lo ideal sería revisar esta característica en un espacio de al menos 3 meses, y cuando menos cada 6 o anualmente dependiendo de la actividad realizada por las áreas/laboratorios.

Monitor

Esta característica muestra en tiempo real las actividades que ocurren dentro del dispositivo, el tráfico existente, algunas tareas de las políticas habilitadas. Mediante gráficas o tablas presentadas, con la intención de mitigar incidentes en tiempo real cuando ocurra algún percance.

Por el momento se ha mencionado el acceso al Firewall y se expusieron las características principales del tablero de la interfaz gráfica, ahora bien, pasemos a materializar las configuraciones para VLAN y el direccionamiento propuesto.

Configuraciones para VLAN y Direccionamiento.

Nuevamente se resalta la importancia de realizar el etiquetado físico de los nodos dentro de la infraestructura, para ello nos podemos apoyar de los planos mostrados en las *Imágenes 5.4, 5.5 y 5.6*, y dentro de los sitios haciendo uso de un probador

de cable con interfaz Ethernet de largo alcance, se procede a identificar el puerto del switch correspondiente a cada nodo existente dentro de la infraestructura, esto es en caso de no expandir los nodos propuestos.

Para el caso de realizar la expansión de nodos, al momento de reconectar cada nodo, es cuando se puede realizar la etiquetación de forma paralela.

VLAN en Switch

Posteriormente se recomienda comenzar con la configuración de los Switch, para acceder a los mismos se puede realizar un procedimiento análogo al acceso por el puerto de consola en el Firewall, véase la Figura 5.10., colocando valores similares en la terminal de comandos, o en el software emulador de terminal.

Una vez realizado el paso anterior, de manera general se mencionará el procedimiento a realizar, ya que como existen Switch de diferente fabricante dentro de la infraestructura, por consiguiente, hay diferencias en los comandos dentro de sus interfaces CLI. Tomando como referencia la *Tabla 5.2* los pasos por seguir para cada VLAN son:

- Se crea la VLAN con su identificador revisando la *Tabla 5.2* para distinguir el área/laboratorio que se está configurando.
- Se establecen los puertos dedicados a la VLAN, nuevamente revisando que correspondan al área/laboratorio que se está configurando.
- Se establece algún puerto como troncal dedicado habilitando la salida de la VLAN por ese puerto. Posteriormente solo se le da salida a cada VLAN que se vaya creando.
- Se conecta el puerto troncal a alguna de las interfaces Ethernet del Firewall.

El siguiente diagrama resume los pasos anteriormente dichos:

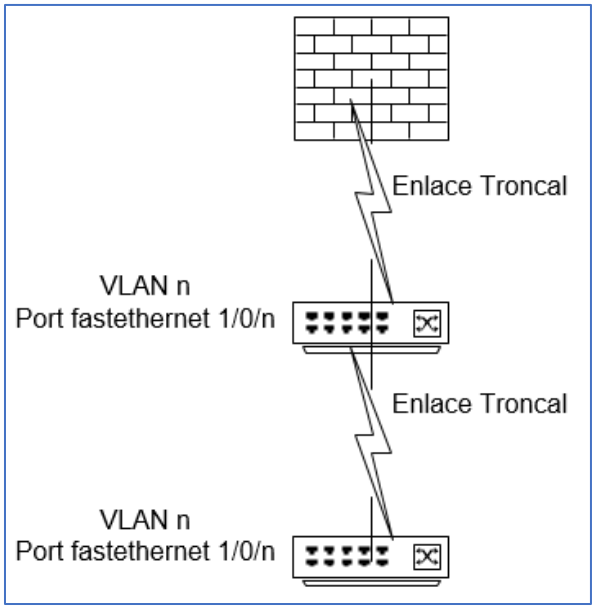


Imagen 5.12. Enlaces troncales VLAN. [A35]

Pasando al Firewall, lo primero por hacer es actualizar el Firmware del dispositivo, entonces se requiere proveer el enlace de internet, conectamos en el puerto WAN 1 la salida a internet, y bajo la configuración de la ruta estática se coloca el destino 0.0.0.0/0 (salida a todas partes) similar a la siguiente imagen:

Destination	Gateway	Interface
0.0.0.0/0		wan1

Imagen 5.13. Ruta Estática. [A36]

Sumado a lo anterior, es necesario crear la política IP para establecer que todo lo contenido en la interfaz **lan** salga hacia internet por la interfaz **wan1**, para ello desde **Policy & Objects->IPv4 Policy**, presionamos el botón **Create New** para abrir el siguiente formulario, llenándolo de forma similar:

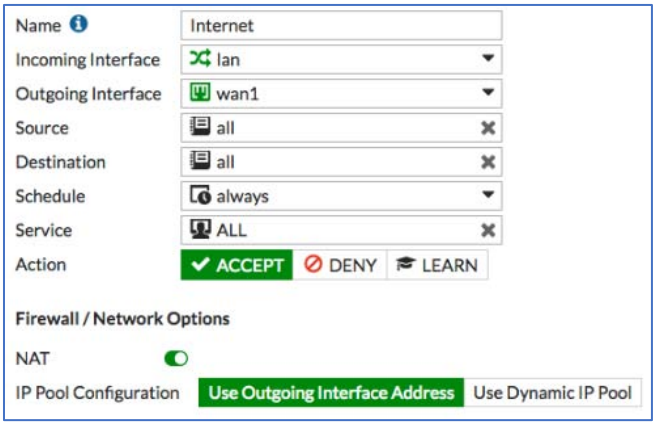


Imagen 5.14. Política IPv4 para Internet. [A37]

Prosiguiendo con la actualización para ello bajo **System->Firmware** revisamos si existe alguna actualización disponible por parte del servidor del fabricante, en caso de existir se solicita la descarga de la actualización, y esperamos a que se realice la instalación, la interfaz presentada es similar a la siguiente imagen:

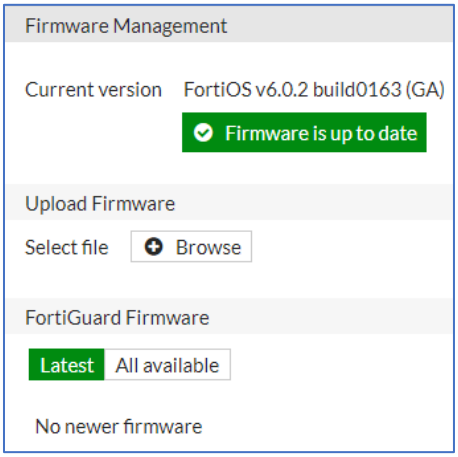


Imagen 5.15. Opción Firmware. [A38]

El siguiente paso es verificar desde la información ofrecida en Main, el estado de la licencia, si no aparece con licencia activada, se requiere realizar la activación, esto puede hacerse en el tablero principal.

Hacer esto requiere completar el siguiente proceso de registro, comencemos dando clic en el botón **Register Now** en la siguiente pantalla:

Figura 5.15. Inicio de registro para licencia. [B30]

Esto nos va a conducir a los formularios siguientes:

Figura 5.16. Formulario de registro. [B31]

En él se ingresan los datos solicitados, se recomienda utilizar un correo del cual se tenga constante uso, para evitar incidentes con la licencia, posterior a esto se pedirán datos adicionales en otro formulario. Al final del proceso bajo **System->Fortiguard->License Information** debemos encontrar algo similar a lo siguiente, para comprar si el proceso se hizo con éxito:

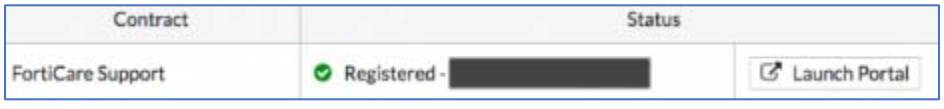


Figura 5.17. Estado de licencia. [B32]

Una vez realizados esos procedimientos se continua con la parte de configuración de las VLAN y las direcciones propuestas previamente.

VLAN en Firewall

Desde **Network->Interfaces**:

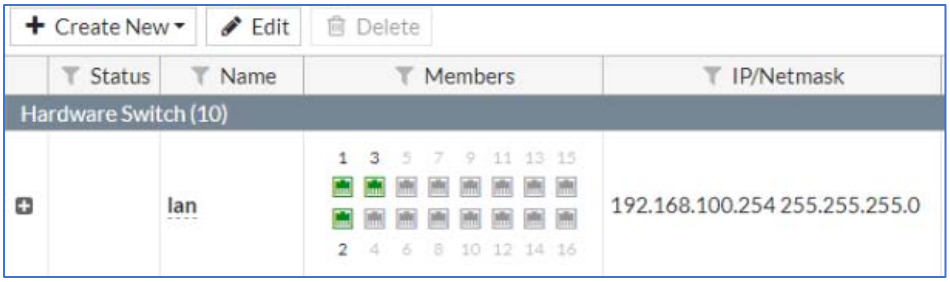


Imagen 5.16. Interfaces LAN. [A39]

Seleccionamos **Create New**, la cual va a presentar un formulario para establecer lo que se desea crear, entre las opciones del formulario viene la posibilidad de definir el tipo de interfaz a crear, seleccionamos que es una **interfaz VLAN**, lo siguiente que solicita es el ID de la VLAN y el ID de red para la misma, esos valores se pueden tomar de las *Tablas 5.2 y 5.4*, en la parte de nombre de interfaz puede ser utilizada para establecer el área/laboratorio, de esa manera se etiqueta de forma lógica la VLAN creada, ese procedimiento se realiza para todas las VLAN presentadas en la *Tabla 5.2.* La siguiente figura muestra un ejemplo de parámetros a ingresar en el formulario:

VLAN Name	VLAN_100
Type	VLAN
Interface	internal
VLAN ID	100
Addressing Mode	Manual
IP/Netmask	172.100.1.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

Figura 5.18. Formulario para VLAN. [B33]

En el procedimiento anterior de forma implícita, se está construyendo el direccionamiento propuesto para cada área/laboratorio, no obstante, para establecer más adelante las políticas de control de tráfico, será necesario el siguiente proceso.

Direccionamiento en Firewall para políticas Traffic Shaping

Bajo **Policy & Objects->Addresses**:

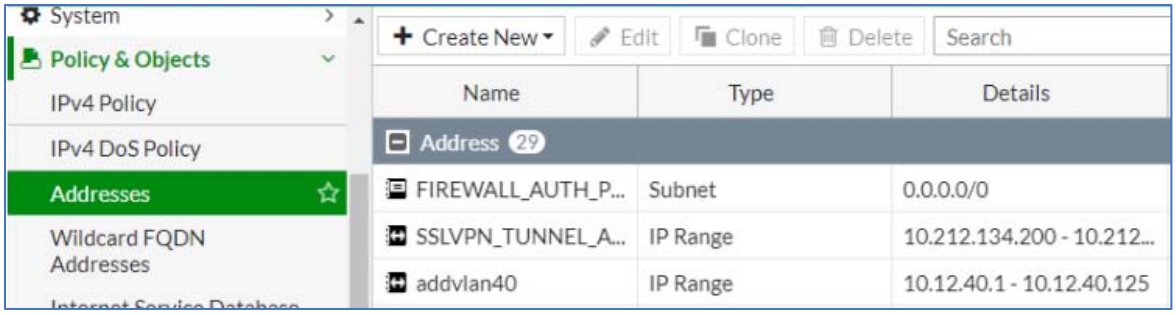


Imagen 5.17. Addresses. [A40]

Ahora vamos a seleccionar nuevamente **Create New**, en el formulario nos pedirá los datos de nombre, se sugiere colocar el nombre de la **vlan** a la que se le va a crear el rango, después en tipo de dirección se elige **IP Range**, dentro de ese rango se pondrán los rangos propuestos en la *Tabla 5.4.* La figura subsecuente muestra un formulario similar para establecer un rango de dirección:

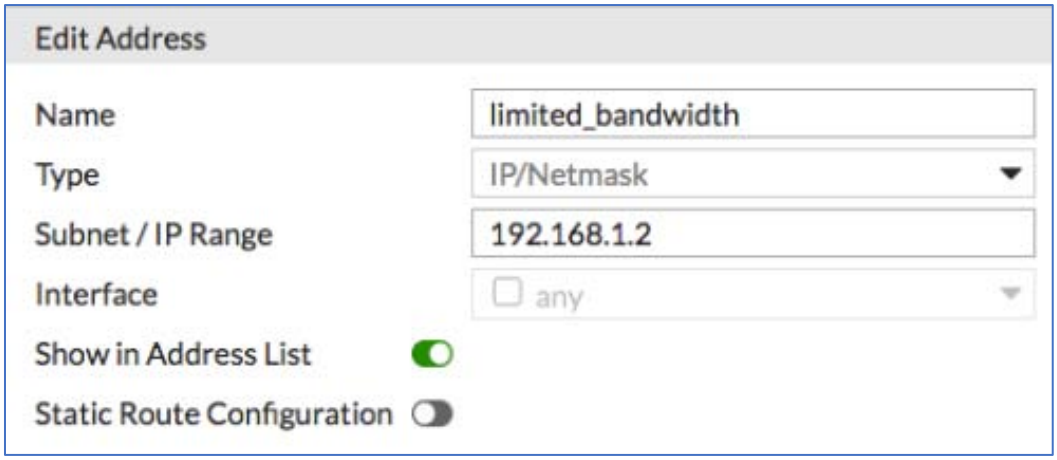


Figura 5.19. Edit Address. [B34]

Para cada área/laboratorio, hecho esto ya se tiene dado un primer paso para el control de tráfico el cuál se verá posteriormente.

