UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

DESARROLLO DE UN MODELO DE SEGURIDAD PARA REDES DE AREA LOCAL

PINCAY ROMERO KELVIN GIOVANNI
INGENIERO DE SISTEMAS

MACHALA
2021

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

DESARROLLO DE UN MODELO DE SEGURIDAD PARA REDES DE AREA LOCAL

PINCAY ROMERO KELVIN GIOVANNI
INGENIERO DE SISTEMAS

MACHALA
2021

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO TITULACIÓN
PROPUESTAS TECNOLÓGICAS

DESARROLLO DE UN MODELO DE SEGURIDAD PARA REDES DE AREA LOCAL

PINCAY ROMERO KELVIN GIOVANNI
INGENIERO DE SISTEMAS

MOROCHO ROMAN RODRIGO FERNANDO

MACHALA, 27 DE SEPTIEMBRE DE 2021

MACHALA
2021

Titulacion_PincayKelvin_20210920

INFORME DE ORIGINALIDAD

6%	4%	0%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	culturacion.com Fuente de Internet	1%
2	Submitted to Melbourne Institute of Technology Trabajo del estudiante	<1%
3	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1%
4	Submitted to Universidad Carlos III de Madrid Trabajo del estudiante	<1%
5	es.scribd.com Fuente de Internet	<1%
6	manejoderedesconaleptlalpan1grup-608.blogspot.com Fuente de Internet	<1%
7	Submitted to Fundacion Universitaria Juan de Castellanos Trabajo del estudiante	<1%
8	Submitted to Universidad Catolica De Cuenca Trabajo del estudiante	

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, PINCAY ROMERO KELVIN GIOVANNI, en calidad de autor del siguiente trabajo escrito titulado DESARROLLO DE UN MODELO DE SEGURIDAD PARA REDES DE AREA LOCAL, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 27 de septiembre de 2021

PINCAY ROMERO KELVIN GIOVANNI
0704411016

DEDICATORIA

El presente trabajo se lo dedico principalmente a Dios, ya que gracias a su bendición he podido cumplir cada una de mis metas, tanto en la parte académica, profesional y personal, dándome las fuerzas necesarias para no decaer.

A mi padre y mis abuelos quienes estuvieron desde el principio, en las buenas y malas hasta este momento y me brindaron el apoyo incondicionalmente, a mi familia en general que estuvieron conmigo durante toda esta etapa, me supieron aconsejar y sobre todo con mis seres más allegados que lastimosamente hoy no están conmigo pero que desde el cielo me iluminan y comparten este logro alcanzado.

De Igual forma a mis maestros, los cuales supieron inculcarme de conocimientos y valores de la mejor manera, a mis compañeros, colegas y amigos en general que de alguna u otra manera estuvieron apoyándome en este proceso.

AGRADECIMIENTO

Agradecer habla bien del corazón y hace que tu corazón hable, de esta forma en primer lugar agradezco a Dios ya que gracias a la fortaleza y vigor que me brinda hoy estoy consiguiendo mis objetivos.

A mi padre que siempre me apoyó en toda circunstancia como persona y profesional, a mi madre que desde el cielo me ilumina y me da las fuerzas necesarias para seguir adelante, mis abuelos quienes estuvieron conmigo en las buenas y malas a pesar de todo y de las adversidades.

Finalmente expreso mi grato y sincero agradecimiento a mis seres queridos que estuvieron conmigo en todo el proceso brindándome apoyo incondicional y que hoy me bendicen desde el cielo, a mi tutor, el Ing. Rodrigo Fernando Morocho Román por su gran ayuda, colaboración para despejar todas mis interrogantes en el desarrollo del presente trabajo, y gracias a él he adquirido sabios conocimientos que me van a servir en la etapa profesional.

RESUMEN

En la actualidad, la interconectividad global se ha vuelto un recurso importante y necesario para la comunicación personal y laboral, una de las tecnologías para esta comunicación es el internet, debido a que permite estar conectado con múltiples personas entre los cuales pueden ser amigos, familiares, etc. Esta comunicación se realiza mediante los ordenadores, dispositivos móviles, entre otras herramientas, a través de una red o conjunto de redes informáticas.

La red de computadores que se describe como un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos y las cuales comparten información, dicha información en la mayoría de veces es de gran relevancia para los usuarios, por ende se debe tomar en cuenta varios aspectos con respecto a las redes, y una de las más importantes es la seguridad que debe brindarse a la misma, existen diferentes tipos de redes, en el presente trabajo se aborda la red de área local con los diferentes controles de seguridad que esta conlleva.