Por el momento tenemos cubiertas las configuraciones iniciales para la **Propuesta A**, ahora pasemos a realizar configuraciones para **ambas propuestas**.

Router con Access Point

En el caso de la **Propuesta A**, es necesario que las configuraciones dentro del Firewall se encuentren en correcta operación, además de que solo se podrá disponer de un nodo para la instalación de este dispositivo de red.

Para el caso de la **Propuesta B** se puede decir que son las primeras configuraciones, tanto en general como en materia de direccionamiento privado. También como en la otra propuesta se deberá definir el nodo dedicado para la conexión del dispositivo.

Primeramente, dado que será un segmento privado muy limitado (para prestadores de servicio social o becarios temporales), se sugiere establecer el siguiente direccionamiento por área/laboratorio:

Área/Laboratorio	ID de Red	Gateway
Coordinación	192.168.10.0	192.168.10.32
Administración	192.168.20.0	192.168.20.32
Laboratorio de Cómputo	192.168.30.0	192.168.30.64
Seguridad Informática	192.168.40.0	192.168.40.64
INNOVA UNAM	192.168.50.0	192.168.50.32
Medición, Instrumentación y Control	192.168.60.0	192.168.60.32
Ingeniería Mecánica	192.168.70.0	192.168.70.32
Estudios Ambientales	192.168.80.0	192.168.80.32
Ingeniería Ambiental	192.168.90.0	192.168.90.32
Auditorio y Espacios Audiovisuales	192.168.100.0	192.168.100.128
Jardín Botánico	192.168.110.0	192.168.110.32

Tabla 5.5. Direccionamiento privado para Router con AP. [TA8]

Además, se recomienda establecer políticas de control de límite de usuarios, para no exceder el valor implícito en las direcciones de Gateway, por ejemplo, si el gateway sugiere .32 entonces el número máximo de clientes será 31. Un poco más adelante, se verá como establecer esas configuraciones.

Configuraciones Iniciales en Router

Posterior a sacar el dispositivo de su embalaje, suministramos energía eléctrica conectando su fuente de energía a la toma de corriente, conectamos un cable Ethernet del nodo dedicado al puerto WAN del Router, con otro cable de red conectamos al puerto 1 una computadora con cualquier Sistema Operativo que cuente con interfaz gráfica y navegador de internet, la siguiente figura muestra lo dicho de forma compacta:

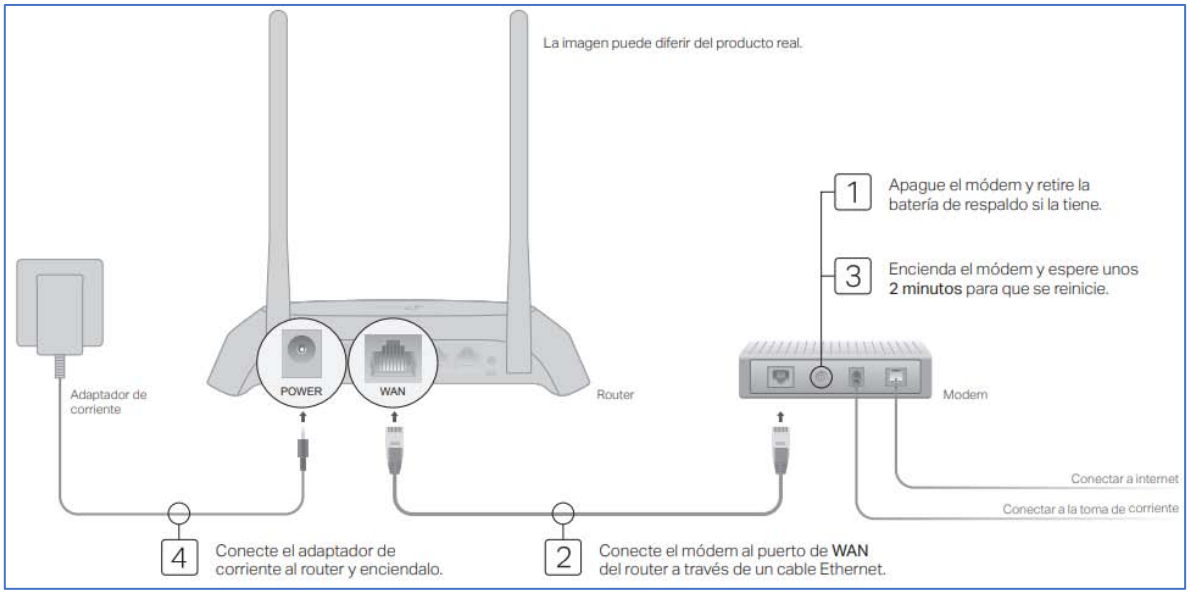


Figura 5.20. Guía Rápida. [B35]

En la figura podemos ver que la conexión a Internet está dada por un Modem, para el caso de las áreas/laboratorios, esa conexión la ofrece el nodo dedicado para el Router.

Luego de finalizar las conexiones físicas, desde una computadora con navegador de Internet, ingresamos la dirección http://tplinkwifi.net, al hacerlo nos presentará el siguiente formulario para ingresar credenciales:

Imagen 5.18. Login en Router. [A41]

Las credenciales por defecto para ingresar a la interfaz gráfica del dispositivo son usuario: **admin** y contraseña: **admin**, se recomienda cambiar esas configuraciones, en los siguientes pasos a realizar se muestra cómo hacer ese cambio.

Ingresando las credenciales antes mencionadas, se tendrá acceso a un tablero (dashboard) análogo al siguiente:

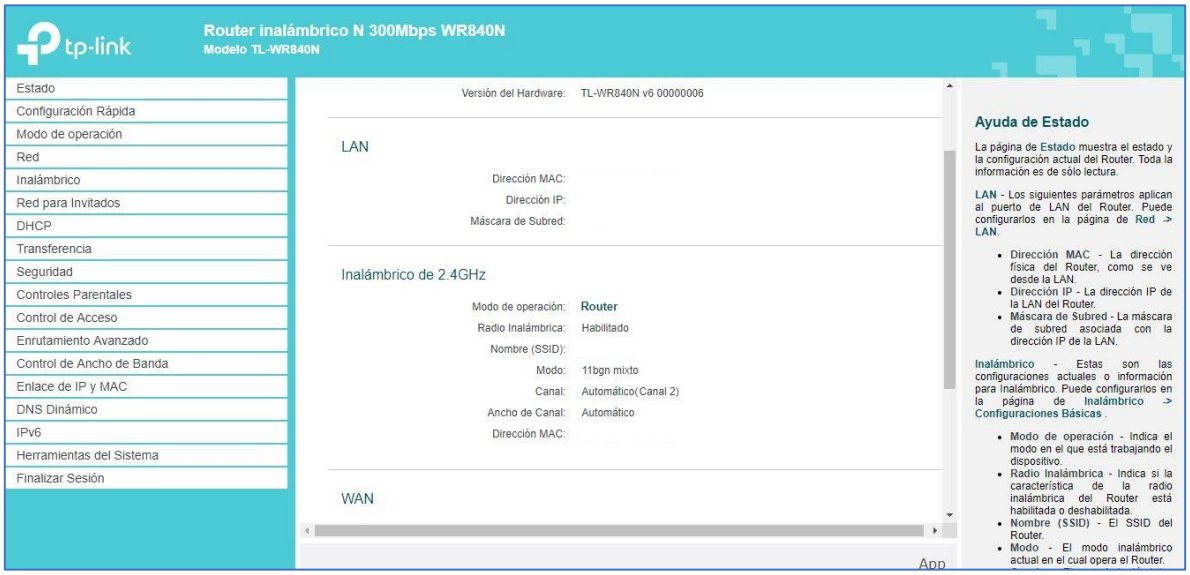


Imagen 5.19. Tablero principal en Router. [A42]

En la columna izquierda aparecen clasificadas las características con las que cuenta el dispositivo, en la columna central se muestra la información o los formularios de configuración, y en la columna derecha vemos información de apoyo para realizar los cambios dependiendo de la característica y opción seleccionada, podemos apoyarnos de esta columna para tener mayor precisión en lo que hacemos.

Para dar inicio a las configuraciones del Router, partamos con el cambio de las credenciales de acceso al dispositivo, para ello en la columna izquierda en el tablero principal elegimos **Herramientas del Sistema->Contraseña** llegando al siguiente formulario:

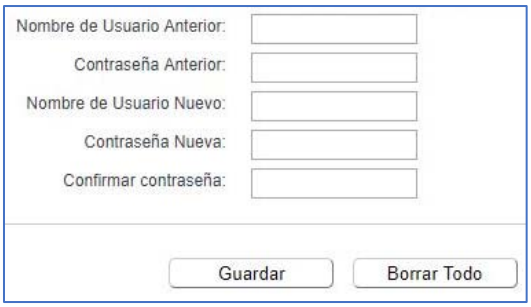


Imagen 5.20. Cambio de contraseña. [A43]

En los campos se coloca la información solicitada, nuevamente es muy importante **documentar** este paso, para realizar la documentación se puede tomar la presente propuesta como referencia para estructurar el documento, se sugiere que además de contar con una copia digital resguardada en medios de almacenamiento masivo, se cuente con una copia impresa archivada.

Ahora configuremos el perfil de uso para el dispositivo, la dirección WAN, la red inalámbrica con prácticas elementales de seguridad, y el rango de usuarios permitidos.

Perfil, Enlaces WAN y LAN

Por defecto, el dispositivo cuenta con un asistente para realizar la mayoría de las configuraciones mencionadas, es práctico para una primera configuración, pero, para el caso de la propuesta se harán las configuraciones de forma manual, con la intención de ofrecer mayor precisión en los casos en que se tenga que hacer modificaciones en las configuraciones.

Para elegir el perfil de uso, seleccionamos la característica **Modo de operación**, la cual nos mostrará las siguientes opciones:

Imagen 5.21. Opciones en modo de operación. [A44]

Elegimos **Router inalámbrico**, después damos clic en el botón Guardar.

Ahora para configurar el enlace WAN (el cual provee la salida a Internet), seleccionamos **Red->WAN**, para llegar al siguiente formulario:

Imagen 5.22. Enlace WAN. [A45]

En la casilla **Tipo de Conexión** despliega una lista de objetos, elegimos **IP Estática** y llenamos los campos solicitados:

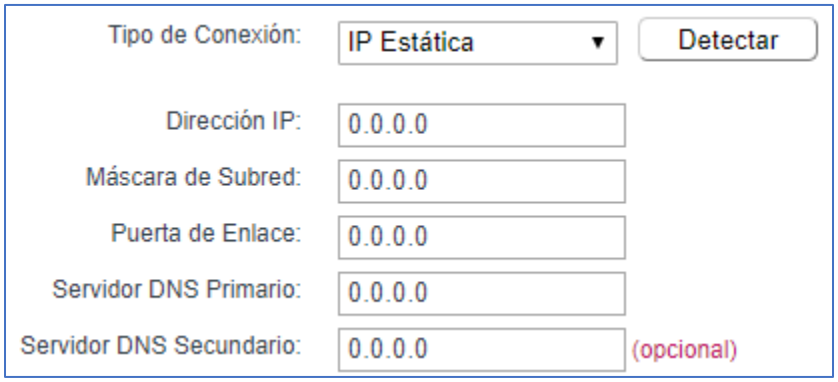


Imagen 5.23. Enlace WAN estático. [A46]

En **Dirección IP** colocamos la dirección asignada para ese nodo, en **Máscara de Subred** escribimos el segmento correspondiente a la dirección del nodo, en **Puerta de Enlace** se ingresa la salida que tiene el segmento de la dirección del nodo, en **Servidor DNS Primario** asignamos la dirección 132.248.10.2, y en **Servidor DNS Secundario** ponemos la dirección 132.248.204.1, finalizamos el procedimiento dando clic en el botón Guardar.

Continuemos con establecer el enlace LAN/Gateway para la red privada del dispositivo, seleccionando **Red->LAN** se despliega el siguiente formulario:

Imagen 5.24. Enlace LAN. [A47]

En el campo **Dirección IP** colocamos el segmento Gateway correspondiente a cada área/laboratorio, para ello podemos tomar la información de la *Tabla 5.5*, y en **Máscara de Subred** colocamos 255.255.255.0.

Red Wi-Fi y número de direcciones disponibles para usuarios

Para crear la red inalámbrica seleccionamos la característica **Inalámbrico->Configuraciones Básicas** para desplegar este formulario:

Imagen 5.25. Configuraciones Inalámbricas. [A48]

Como nombre de la red se recomienda colocar el nombre del área/laboratorio, en los demás campos se sugiere dejarlos de forma similar a la *Imagen 5.24*, como **práctica de seguridad** se considera adecuado Deshabilitar la Transmisión SSID, de esa manera cuando algún usuario desee conexión tendrá que consultar al administrador local del área/laboratorio el ID de Red Inalámbrica.

Para establecer la clave de acceso a la red seleccionamos **Inalámbrico->Seguridad Inalámbrica** para ver lo siguiente:

Imagen 5.26. Seguridad Inalámbrica. [A49]

Se recomienda ampliamente elegir el tipo **WPA/WPA2 – Personal**; la contraseña inalámbrica queda a libertad de cada área/laboratorio, reiterando nuevamente la importancia documentar esa información para evitar problemas de acceso.

Otra medida de seguridad recomendable es deshabilitar el acceso WPS (Wi-Fi Protected Setup), para ello bajo **Inalámbrico->WPS**:

Imagen 5.27. Acceso WPS. [A50]

La razón es que esta característica ofrece acceso presionando un botón físico del dispositivo, con un PIN numérico como medida de seguridad. En un entorno doméstico privado sería recomendable y práctico contar con la característica, pero en el Centro Tecnológico Aragón hay afluencia constante de personas, por lo que ese atributo representa un riesgo.

Finalmente, para configurar el rango direcciones IP para la cantidad de usuarios específico, seleccionamos **DHCP->Configuraciones de DHCP**, para llegar al siguiente formulario:

Imagen 5.28. Opciones para servicio DHCP. [A51]

Se recomienda dejar habilitado el servicio DHCP (Dynamic Host Configuration Protocol), ya que ese servicio proporciona de forma dinámica las direcciones IP para los dispositivos a conectar.

Si tomamos como ejemplo que se va a configurar al Router del **Laboratorio de Cómputo**, empleado la información de la *Tabla 5.5* colocamos en **Dirección IP de Inicio**: 192.168.30.1, mientras que en **Dirección IP Final** ingresamos: 192.168.30.63, en **Tiempo de Arrendamiento** se sugiere poner 60 minutos, y en los demás campos podemos hacer caso omiso, debido a que esos campos se cubrieron en características anteriores.

Hasta ahora hemos hecho configuraciones iniciales para las **Propuestas A** y **B**, en el siguiente subcapítulo revisaremos configuraciones específicas, en materia de seguridad y control de banda ancha.

5.3. Políticas para control de tráfico y seguridad.

Debido a que hemos visto algunas propuestas con base en diseño y funcionamiento, así como la materialización de ellas.

En este subcapítulo se plantean ideas para establecer políticas en características como el control de tráfico dentro de la infraestructura. Además, se propondrán algunas políticas de seguridad para el contenido web, grupos de direcciones IP virtuales, y elementos básicos de seguridad en servidores.

Es preciso aclarar aunque la mayoría de las ideas son para la **Propuesta A**, se eligieron algunos planteamientos adecuados para la **Propuesta B**, y de igual manera que en el subcapítulo anterior, se comenzará revisando cada idea propuesta, para después pasar a su implementación a través de configuraciones en los dispositivos.

5.3.1. Control de ancho de banda mediante Traffic Shaping.

Contar con un control de ancho de banda, da la ventaja de que se garantice acceso ágil a internet de forma constante para todas las áreas/laboratorios, para realizar

esta práctica de forma adecuada se sugieren los siguientes controles para las áreas/laboratorios:

Área/Laboratorio	Horario laboral	Tráfico Disponible	Horario libre	Tráfico Disponible
Coordinación	7 – 15 Hrs & 17 – 20 Hrs	50 Mbps simétrico	15 – 17 Hrs	100 Mbps simétrico
Administración	7 – 15 Hrs & 17 – 20 Hrs	50 Mbps simétrico	15 – 17 Hrs	100 Mbps simétrico
Laboratorio de Cómputo	7 – 20 Hrs	100 Mbps simétrico	-	-
Seguridad Informática	7 – 20 Hrs	100 Mbps simétrico	-	-
INNOVA UNAM	7 – 15 Hrs & 17 – 20 Hrs	30 Mbps simétrico	15 – 17 Hrs	100 Mbps simétrico
Medición, Instrumentación y Control	7 – 15 Hrs & 17 – 20 Hrs	50 Mbps simétrico	15 – 17 Hrs	100 Mbps simétrico
Ingeniería Mecánica	7 – 15 Hrs & 17 – 20 Hrs	50 Mbps simétrico	15 – 17 Hrs	100 Mbps simétrico
Estudios Ambientales	7 – 15 Hrs & 17 – 20 Hrs	30 Mbps simétrico	15 – 17 Hrs	100 Mbps simétrico
Ingeniería Ambiental	7 – 15 Hrs & 17 – 20 Hrs	50 Mbps simétrico	15 – 17 Hrs	100 Mbps simétrico
Auditorio y Espacios Audiovisuales	7 – 20 Hrs	100 Mbps simétrico	-	-
Jardín Botánico	7 – 15 Hrs & 17 – 20 Hrs	30 Mbps simétrico	15 – 17 Hrs	100 Mbps simétrico

Tabla 5.6. Controles de Ancho de Banda. [TA9]

La tabla maneja horarios en los que se aplica el control de tráfico, los cuales son comúnmente las horas laborales para todas las áreas/laboratorios, incluyendo un horario especial el cual coincide con las horas de comida; en ese horario se deja abierto todo el ancho de banda disponible.

Es recomendable tener un control simétrico debido a que, en el análisis realizado dentro de las áreas/laboratorios, ese tipo de tráfico se considera adecuado para la descarga/subida de información, por cada área/laboratorio del Centro Tecnológico Aragón. Pasemos a plasmar la idea en configuraciones en los dispositivos.

Firewall

Ahora bien, para materializar la idea, en la **Propuesta A**, es necesario que las características mostradas en el subcapítulo anterior se encuentren en operación. Posterior a ello, se tienen que hacer los siguientes pasos dentro de la interfaz gráfica de usuario GUI en el Firewall, desde **Policy & Objects->Traffic Shapers** presionando el botón **Create New** arrojará el siguiente formulario:

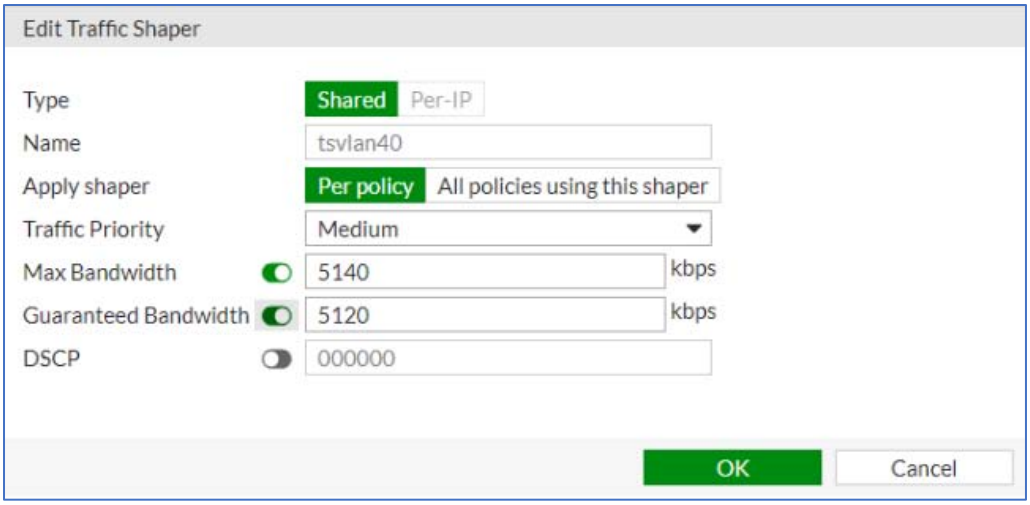


Imagen 5.29. Formulario Traffic Shaper. [A52]

En el **nombre** se recomienda poner como etiqueta que se trata de un Traffic Shaper, sobre la VLAN del área/laboratorio que se esté configurando, en la *Imagen 5.28.* ejemplifica como realizar eso, en **Apply shaper** se sugiere dejar por defecto la opción **Per policy** ya que cada área/laboratorio tendrá su propia política de control de tráfico, con una prioridad en **Medium**, en la casilla **Max Bandwidth** se coloca el

valor de tráfico máximo (dada en kbps) para esto utilicemos la *Tabla 5.6.*, donde por ejemplo si se trata de 50 Mbps se colocaría 51,300 kbps (dada la multiplicación 50 x 1024 sumando 100), por último en la casilla **Guaranteed Bandwidth** se pone el valor para el ancho de banda garantizado, por ejemplo si se trata de 50 Mbps se colocaría 51,200 kbps. Esto se hace solo para los valores definidos en la *Tabla 5.6*.

A continuación, pasamos a crear la política de control, para llevarlo a cabo desde **Policy & Objects -> Traffic Shaping Policy**:

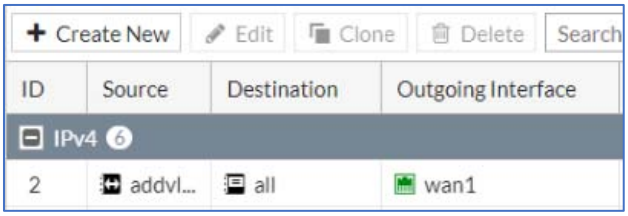


Imagen 5.30. Traffic Shaping Policies. [A53]

Presionando **Create New** abrirá el siguiente formulario:

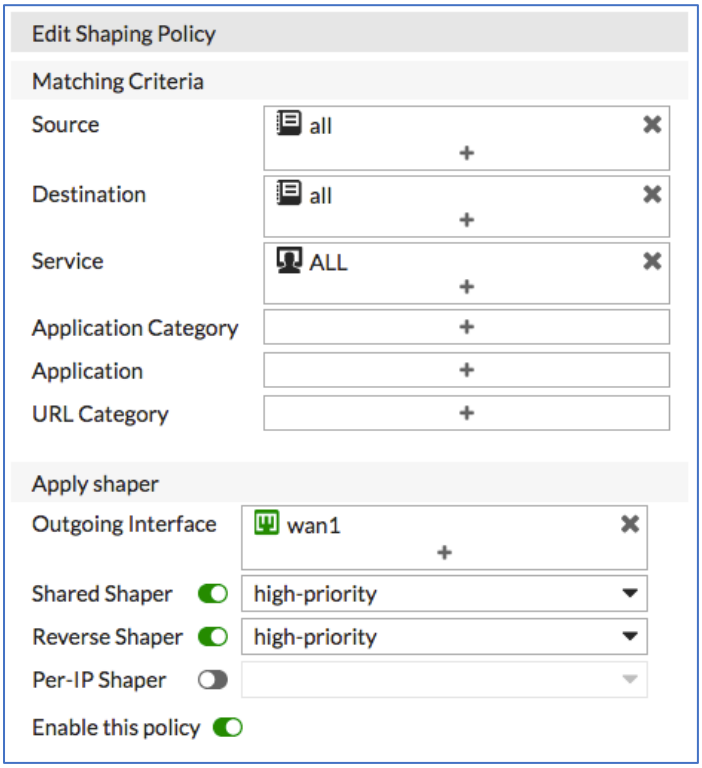


Imagen 5.31. Formulario Shaping Policy. [A54]

En **Source** elegimos el rango de direcciones creado previamente en el subcapítulo anterior, ese rango debe corresponder con la VLAN del área/laboratorio que estemos configurando, en **Destination** elegimos **all**, en **Service** se elige **ALL** esto permite que el Shaper se aplique a los servicios solicitados en protocolos **TCP** o **UDP**, en **Outgoing Interface** elegimos **wan1** o la interfaz donde se haya colocado la salida a internet, para **Shared Shaper** buscamos el shaper creado en el formulario de la *Imagen 5.28.*, nuevamente correspondiendo con el área/laboratorio que se está configurando, este campo establece el tráfico para la carga de información, y en **Reverse Shaper** de hace un proceso similar que en Shared Shaper, este campo establece el tráfico para la descarga de información, verificamos que la casilla **Enable this policy** se encuentre habilitada.

Una vez realizado lo anterior verificamos la creación de la política desde **Policy & Objects->Traffic Shapers**:

5.32. Traffic Shaper creado. [A55]

Concluyendo con el Firewall, para asignar los horarios de operación de los shapers, primero ya debe estar establecida la hora, fecha y zona horaria en el dispositivo.

Para hacer esto desde **System->Settings->System Time** bajo la siguiente subinterfaz:

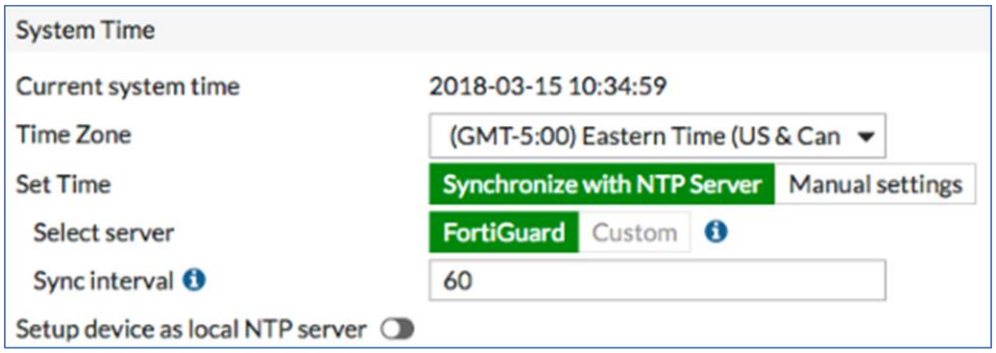


Figura 5.21. System Time. [B36]

Elegimos la zona horaria **GMT-6:00 Central Time (Mexico City)**, dejando habilitada la casilla **Synchronize with NTP Server**, para que de forma automática coloque la fecha y hora correspondientes a la zona horaria.

Después, desde **Policy & Objects->Schedules**, creamos el horario dando clic en el botón **Create New**, dentro del formulario se establecen las horas con base en la *Tabla 5.6.*, la misma sugiere 3 tipos de horario, asegurando de estar en la casilla **Recurring** y de ponerle un nombre adecuado a los valores de la *Tabla 5.6*.

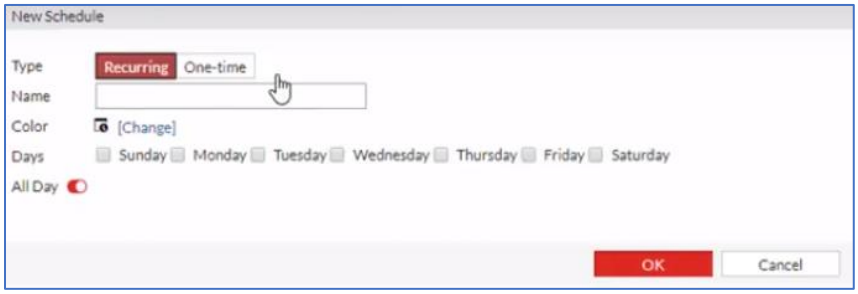


Figura 5.22. Schedule. [B37]

Posteriormente, será necesario definir las políticas IP por cada VLAN, para que de esta forma se les asignen sus shapers y horario de estos, para ello vamos a **Policy & Objects->IPv4 Policy**, con el botón **Create New** abrirá un formulario similar al de la *Imagen 5.14.* poniendo particular atención en el siguiente campo:

Imagen 5.33. Campo de horario. [A56]

Se selecciona el horario creado en el apartado **Schedules**, y definimos las políticas por cada horario para cada VLAN.

Router con Access Point

Por otra parte, para **ambas propuestas** se puede establecer control de tráfico en los Router con Access Point sugeridos, para realizarlo desde la interfaz gráfica del dispositivo accedemos a la característica **Control de Ancho de Banda**, para desplegar la siguiente pantalla:

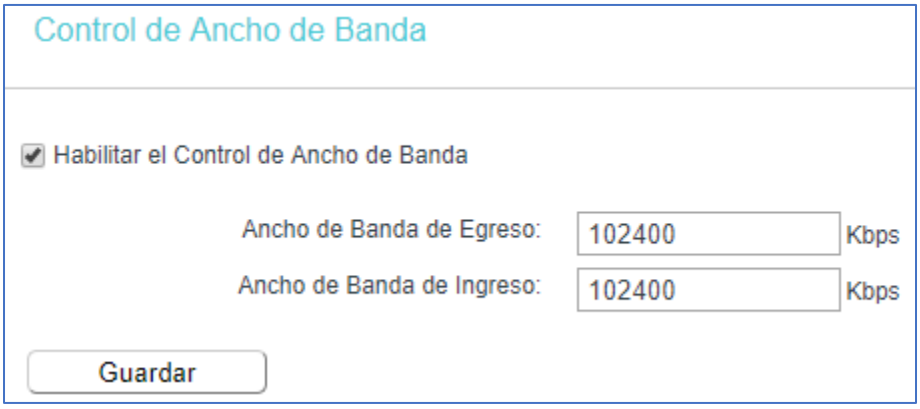


Imagen 5.34. Control de Ancho de Banda. [A57]

El campo **Ancho de Banda de Egreso** se refiere a la carga de información hacia Internet, mientras que **Ancho de Banda de Ingreso** se refiere a la descarga de información desde Internet, dado que la *Tabla 5.6.* sugiere tráfico simétrico se colocarán los mismos valores en ambos campos. Por ejemplo, si estamos configurando el Router del Laboratorio de Cómputo se pone un valor análogo al de la *Imagen 5.34.* en kbps, a diferencia de la **Propuesta A**, no es posible establecer un control de horario general.

Una característica interesante que presentan estos dispositivos es la posibilidad de crear una red inalámbrica para invitados, lo cual representa una alternativa al control de horarios ya que en esa red se establece menor cantidad de tráfico y en horarios específicos, para adoptar esta prestación, desde el tablero de la interfaz gráfica seleccionamos **Red para invitados**, para abrir la siguiente pantalla:

Imagen 5.35. Red para invitados. [A58]

En el campo **Permitir que los invitados tengan Acceso a mi Red Local**, es imprescindible deshabilitarla como práctica elemental de seguridad, los otros 2 campos se recomienda poner las opciones como en la *Imagen 5.35.*

Aunado a lo anterior, podemos notar que es posible establecer control de ancho de banda para esta red, esos campos se dejan a consideración del administrador de área colocar los valores que considere adecuados, siempre y cuando no supere los rangos planteados en la *Tabla 5.6.*

Posteriormente, se configuran las características de seguridad para acceso a la red inalámbrica de invitados, nuevamente se recomienda elegir la encriptación WPA2, colocando una contraseña de al menos 8 caracteres entre números, letras y caracteres especiales.

Finalmente, en la parte inferior de la pantalla desplegada en la *Imagen 5.35.* se puede definir el control de tráfico, por días de la semana, y rango de horas (con hora

de inicio y de final), aunque, para asegurar que esto funcione es imprescindible configurar el dispositivo en la fecha y hora correcta.

Ahora veamos las configuraciones para el contenido web.

5.3.2. Políticas de Seguridad para contenido en Internet.

Internet ofrece un amplio contenido de información de muchas maneras, ofreciendo ventajas para mejorar la productividad, sin embargo, existe mucho contenido el cual puede considerarse, desde factor de riesgo hasta representar una amenaza para los usuarios, y en este caso para la infraestructura existente dentro del Centro Tecnológico Aragón.

Ante ese contexto, se pueden establecer controles para el acceso a contenidos en Internet para las áreas/laboratorios, para esto la siguiente tabla ofrece algunos planteamientos sobre los contenidos que se consideran adecuados tener acceso:

Área/Laboratorio	Contenido dentro de su contexto	Contenido fuera de su contexto
Coordinación	- Académico - Gubernamental - Entretenimiento - Multimedia - Herramientas de Ofimática	- Herramientas de Auditoría en Seguridad Informática - Herramientas especializadas de Computación - Software P2P - Sitios para adultos
Administración	- Académico - Gubernamental - Entretenimiento - Multimedia - Herramientas de Ofimática	- Herramientas de Auditoría en Seguridad Informática - Herramientas especializadas de Computación - Software P2P - Sitios para adultos
Cómputo	- Académico - Gubernamental - Entretenimiento - Multimedia - Herramientas de Ofimática - Herramientas de Seguridad Informática - Herramientas especializadas de Computación	- Software P2P - Sitios para adultos
Seguridad Informática	- Académico - Gubernamental	- Herramientas especializadas de Computación

	- Entretenimiento - Multimedia - Herramientas de Ofimática - Herramientas de Auditoría en Seguridad Informática	- Software P2P - Sitios para adultos
INNOVA UNAM	- Académico - Gubernamental - Entretenimiento - Multimedia - Herramientas de Ofimática	- Herramientas de Auditoría en Seguridad Informática - Herramientas especializadas de Computación - Software P2P - Sitios para adultos
Medición, Instrumentación	- Académico - Gubernamental - Entretenimiento - Multimedia - Herramientas de Ofimática	- Herramientas de Auditoría en Seguridad Informática - Herramientas especializadas de Computación - Software P2P - Sitios para adultos
Ingeniería Mecánica	- Académico - Gubernamental - Entretenimiento - Multimedia - Herramientas de Ofimática	- Herramientas de Auditoría en Seguridad Informática - Herramientas especializadas de Computación - Software P2P - Sitios para adultos
Estudios Ambientales	- Académico - Gubernamental - Entretenimiento - Multimedia - Herramientas de Ofimática	- Herramientas de Auditoría en Seguridad Informática - Herramientas especializadas de Computación - Software P2P - Sitios para adultos
Ingeniería Ambiental	- Académico - Gubernamental - Entretenimiento - Multimedia - Herramientas de Ofimática	- Herramientas de Auditoría en Seguridad Informática - Herramientas especializadas de Computación - Software P2P - Sitios para adultos
Auditorio y Espacios Audiovisuales	- Académico - Gubernamental - Entretenimiento - Multimedia - Herramientas de Ofimática	- Herramientas de Auditoría en Seguridad Informática - Herramientas especializadas de Computación - Software P2P - Sitios para adultos
Jardín Botánico	- Académico - Gubernamental - Multimedia - Herramientas de Ofimática	- Herramientas de Auditoría en Seguridad Informática - Herramientas especializadas de Computación - Entretenimiento

	- Software P2P - Sitios para adultos

Tabla 5.7. Contenidos en Internet. [TA10]

Se proponen esos criterios de contenido en Internet, con base en el análisis de las actividades que realiza cada área/laboratorio. Para esto se sugiere el planteamiento de adoptar un filtro de contenidos web, esta práctica de seguridad es posible realizarla para **ambas propuestas**, no obstante, existen grandes diferencias entre ellas.

Por el lado de la **Propuesta A**, configurar esta característica es simple, automatizado y ampliamente robusto, mientras que del lado de la **Propuesta B** las reglas se establecen de forma manual, una a una, por lo que resulta necesario consultar bases de datos de contenidos web para tener referencias y con ello establecer de cada regla.

A continuación, se muestra de qué forma podemos implementar ambas propuestas, comenzando con la **Propuesta A**.

Firewall

Estando en el tablero principal, vamos a la característica **Security Profiles->Web Filter**, la cual arroja la siguiente subinterfaz:

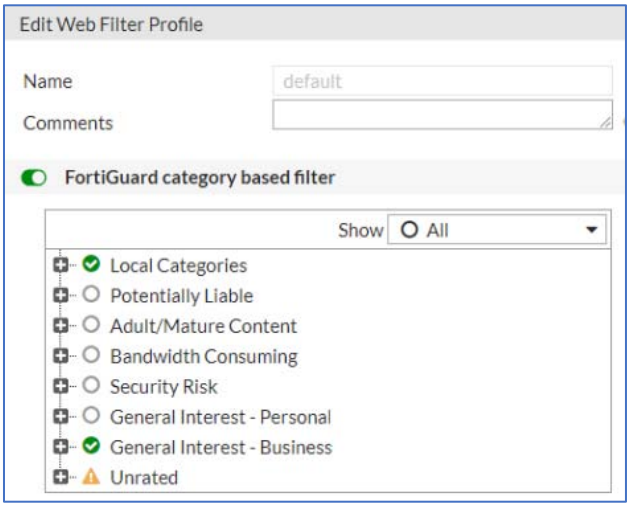


Imagen 5.36. Categorías de Web Filter. [A59]

La cual muestra todas las categorías con las que cuenta el filtro de contenidos del Firewall, decimos que es automatizado porque mantiene conexión constante con bases de datos de contenidos web. Entonces, para establecer los criterios propuestos en la *Tabla 5.7*, tenemos que ir revisando las opciones que ofrece cada categoría y subcategoría, eligiendo los perfiles que consideremos corresponden a los criterios planteados en la tabla. Para cubrir los criterios por áreas/laboratorios, es necesario crear varios perfiles web filter, la manera de hacerlo es dando clic en el siguiente botón **+** dentro del mismo tablero:

Imagen 5.37. Añadir perfiles Web Filter. [A60]

Una vez que hayamos realizado lo anterior, lo que sigue es agregar el filtro en cada política IPv4 que hayamos creado en el tablero de **Policy & Objects->IPv4 Policy**, seleccionamos la política a editar y habilitamos la siguiente casilla:

Imagen 5.38. Agregando Web Filter. [A61]

Para **ambas propuestas** se requiere configurar los Router.

Router con Access Point

Teniendo acceso al dispositivo, seleccionamos la característica **Control de Acceso**, desplegando la siguiente subinterfaz:

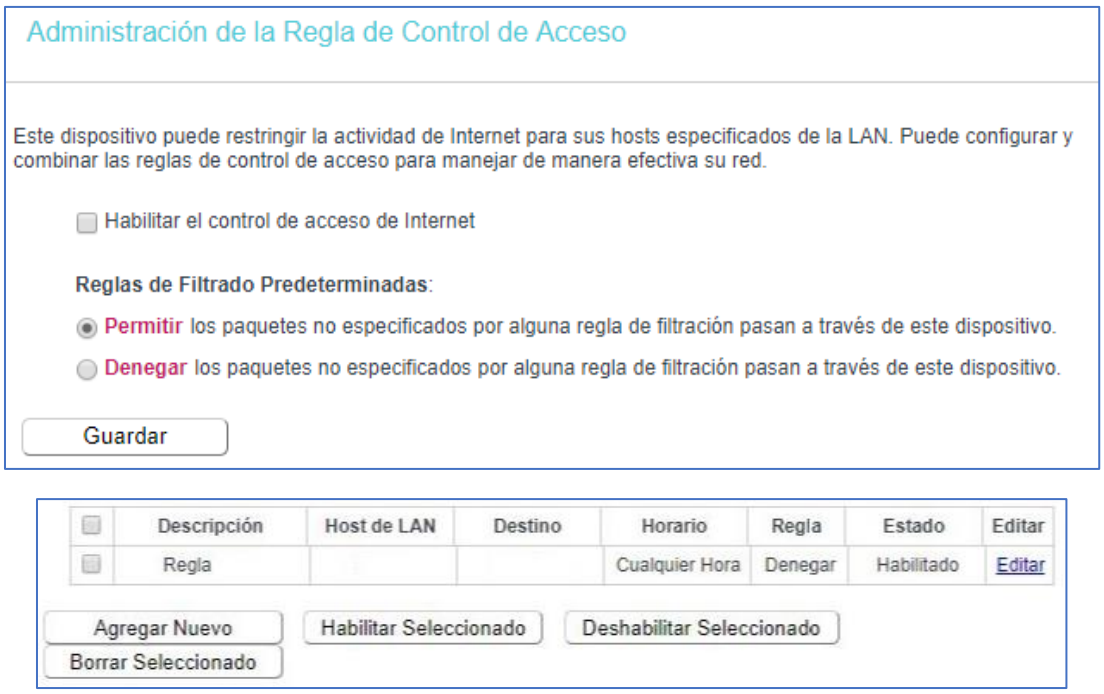


Imagen 5.39. Reglas de Control de Acceso. [A62]

Haciendo clic en el botón **Agregar Nuevo**, nos mandará a establecer los siguientes parámetros:

Imagen 5.40. Añadiendo regla. [A63]

En el apartado **Destino** es dónde se añaden las direcciones que se pretenden permitir o denegar, eso queda a consideración del administrador, al dar clic en ese apartado eligiendo Dirección URL, visualizaremos lo siguiente:

Imagen 5.41. Agregando destino. [A64]

En **Descripción** se recomienda poner el nombre del destino que se pretende permitir/denegar, y en **Agregar Dirección** colocamos la URL para filtrar. Esto se hace por cada sitio web que se desee filtrar. Al final se guarda todo el procedimiento realizado.

Estas configuraciones pueden hacerse para **ambas propuestas**, destacando la diferencia que en la **Propuesta A** solo se usa para establecer las pequeñas redes inalámbricas privadas, resultando ser incluso una característica opcional por implementar, puesto que en el Firewall ya existe un filtro de contenidos en Internet.

Del lado de la **Propuesta B** es el filtro de contenidos web disponible a utilizar para cada área/laboratorio, no obstante, el procedimiento a realizar resulta más largo y un tanto engorroso pero posible.

A continuación, se cerrará la presente propuesta, lo último que mencionaremos serán unas características de seguridad para servidores y para el manejo de direcciones públicas en las áreas/laboratorios que lo deseen adoptar.

5.3.3. Políticas de Seguridad en Servidores.

Para concluir la presente propuesta, se presentan unas últimas ideas por plantear con respecto a seguridad en servidores, y con una alternativa para el manejo de direcciones públicas sin comprometer la infraestructura.

Es importante mencionar que tanto la idea como la implementación, solo es posible realizar dentro de la **Propuesta A**, ya que las configuraciones se hacen en el Firewall.

DMZ

Anteriormente, se resaltó la importancia de establecer una Zona Desmilitarizada **DMZ** dentro de la infraestructura de red, esta zona por prácticas elementales de seguridad debe estar aislada, incluso se recomienda que los nodos pertenecientes a la misma se deben colocar de diferente color, o con una etiqueta especial indicando que el nodo es dedicado para la instalación de un servidor.

Se planteó la instalación de un switch dedicado a esta zona, considerando que el dispositivo sea de tipo plug & play debido a que no es necesario realizar configuraciones administrativas dentro del mismo, su función se limita a distribuir los nodos dedicados a la **DMZ**.

Con base en lo anterior, el siguiente diagrama muestra la distribución planteada para esta idea:

Imagen 5.42. Infraestructura DMZ. [A65]

La implementación de esta zona se realiza de una manera sencilla, nuevamente se reitera que el Firewall ya debe estar en correcta operación previo a realizar estas

configuraciones. Para llevar a cabo la materialización de la **DMZ** vayamos a la característica **Network->Interfaces** y seleccionamos **dmz**:

Imagen 5.43. Interfaz DMZ. [A66]

Posteriormente, damos clic al botón **Create New** el cual abre una subinterfaz parecida a la siguiente:

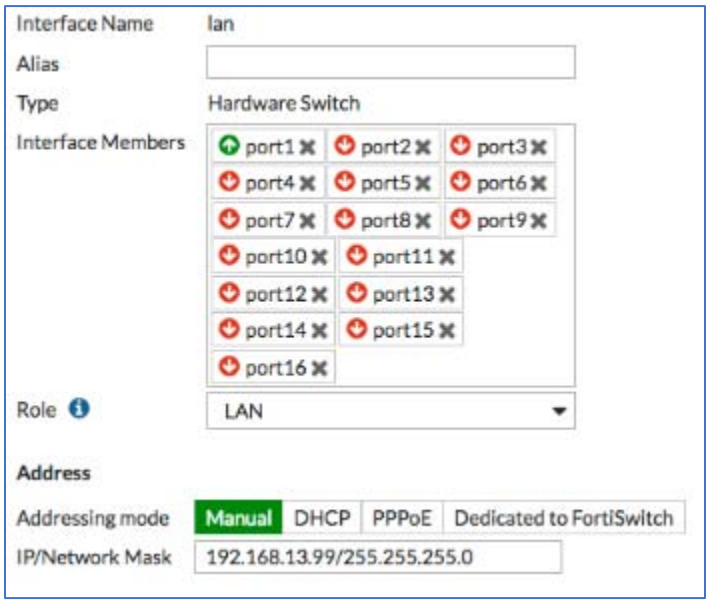


Imagen 5.44. Configurando interfaz. [A67]

Las diferencias están en **Interface Name** en lugar de decir **lan** marca la interfaz **dmz**, hay que asegurarnos que en **Interface Members** solo se encuentre el puerto dedicado a **DMZ**, de no ser así aparecerá el botón **+** el cual añade puertos, haciendo clic en ese botón buscamos el puerto **dmz** y lo añadimos. También hay que asegurarnos que en **Role** esté indicado que se trata de **DMZ**.

En el apartado **Address**, se recomienda colocar el ID de red o el gateway del segmento de direcciones públicas donde vayan a estar alojados los servidores, además de la máscara de red, esos datos pueden solicitarse al administrador general de la red del Centro Tecnológico Aragón.

Después de hacer este paso, lo siguiente es establecer políticas **IPv4** para añadir elementos de seguridad como control de puertos, o filtro de contenidos, para hacerlo desde **Policy&Objects->IPv4 Policy**, creamos la política de forma similar que en la *Imagen 5.14* teniendo especial atención en los campos:

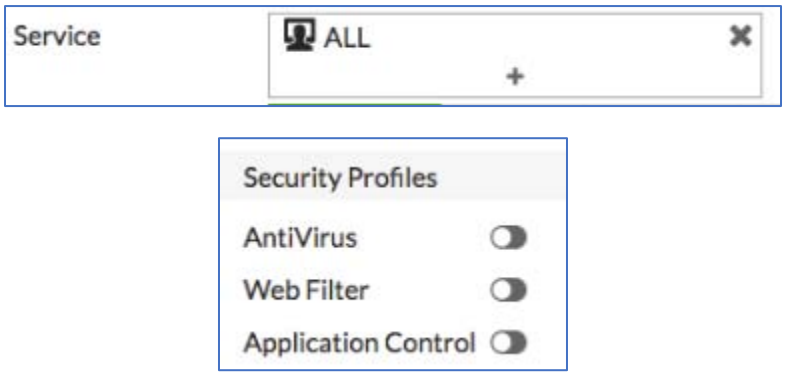


Imagen 5.45. Agregando características de seguridad. [A68]

En **Service** se eligen los puertos y servicios que deseamos habilitar en la política, para ello nos ofrece una subinterfaz mostrando los servicios más utilizados, esto es práctico para dar blindaje a los dispositivos que se encuentran tras la DMZ.

Es muy importante mencionar que, para lograr establecer esta zona, es necesario implementar el switch dedicado y hacer la etiquetación de los nodos, de lo contrario se incrementará la dificultad la realización de este planteamiento de forma considerable.

Dado que esta zona está aislada, se tienen grados de libertad para realizar las configuraciones, no obstante, se recomienda no hacer caso omiso a las ideas propuestas previas.

Cerremos el subcapítulo con las últimas ideas a proponer.

Grupo de direcciones IP Virtual (Virtual IP Pool)

Crear un IP Pool, permite utilizar **direcciones públicas** con algunas medidas de seguridad, su función es algo parecida a una traducción de direcciones, puesto que detrás de la dirección pública se puede establecer una dirección privada, pero con medidas de seguridad, como el control de puertos, con la diferencia que la

referencia es 1 a 1, esto es una dirección privada por una dirección pública, facilitando el acceso desde fuera de la infraestructura del Centro Tecnológico Aragón.

Cuando alguna área/laboratorio vaya a requerir esta característica, desde el Firewall vamos a **Policy&Objects->Virtual IPs**, para desplegar la subinterfaz:

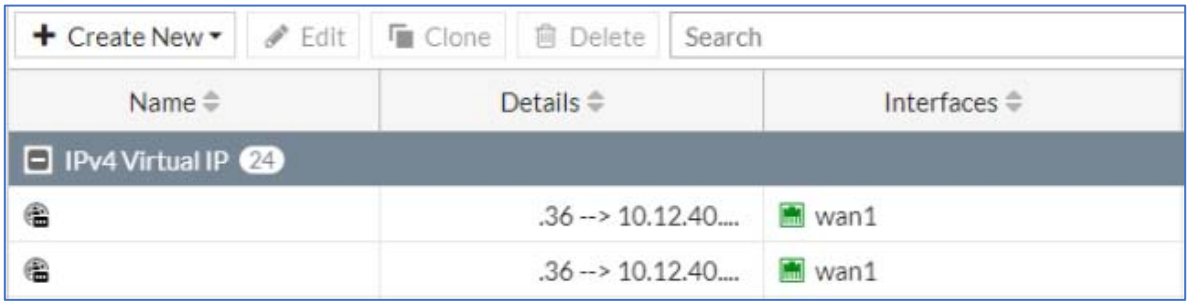


Imagen 5.46. Interfaz Virtual IPs. [A69]

Dando clic en el botón **Create New** accedemos al siguiente formulario:

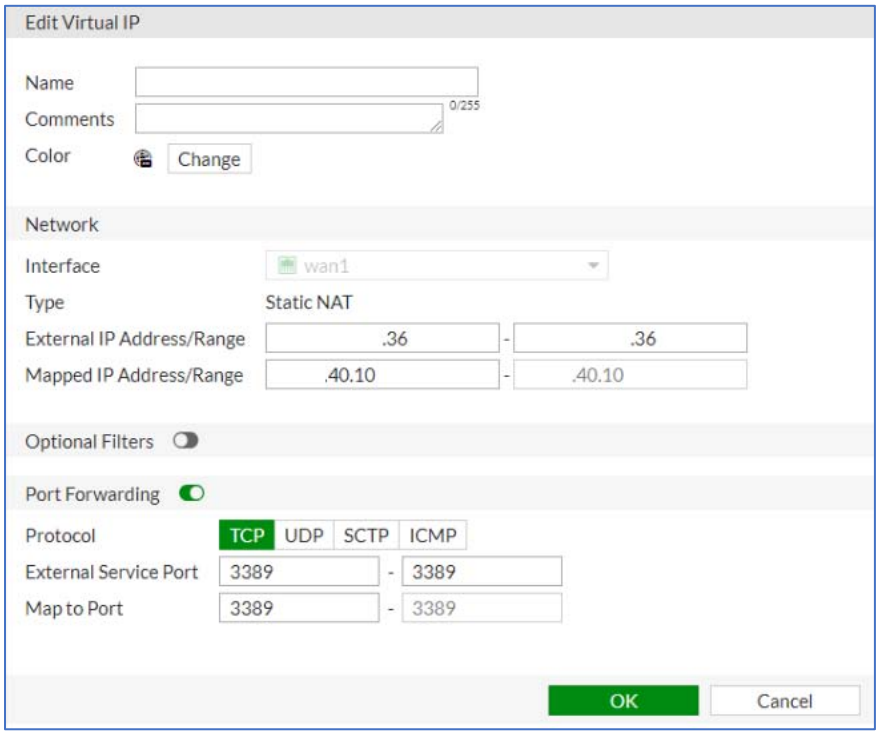


Imagen 5.47. Formulario Virtual IP. [A70]

En el campo **External IP Address/Range** colocamos la dirección pública por la que se desea salir, en **Mapped IP Address/Range** colocamos la dirección privada de la

cual se desea salir. Si se desea añadir filtros se habilita la casilla **Optional Filters**, ahora, bajo **Port Forwarding** elegimos el tipo de puerto que deseamos habilitar, además del rango de puertos a permitir, se deja a consideración del administrador definir los puertos por permitir, aunque como buena práctica se recomienda habilitar puertos específicos para no dejar abiertos posibles puntos de entrada.

Creación de archivos de respaldo en dispositivos

Por último, se subraya con mucho énfasis el siguiente planteamiento, el cual es realizar un respaldo de seguridad de las configuraciones realizadas tanto en el Firewall como en los Router con Access Point, esto es debido a que se puede presentar el caso en que sea necesario hacer una reinstalación en el contexto de falla de hardware (ocasionando cambio físico de algún dispositivo), o cuando se requiera dar un reset general en caso de un error grave intratable de software.

La intención de este planteamiento es evitar perder tiempo, en rehacer todas las configuraciones mostradas a lo largo de los anteriores subcapítulos, es una práctica básica de seguridad contar con archivos de respaldo de sistema de los dispositivos.

Firewall

Desde el tablero principal vamos hacia la esquina superior derecha en el ícono de usuario:

Imagen 5.48. Sección de usuario. [A71]

Al hacer clic en el ícono se desplegará el siguiente submenú:

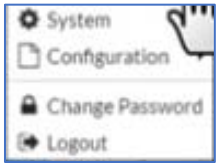


Imagen 5.49. Menú de usuario. [A72]

Posicionamos el cursor sobre **Configuration** para desplegar otro submenú:

Imagen 5.50. Menú en Configuration. [A73]

Seleccionamos la opción **Backup** para presentar la siguiente subinterfaz:

Imagen 5.51. Interfaz Backup. [A74]

Por defecto viene seleccionada la casilla **Local PC**, esto es para guardar el archivo de respaldo dentro del disco duro local en la máquina donde nos encontremos realizando la administración.

Otra casilla presentada es **USB Disk**, esto es en caso de que tengamos un dispositivo de almacenamiento masivo USB conectado en el puerto físico del Firewall para guardar el archivo de configuración de respaldo, esto se deja a consideración del administrador general de la red.

Una característica extra, es la posibilidad de habilitar encriptación al momento de crear el archivo de respaldo, esto es, se le añade una contraseña de seguridad al archivo, esto también se deja consideración al administrador de red, sin embargo, como buena práctica si decide habilitar la opción, se considera necesario documentar la contraseña, para evitar incidentes.

Cuando se requiera utilizar el archivo de configuración de respaldo, se elige **User->Configuration->Restore** y en la subinterfaz se presiona el botón **Restore from a Backup File**, y de igual manera dependiendo la interfaz a utilizar nos posicionamos en la casilla **Local PC** o **USB Disk**, seleccionamos el archivo .conf a utilizar para cargarlo.

Router con Access Point

Estando en el tablero principal elegimos **Herramientas del Sistema->Copia de Seguridad y Restauración**, para mostrar la siguiente pantalla:

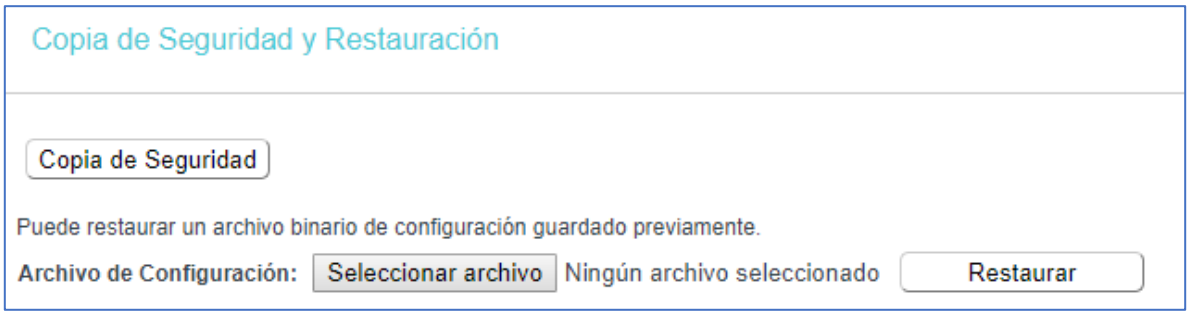


Imagen 5.52. Interfaz Copia de Seguridad. [A75]

Damos clic en el botón **Copia de Seguridad** para abrir una ventana de explorador de archivos del sistema operativo donde nos encontremos realizando el procedimiento, buscamos un directorio para alojar el archivo de configuración .bin.

Si deseamos restaurar el dispositivo con el archivo de respaldo, hacemos un proceso análogo, con la diferencia de que daremos clic en el botón **Seleccionar archivo** para buscar el archivo, una vez realizado esto, procedemos a dar clic en el botón **Restaurar**.

Esta práctica de seguridad aplica para **ambas propuestas**, pero, es muy recomendable contar con más de una copia de esos archivos, además de tenerlos almacenados en dispositivos de almacenamiento.

Con estas últimas características planteadas concluimos este capítulo, lo último a revisar a continuación son algunas consideraciones sobre adoptar las ideas sugeridas realizadas, mostrando ventajas y desventajas de considerar los planteamientos. También se analizará lo viable de adaptar algunas características de las propuestas con la infraestructura actual, y finalmente las posibilidades de mejora continua de la presente propuesta.

6. Consideraciones Económicas y Viabilidad.

Hasta este punto hemos revisado el contexto actual del Centro Tecnológico Aragón, y las necesidades de las áreas/laboratorios. Ante ello se hicieron una serie de propuestas para buscar mejorar el contexto y satisfacer la mayoría de las necesidades expuestas por las áreas/laboratorios del Centro Tecnológico.

Sin embargo, es necesario revisar el impacto de algunas consideraciones económicas sobre lo que se propone, con la finalidad de evaluar la viabilidad de lo que se plantea. Además, se añadirá como contrapeso el análisis del impacto en la funcionalidad, bajo la relación costo/beneficio de adoptar las sugerencias propuestas.

Con base en lo anterior, las consideraciones que revisaremos son con respecto a los dispositivos propuestos, a la actualización del cableado estructurado, y sobre lo viable que resulta adaptar los planteamientos con la infraestructura actual.

Posterior a ello, se ofrecerán algunos planteamientos para incorporar nuevas características, para mantener actualizada la infraestructura de red con prestaciones nuevas. Sumado a ello, se mencionará la viabilidad de adaptar lo propuesto anteriormente en unidades técnicas/administrativas de la Facultad de Estudios Superiores Aragón.

6.1. Justificación de Dispositivos de Red.

Partamos revisando el efecto económico ejercido por los dispositivos de red propuestos en el capítulo anterior. Recordemos que se ofrecieron 2 propuestas, a las cuales se les dieron los nombres de **Propuesta A** y **Propuesta B**.

Propuesta A

Para la primera de ellas se planteó la inclusión de un Firewall **FortiGate 60E**, el cual si se desea adoptar implica tener presente sus impresiones económicas, en ese sentido el dispositivo ronda en un rango de precios desde los **$1,100 CAD ~ $1,500**

CAD (Precio en Dólar Canadiense), dependiendo del distribuidor, lo cual en tipo de cambio actual en peso mexicano (1 CAD = 17 MXN) el rango es de los **$18,700 MXN ~$25,500 MXN**.

Ese precio se considera accesible tomando en cuenta que va a proveer a todo el centro, por consiguiente, todas las áreas/laboratorios pueden tener acceso a las prestaciones que ofrece el dispositivo.

Continuando con las consideraciones económicas en la **Propuesta A**, otro instrumento presentado es el Switch **TP-LINK Modelo TL-SG1024D**, cuya función principal es alojar la Zona Desmilitarizada **DMZ** para la instalación de los servidores en un ambiente aislado del resto de la infraestructura.

Si se desea adoptar el dispositivo, su precio ronda entre **$2,100 MXN ~ $2,500 MXN**, por lo que su adquisición presenta un bajo efecto económico, tomando en cuenta que va a servir para toda la unidad, facilitando la inclusión de servidores a voluntad de las áreas/laboratorios.

Propuestas A y B

En ambas propuestas se planteó la inclusión de dispositivos Router con Access Point, específicamente los modelos **TP-LINK TL-WR840N**, los cuales tienen la finalidad de crear pequeñas redes privadas inalámbricas para las áreas/laboratorios, ofreciendo salida a Internet particular a prestadores de servicio social o a colaboradores/becarios de proyectos temporales.

El costo del dispositivo ronda entre los **$300 MXN ~$350 MXN**, por lo que su adquisición resulta ampliamente flexible, en comparación de las características que este ofrece, de las cuales se hablaron en el capítulo anterior.

Relación Costo/Beneficio de las propuestas

Después de haber hecho un análisis económico concreto sobre los dispositivos propuestos, es pertinente hacer una comparativa sobre los efectos de si/no adquirir de dichos instrumentos.

Actualmente se encuentra muy expuesta la infraestructura de red, por consiguiente, todas las áreas/laboratorios comparten el mismo contexto, los efectos de esa condición son la existencia de múltiples riesgos y amenazas, mismas que pueden llegar a tener las siguientes consecuencias:

- Continuo deterioro en los dispositivos de red.
- Incremento continuo de problemas de funcionamiento de la infraestructura de red.
- Daños o problemas en dispositivos de los sitios principales de la infraestructura de red.
- Daños o problemas de impacto variable sobre las computadoras o recursos privados de las áreas/laboratorios.
- Filtración de información privada en el tráfico generado por las áreas/laboratorios.
- Infiltración de atacantes pasivos/activos dentro de la infraestructura de red.
- Posibilidad de secuestro de la información privada sensible.
- Punto de entrada no solo para la unidad sino para las demás secciones de la Facultad.

En términos financieros, si suceden los peores casos de siniestro por parte de las amenazas y riesgos, esto se puede traducir en los siguientes impactos económicos:

- El secuestro o alteración grave de información presenta un costo indeterminado, por tanto, resulta invaluable hacer una precisión económica.
- Si algún dispositivo de red como un Switch se daña, el reemplazarlo tiene un costo aproximado de **$7,000 MXN** dado que son de tipo administrable.
- En el caso menos deseable el cual es que varios o todos los dispositivos de los sitios en el CTA se dañen por algún ataque, la pérdida puede traducirse en un rango de **$21,000 MXN** hasta los **$63,000 MXN**.
- El daño de algún recurso de red como una impresora (considerando el caso hipotético que exista una para toda la unidad) podría verse reflejado en una pérdida estimada de **$8,000 MXN**.

- El daño de un solo equipo de cómputo es de alrededor **$8,000 MXN**, si el impacto de un ataque es a gran escala (todas las áreas/laboratorios) puede crecer de forma casi exponencial.
- Siguiendo el punto anterior, suponiendo que en toda la unidad existan un estimado de 25 a 30 equipos de cómputo (número del que tan solo el laboratorio de cómputo cuenta con la mitad), si todos esos equipos resultan dañados por el ataque la pérdida asciende a un estimado de **$240,000 MXN**.

Costo en Propuesta A	Costo en Propuesta B	Costo de Riesgo en menor impacto	Costo de Riesgo en el peor caso
$31,850 MXN	$3,850 MXN	$37,000 MXN	$311,000 MXN

Tabla 6.1. Costos. [TA11]

Entonces el impacto total en el peor de los casos ronda en los **$311,000 pesos MXN**.

En contraparte el impacto económico global de la adquisición de los dispositivos planteados, considerando el precio más elevado, la suma aproximada de la obtención de estos es de **$31,850 pesos MXN**, por lo que en una comparativa la inversión requerida es 10 veces menor a las pérdidas potenciales. Eso sin tomar en cuenta que la pérdida de información es invaluable.

Lo anterior nos hace ver un beneficio con escala 10 a 1, por lo que el gasto se vuelve muy redituable.

Por otra parte, respecto a funcionamiento, en el capítulo anterior se mencionaron características con las que cuentan los dispositivos, por lo que el panorama pasaría de un contexto en el que existen casi nulas prácticas de seguridad y un tráfico desmedido. A uno en el que existirían desde las prácticas más elementales en materia de seguridad, hasta la posibilidad de crear políticas especializadas de seguridad, además, de que se contaría con un control del tráfico, garantizando que exista conectividad eficiente para todo el centro.

6.2. Justificación de Cableado Estructurado.

Otra cuestión que se ha propuesto es la actualización del cableado estructurado, esto tiene la intención de proveer canales de comunicación con estándares nuevos, incrementando los índices de eficiencia.

En contraparte, el cableado actual presenta los siguientes detalles por considerar:

- Presenta la misma cantidad de años que el Centro Tecnológico Aragón.
- No todos los nodos “instalados” funcionan.
- La velocidad de ancho de banda máximo a alcanzar es de **100 Mbps**, el cual se considera por debajo a comparación con centros de investigación en otras universidades.
- No ofrecen la cualidad de poder adoptar servicios **Voz sobre IP**.
- No se cuenta con identificación física de todos los nodos, por lo que dificulta la tarea de documentar adecuadamente los nodos en un diagrama.

Ahora bien, durante la elaboración de la presente propuesta de actualización, surgió la iniciativa de hacer una valoración de actualizar el cableado estructurado, por parte del administrador general de la red de la Facultad de Estudios Superiores Aragón, y el administrativo encargado de coordinar ese tipo de proyectos.

En dicho proceso, algunas empresas dedicadas a ofrecer esa clase de servicio enviaron propuestas económicas, las cuales rondaban en precios desde los **$295,000 MXN**.

Las ventajas de considerar la financiación son:

- Los canales de comunicación tendrán estándares de comunicación recientes.
- Las velocidades de transmisión serán mucho mayores a **100 Mbps**.
- Se podrá realizar la etiquetación y documentación de todos los nodos.
- Se podrá considerar la inclusión de servicios **Voz sobre IP**, cuando se desee dejar atrás las tecnologías analógicas en las comunicaciones por voz.

- Personal capacitado dará la solución, lo que ofrece precisión o una atención inmediata ante situaciones de falla.

Por otro lado, si se quisiera prescindir de este planteamiento, hay que considerar que los precios tanto de los componentes como del servicio pueden presentar incrementos incalculables, debido a la volatilidad continua del mercado, por lo que a la larga puede representar una inversión mayor.

Después de haber hecho los análisis costo/beneficio respecto a todo lo propuesto, revisemos la factibilidad de implementar alguno de los planteamientos conservando la infraestructura actual.

6.3. Justificación de Viabilidad con la Infraestructura Actual.

Supongamos que no se desea instaurar ninguno de los dispositivos planteados ¿sería posible llevar a cabo alguna de las ideas detrás propuestas?, una respuesta breve es sí es posible, pero realmente solo muy pocas cosas se pueden realizar, concretamente el manejo de puertos de comunicación por cada computadora perteneciente a la infraestructura.

Esto se realiza desde el firewall del sistema operativo de la computadora, brindando algunos controles de seguridad, pero el impacto solo se limitaría a la computadora que se ha configurado, por lo que los problemas ajenos a ella no se resolverían.

En pocas palabras es muy **poco viable** ver mejoras si se mantiene la infraestructura sin cambios.

Otro caso por suponer es considerar solo la **Propuesta B**, sobre la infraestructura actual sin presentar cambios en su cableado estructurado. En este contexto, **es viable**, pero con algunas consideraciones que se tienen que resolver previo a la instalación de los dispositivos planteados.

Concretamente realizar el etiquetado de los nodos, ya que es imprescindible contar con al menos un nodo dedicado para la instalación del Router con Access Point propuesto. Dicho etiquetado es recomendable que se realice con personal

capacitado, de lo contrario pueden surgir problemas de precisión en el procedimiento.

Y el último caso a suponer, es considerar la **Propuesta A**, sobre la infraestructura actual sin presentar cambios en el cableado, y sin la instalación del Switch dedicado. Este contexto **es viable**, pero también presenta consideraciones por resolver previo a instalar los dispositivos.

Nuevamente está el tema del etiquetado de los nodos, sumado a que se tendrían que hacer configuraciones adicionales en puertos de alguno de los Switch para los que se vaya a reservar la **DMZ**, eso no mantendría aislada dicha zona de los servidores, además de que limitaría el número de estos a instalar. En ese sentido los efectos se ven en que siguen formando parte de la infraestructura, representando un posible punto de entrada para las amenazas existentes en Internet.

Dicho todo esto, a continuación, cerraremos el presente capítulo con algunas premisas para la extensión y actualización de las propuestas realizadas.

6.4. Bases para expansión y actualización.

A lo largo de la propuesta, se han realizado planteamientos para mejorar el contexto actual de la infraestructura de red del Centro Tecnológico Aragón, los cuales son posibles materializar mediante los dispositivos de red sugeridos. Esos dispositivos, ofrecen la posibilidad de cubrir la mayoría de las necesidades expuestas por parte de las áreas/laboratorios.

Sin embargo, no se limitan solo a satisfacer dichas necesidades, por el contrario, ofrecen la posibilidad de incluir más características, posicionándonos en la **Propuesta A** se destacan las siguientes:

- ✓ Posibilidad de crear túneles VPN para conexiones privadas.
- ✓ Poner restricciones en puertos de comunicación para interfaces físicas, VLAN, DMZ.
- ✓ Creación de políticas de seguridad para servicios **VoIP**.

- ✓ Control de tráfico para servicios **VoIP**.
- ✓ Configuraciones especiales para servicios de **Alta Disponibilidad**.
- ✓ Bloqueo de contenidos en redes sociales, excepto en los casos que se trate de grupos de trabajo.
- ✓ Bloqueos de inspecciones comunes por atacantes pasivos.
- ✓ Servicio de antivirus para el Firewall y para la infraestructura a la vez.

Del lado de la **Propuesta B** podemos incluir las siguientes características:

- ✓ Bloqueo específico de la red privada a ciertos dispositivos.
- ✓ Espacios dedicados a computadoras de conexión constante.
- ✓ Servicio de control parental para limitar acceso a algunos usuarios por tiempo y contenidos.
- ✓ Capacidad de establecer técnicas de ruteo avanzadas.

Lo dicho anteriormente, representan actualizaciones constantes a adoptar conforme se maneje un mayor número de conceptos e ideas, en temas de redes y seguridad.

Por otra parte, con expansión nos referimos a que todas las ideas planteadas, no se limitan solamente a servir al Centro Tecnológico Aragón, pueden adaptarse a cualquier unidad de la Facultad de Estudios Superiores Aragón, e inclusive a la Universidad en general.

Ya que solo se deben adaptar los planteamientos, de acuerdo a la infraestructura de la unidad que lo desee incorporar, es por ello que las configuraciones propuestas tienen una estructura similar a la de algún manual técnico, ya que la intención es incentivar al personal con conocimientos básicos a llevar a cabo los planteamientos con la mayor precisión posible.

Incluso el presente documento puede fungir como guía al momento de elaborar la documentación técnica.

En términos simples, la expansión la define el interesado en llevar a cabo los planteamientos expuestos a lo largo de esta propuesta, con base en las necesidades de la unidad o incluso con base en sus necesidades profesionales.

Y así concluimos la presente propuesta, destacando que la intención principal de la misma es servir en cualquier contexto en el que pueda ser aplicada, ofreciendo algunos conceptos e ideas en pro de ofrecer alternativas de solución y actualización.

7. Conclusiones.

La realización de la propuesta fue un incentivo para poner en práctica las técnicas y los conocimientos adquiridos, a lo largo de la etapa de estudiante de Ingeniería en Computación. Además de fomentar la disposición por adquirir prácticas adicionales, con la intención de ofrecer un planteamiento más integral.

Fue muy grato el proceso a realizar, desde proceder a investigar, documentar, y analizar un contexto, debido a que no solamente se puso en práctica los conocimientos manejados en condición de egresado, sino que también requirió buscar conceptos adicionales para dar fundamento a planteamientos surgidos del análisis del contexto.

Como egresado puedo mencionar con agrado que los conocimientos adquiridos en el aula fueron una base sólida para adquirir nuevas ideas, sin tener que pasar por un complejo proceso de adaptación, en ese sentido, la Facultad de Estudios Superiores Aragón ofrece conocimiento de calidad, con posibilidades de sentar cimientos para actualización.

La propuesta reafirmó mi interés en desarrollar mis habilidades profesionales orientadas hacia el área de redes de computadoras y seguridad, ya que con júbilo puedo expresar el gozo que sentí en ser orientado a desarrollar la investigación, el análisis y los planteamientos para poder ofrecer alternativas de solución, quizá elementales pero la disciplina de Ingeniería busca la solución de problemas.

Debo señalar que la breve experiencia profesional adquirida, en una oportunidad laboral temporal ofrecida, fortaleció en gran medida los planteamientos realizados a lo largo del diseño de la propuesta, esto me permite argumentar que, si solo limitamos el conocimiento a lo que se adquiere en el aula, es posible ofrecer soluciones, pero el alcance de las soluciones presentará numerosas áreas de oportunidad.

Entonces, me atrevo a subrayar la importancia de tener la apertura de adquisición constante de conocimiento fuera del aula, ya sea mediante cursos extracurriculares o en adquirir responsabilidades laborales acorde al nivel que se posee como estudiante.

Siguiendo la idea anterior, también es de suma importancia tener bases muy sólidas en todas las áreas de conocimiento ofrecidas a lo largo de la carrera, ya que guardan una relación estrecha, resultando muy común el contexto en el que se deba manejar conocimiento de más de un área en el ámbito laboral.

Respecto a la propuesta se pudo mostrar el contexto actual del Centro Tecnológico Aragón, destacando algunas áreas de oportunidad para mejorar el funcionamiento, a nivel técnico y en materia de seguridad.

Para lo anterior, primero se consideró importante revisar algunos conceptos elementales en materia de redes y seguridad, esta razón fue incentivo suficiente para desarrollar una base teórica, con intención de ofrecer una retroalimentación al estudiante/practicante/egresado interesado en llevar a cabo la implementación de la propuesta.

Por otra parte, los planteamientos desarrollados contienen prácticas básicas a adoptar, las cuales con agrado se puede afirmar que permiten dar alternativas de solución, para mejorar el contexto de los espacios de trabajo dentro del Centro Tecnológico Aragón.

Finalmente, es posible expresar la satisfacción de haber podido desarrollar una base técnica a mejorar para el uso de cualquier académico o estudiante, o al menos fomentar una iniciativa de mejora en donde se pueda aplicar la propuesta ofrecida.

8. Referencias.

Imágenes

- A1: Imagen 2.1 Representación gráfica de un Switch. Elaboración Propia
- A2: Imagen 2.2 Representación gráfica de un Router. Elaboración Propia
- A3: Imagen 2.3 Representación gráfica de un Access Point. Elaboración Propia
- A4: Imagen 2.4 Representación gráfica de un Firewall. Elaboración Propia
- A5: Imagen 2.5 Topología de Tipo Árbol. Elaboración Propia
- A6: Imagen 2.6 Funcionamiento de Internet. Elaboración Propia
- A7: Imagen 2.7 Wi-Fi de Infraestructura. Elaboración Propia
- A8: Imagen 2.8 Red Ad-hoc. Elaboración Propia
- A9: Imagen 2.9 Modelo OSI, funciones en capas. Elaboración Propia
- A10: Imagen 2.10 Modelo OSI, flujo de comunicación. Elaboración Propia
- A11: Imagen 2.11 Factores de Riesgo y Daño Potencial. Elaboración Propia
- A12: Imagen 2.12. Zona Desmilitarizada. Elaboración Propia
- A13: Imagen 3.1. Site Principal. Elaboración Propia
- A14: Imagen 3.2. Espacio de Comunicación en el primer piso. Elaboración Propia
- A15: Imagen 3.3. Espacio de Comunicación en el segundo piso. Elaboración Propia
- A16: Imagen 3.4. Distribución Actual PB. Plano Elaborado por Ing. Manuel Arellano, Edición Propia
- A17: Imagen 3.5. Distribución Actual P1. Plano Elaborado por Ing. Manuel Arellano, Edición Propia
- A18: Imagen 3.6. Distribución Actual P2. Plano Elaborado por Ing. Manuel Arellano, Edición Propia
- A19: Imagen 3.7. Modelo de Red Actual. Elaboración Propia
- A20: Imagen 3.8. Pregunta 3. Elaboración Propia

- A21: Imagen 3.9. Pregunta 4. Elaboración Propia
- A22: Imagen 3.10. Pregunta 5. Elaboración Propia
- A23: Imagen 3.11. Pregunta 6. Elaboración Propia
- A24: Imagen 5.1. Topología Actual. Elaboración Propia
- A25: Imagen 5.2. Topología Propuesta A. Elaboración Propia
- A26: Imagen 5.3. Topología Propuesta B. Elaboración Propia
- A27: Imagen 5.4. Planta Baja. Plano Elaborado por Ing. Manuel Arellano, Edición Propia
- A28: Imagen 5.5. Primer Piso. Plano Elaborado por Ing. Manuel Arellano, Edición Propia
- A29: Imagen 5.6. Segundo Piso. Plano Elaborado por Ing. Manuel Arellano, Edición Propia
- A30: Imagen 5.7. VLAN en Topología A. Elaboración Propia
- A31: Imagen 5.8. Opciones en interfaz Ethernet. Elaboración Propia
- A32: Imagen 5.9. Asignación IP. Elaboración Propia
- A33: Imagen 5.10. Tablero principal FortiGate. Elaboración Propia
- A34: Imagen 5.11. Tablero de FortiView. Elaboración Propia
- A35: Imagen 5.12. Enlaces troncales VLAN. Elaboración Propia
- A36: Imagen 5.13. Ruta Estática. Elaboración Propia
- A37: Imagen 5.14. Política IPv4 para Internet. Elaboración Propia
- A38: Imagen 5.15. Opción Firmware. Elaboración Propia
- A39: Imagen 5.16. Interfaces LAN. Elaboración Propia
- A40: Imagen 5.17. Addresses. Elaboración Propia
- A41: Imagen 5.18. Login en Router. Elaboración Propia
- A42: Imagen 5.19. Tablero principal en Router. Elaboración Propia
- A43: Imagen 5.20. Cambio de contraseña. Elaboración Propia
- A44: Imagen 5.21. Opciones en modo de operación. Elaboración Propia
- A45: Imagen 5.22. Enlace WAN. Elaboración Propia
- A46: Imagen 5.23. Enlace WAN estático. Elaboración Propia
- A47: Imagen 5.24. Enlace LAN. Elaboración Propia

- A48: Imagen 5.25. Configuraciones Inalámbricas. Elaboración Propia
- A49: Imagen 5.26. Seguridad Inalámbrica. Elaboración Propia
- A50: Imagen 5.27. Acceso WPS. Elaboración Propia
- A51: Imagen 5.28. Opciones para servicio DHCP. Elaboración Propia
- A52: Imagen 5.29. Formulario Traffic Shaper. Elaboración Propia
- A53: Imagen 5.30. Traffic Shaping Policies. Elaboración Propia
- A54: Imagen 5.31. Formulario Shaping Policy. Elaboración Propia
- A55: Imagen 5.32. Traffic Shaper creado. Elaboración Propia
- A56: Imagen 5.33. Campo de horario. Elaboración Propia
- A57: Imagen 5.34. Control de Ancho de Banda. Elaboración Propia
- A58: Imagen 5.35. Red para invitados. Elaboración Propia
- A59: Imagen 5.36. Categorías de Web Filter. Elaboración Propia
- A60: Imagen 5.37. Añadir perfiles Web Filter. Elaboración Propia
- A61: Imagen 5.38. Agregando Web Filter. Elaboración Propia
- A62: Imagen 5.39. Reglas de Control de Acceso. Elaboración Propia
- A63: Imagen 5.40. Añadiendo regla. Elaboración Propia
- A64: Imagen 5.41. Agregando destino. Elaboración Propia
- A65: Imagen 5.42. Infraestructura DMZ. Elaboración Propia
- A66: Imagen 5.43. Interfaz DMZ. Elaboración Propia
- A67: Imagen 5.44. Configurando interfaz. Elaboración Propia
- A68: Imagen 5.45. Agregando características de seguridad. Elaboración Propia
- A69: Imagen 5.46. Interfaz Virtual IPs. Elaboración Propia
- A70: Imagen 5.47. Formulario Virtual IP. Elaboración Propia
- A71: Imagen 5.48. Sección de usuario. Elaboración Propia
- A72: Imagen 5.49. Menú de usuario. Elaboración Propia
- A73: Imagen 5.50. Menú en Configuration. Elaboración Propia
- A74: Imagen 5.51. Interfaz Backup. Elaboración Propia
- A75: Imagen 5.52. Interfaz Copia de Seguridad. Elaboración Propia

Figuras

- B1: Figura 1.4. Componentes de un sistema de comunicaciones. Basado de Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.2. Editado por M. en C. Felipe de Jesús Gutiérrez López
- B2: Figura 2.8. Cable de par trenzado no apantallado (UTP). Recuperado de Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 36
- B3: Switch Cisco Administrable. Recuperado de https://http2.mlstatic.com/switch-cisco-smb-sg200-10fp-admin-l2-8-puertos-gigabit-poe-D_NQ_NP_867508-MEC25749326560_072017-O.webp (30/09/2018)
- B4: Switch TP-Link Plug & Play. Recuperado de https://www.euronics.ee/UserFiles/Products/Images/173202-switch-tplink-2-medium.png (30/09/2018)
- B5. Router Cisco. Recuperado de https://static.fnac-static.com/multimedia/Images/ES/MC/07/60/4f/5201927/1540-1/tsp20161006161041/Router-Cisco-RV325-VPN-Router-con-filtrado-web.jpg#17ddaf1e-fd78-4dce-bde8-55c8c22a7ee1 (30/09/2018)
- B6: Router Linksys. Recuperado de https://assets.pcmag.com/media/images/479347-linksys-wrt32x-wi-fi-gaming-router.jpg?width=333&height=245 (30/09/2018)
- B7: Access Point Cisco. Recuperado de https://http2.mlstatic.com/punto-de-acceso-inalambrico-cisco-aironet-1042n-access-point-D_NQ_NP_13386-MLM2950587913_072012-F.webp (30/09/2018)
- B8: Firewall Fortigate 200D. Recuperado de http://firewall-chile.cl/wp-content/uploads/2017/08/Firewall-200D-2.png (30/09/2018)
- B9: Figura 1.7. Señales analógica y digital. Recuperado de Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 17

- B10: Figura 1.9. Codificación de una señal analógica en forma digital: muestreo de la señal. Recuperado de Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 18
- B11: Figura 1.10. Modulación por desplazamiento de amplitud. Recuperado de Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 18
- B12: Figura 6.88. Segmentación con VLAN. Recuperado de Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.212
- B13: Figura 6.87. Segmentación LAN Tradicional. Recuperado de Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.212
- B14: Figura 6.98. NAT o IP masquerade. Recuperado de Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo. P.220
- B15: Traffic Shaping. Recuperado de https://cookbook.fortinet.com/traffic-shaping-bandwidth-54/ (30/09/2018)
- B16: Fortigate 60E. Recuperado de https://images-na.ssl-images-amazon.com/images/I/51fGiaWn26L._SL1500_.jpg (07/02/2019)
- B17: Fortigate 60 E. Recuperado de https://images-na.ssl-images-amazon.com/images/I/61SGJcuZAeL._SL1500_.jpg (07/02/2019)
- B18: TP-LINK TL-SG1024D. Recuperado de https://images-na.ssl-images-amazon.com/images/I/61Ua5pMskuL._SL1280_.jpg (26/02/2019)
- B19: TP-LINK TL-WR840N. Recuperado de https://images-na.ssl-images-amazon.com/images/I/31W-T8eciQL.jpg (07/02/2019)
- B20: TP-LINK TL-WR840N. Recuperado de https://images-na.ssl-images-amazon.com/images/I/31jnhWIR8PL.jpg (07/02/2019)
- B21: APC Power Back-UPS. Recuperado de https://images-na.ssl-images-amazon.com/images/I/811l9ylkJuL._SL1500_.jpg (11/02/2019)

- B22: Cable UTP-Cat 6. Recuperado de https://www.conectronica.com/images/stories/CONECTRONICA190/cable-belden-w.jpg (07/02/2019)
- B23: Figura 4.4. Dirección IP en notación binaria y decimal. Recuperado de Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 101
- B24: Recuperado de https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/aee3fe4e-1a08-11e9-9685-f8bc1258b856/fortigate-generic-cookbook-qsg.pdf (21/02/2019) P.4
- B25: Recuperado de https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/aee3fe4e-1a08-11e9-9685-f8bc1258b856/fortigate-generic-cookbook-qsg.pdf (21/02/2019) P.5
- B26: Recuperado de https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/aee3fe4e-1a08-11e9-9685-f8bc1258b856/fortigate-generic-cookbook-qsg.pdf (21/02/2019) P.5
- B27: Recuperado de https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/aee3fe4e-1a08-11e9-9685-f8bc1258b856/fortigate-generic-cookbook-qsg.pdf P.4
- B28: Recuperado de https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/aee3fe4e-1a08-11e9-9685-f8bc1258b856/fortigate-generic-cookbook-qsg.pdf (21/02/2019) P.5
- B29: Recuperado de https://cookbook.fortinet.com/fortigate-registration-and-basic-settings-60/ (26/02/2019)
- B30: Recuperado de https://cookbook.fortinet.com/fortigate-registration-and-basic-settings-60/ (26/02/2019)

- B31: Recuperado de https://cookbook.fortinet.com/fortigate-registration-and-basic-settings-60/ (26/02/2019)
- B32: Recuperado de https://cookbook.fortinet.com/fortigate-registration-and-basic-settings-60/ (26/02/2019)
- B33: Recuperado de Fortinet, Inc. (2015). FortiOS Handbook System Administration. Canada: Fortinet Publications. P.214
- B34: Recuperado de Fortinet, Inc. (2018). The Fortinet Cookbook. agosto 28, 2018, de Fortinet, Inc Sitio web: https://cookbook.fortinet.com/
- B35: Recuperado de https://static.tp-link.com/2018/201802/20180202/7106507931_TL-WR840N(ES)_QIG.pdf (23/02/2019) P.1
- B36: Recuperado de https://cookbook.fortinet.com/fortigate-registration-and-basic-settings-60/ (26/02/2019)
- B37: Recuperado de https://www.youtube.com/watch?v=xtuPNzNrPfI (26/02/2019)

Tablas

- TA1: Elaboración basada de Table 2-1 *Common Security Policies*. Recuperada de Thomas, T. & Stoddard, D. (2012). Network Security First-Step. Indianapolis, EE. UU.: Cisco Press. P.49. Editado por M. en C. Felipe de Jesús Gutiérrez López
- TA2: Tabla 3.1. Lista de Nodos. Elaboración Propia
- TA3: Tabla 3.2. Direccionamiento actual. Tabla elaborada por M. en C. Jesús Hernández Cabrera. Edición Propia y optimizada por M. en C. Felipe de Jesús Gutiérrez López
- TA4: Tabla 5.1. Lista de nodos con expansión. Elaboración Propia. Editado por M. en C. Felipe de Jesús Gutiérrez López
- TA5: Tabla 5.2. Jerarquía de VLAN. Elaboración Propia. Editado por M. en C. Felipe de Jesús Gutiérrez López
- TA6: Tabla 5.3. Clases de Direccionamiento IPV4. Elaboración basada de Tabla 4.1. Clases de Direcciones IP. Recuperada de Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P. 101
- TA7: Tabla 5.4. Direccionamiento CTA. Elaboración Propia
- TA8: Tabla 5.5. Direccionamiento privado para Router con AP. Elaboración Propia
- TA9: Tabla 5.6. Controles de Ancho de Banda. Elaboración Propia
- TA10: Tabla 5.7. Contenidos en Internet. Elaboración Propia. Editado por M. en C. Felipe de Jesús Gutiérrez López
- TA11: Tabla 6.1. Costos. Elaboración Propia. Editado por M. en C. Felipe de Jesús Gutiérrez López
- TB1: Tabla 2.2. Categorías de cable de par trenzado. Basado de Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo. P.37. Editado por M. en C. Felipe de Jesús Gutiérrez López

Bibliografía

- Moro, M. (2013). Infraestructuras de redes de datos y sistemas de telefonía. España: Paraninfo
- Fortinet, Inc. (2018). FortiOS 6.0. agosto 28, 2018, de Fortinet, Inc. Sitio web: http://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortiOS-HTML5-v2/Home.htm
- Fortinet, Inc. (2018). FortiOS Handbook 6.0.2. agosto 28, 2018, de Fortinet, Inc Sitio web: https://docs.fortinet.com/uploaded/files/4320/fortios-handbook-60.pdf
- Fortinet, Inc. (2015). FortiOS Handbook System Administration. Canada: Fortinet Publications
- Castelli, M. (2005). LAN Switching first-step. Indianapolis, EE. UU.: Cisco Press
- INCIBE. (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? , diciembre 10, 2018, de INCIBE Sitio web: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
- ISACA. (2015). Manual de Preparación para el Examen CISA. EE. UU: ISACA
- Thomas, T. & Stoddard, D. (2012). Network Security First-Step. Indianapolis, EE. UU.: Cisco Press
- Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. México: Pearson
- Romero, M., Barbancho, J., Benjumea, J., Rivero, O., Ropero, J., Sánchez, G. & Sivianos, F. (2010). Redes locales. España: Paraninfo
- Fortinet, Inc. (2018). The Fortinet Cookbook. agosto 28, 2018, de Fortinet, Inc Sitio web: https://cookbook.fortinet.com/
- Quanti. (2018). FortiGate 60E Datos técnicos. febrero, 7, 2019, de Solutions S.A. de C.V. Sitio web: https://www.quanti.com.mx/fortigate-60e-datos-tecnicos/