Mediante el presente trabajo se plantea primeramente analizar modelos que existen en cuanto a redes locales ya que si bien no existe un modelo como tal que permita asegurar una LAN tomando en cuenta los aspectos o áreas que la conforman, se puede obtener información relevante lo cual ayuda a identificar las principales vulnerabilidades y medidas que se pueden abarcar para crear un modelo óptimo de seguridad, todo lo mencionado se lo realiza en base a la recolección de información en fuentes científicas, tanto artículos de revistas científicas reconocidas, así como de algunas fuentes externas como el internet e incluso con experiencias de encargados en el área de sistemas y seguridad informática de diferentes empresas principalmente en el cantón Pasaje, para posteriormente tomar las medidas adecuadas que sirvan para armar el modelo de seguridad donde se destaca varios aspectos en ítems importantes que conforman la red local como su infraestructura así como también su conexión inalámbrica y establecimiento de políticas de seguridad, luego dichos controles aplicarlos a una red local en una empresa, teniendo como objetivo el de proponer un modelo de red de área local con un enfoque de seguridad usando las mejores prácticas, garantizando así la

integridad y disponibilidad de la infraestructura existente en una organización, ya que es primordial para un adecuado servicio de sus diferentes funciones dentro de la misma.

Los resultados obtenidos como consecuencia del trabajo planteado es la creación de un modelo de red de área local, la cual se puede determinar como satisfactoria debido a que dicha propuesta fue revisada y evaluada por diferentes profesionales encargados en la seguridad de una LAN de las empresas encuestadas, donde se destaca que el modelo estuvo focalizado en las áreas correctas que conforma la red local así como que los controles que se especifican en el mismo, si cumplen con los objetivos deseados ya que se aplicaron las mejores prácticas, permitiendo ser un gran aporte para empresas que desean asegurar su red de área local, ya que estos controles brindan seguridad y operatividad de la organización.

Palabras clave:

Red de computadoras, LAN, VLAN, WLAN, Seguridad, Políticas de seguridad.

ABSTRACT

Currently, global interconnectivity has become an important and necessary resource for personal and work communication, one of the technologies for this communication is the internet, because it allows you to be connected with multiple people, including friends, family , etc. This communication is done through computers, mobile devices, among other tools, through a network or set of computer networks.

The computer network that is described as a set of equipment connected by means of cables, signals, waves or any other method of data transport and which share information, said information in most times is of great relevance to users, Therefore, several aspects must be taken into account with respect to networks, and one of the most important is the security that must be provided to it, there are different types of networks, in this work the local area network is addressed with the different security controls that this entails.

Through the present work, it is first proposed to analyze existing models in terms of local networks since although there is no model as such that allows ensuring a LAN taking into account the aspects or areas that make it up, relevant information can be obtained which helps to identify the main vulnerabilities and measures that can be covered to create an optimal security model, all the aforementioned is done based on the collection of information in scientific sources, both articles from recognized scientific journals, as well as from some external sources such as the internet and even with experiences of managers in the area of systems and computer security of different companies mainly in the canton Pasaje, to later take the appropriate measures that serve to build the security model where several aspects are highlighted in important items that make up the local network as its infrastructure as well as its wireless connection a and establishment of security policies, then these controls apply them to a local network in a company, aiming to propose a local area network model with a security approach using best practices, thus guaranteeing the integrity and availability of the existing infrastructure in an organization, since it is essential for an adequate service of its different functions within it.

The results obtained as a result of the proposed work is the creation of a local area network model, which can be determined as satisfactory because said proposal was

reviewed and evaluated by different professionals in charge of the security of a LAN of the surveyed companies. , where it is highlighted that the model was focused on the correct areas that make up the local network as well as that the controls that are specified in it, if they meet the desired objectives since the best practices were applied, allowing to be a great contribution to companies that want to secure their local area network, since these controls provide security and operability of the organization.

Keywords:

Computer network, LAN, VLAN, WLAN, Security, Security policies.

CONTENIDO

TABLA DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

Una empresa que no envíe datos confidenciales a través de Internet e intranets (LAN) no es posible en la actualidad. Las medidas de seguridad incluyen soluciones de hardware y software para la seguridad de la información, medidas de seguridad necesarias para una correcta comunicación entre host, así como la multidifusión de IP que es un mecanismo útil para distribuir datos de gestión en una red de área local. [1]

Las redes LAN son bastante eficientes porque permiten la transferencia de archivos entre ordenadores y como estas están conectadas a internet, corren el riesgo de ser atacadas por ciberdelincuentes para robar datos o atacar con diferentes tipos de malware a nuestros equipos. Muchas de las veces al momento de contratar un servicio de internet no toman las debidas precauciones e investigan que seguridad brindan estas empresas de internet. [2]

La presente investigación se enmarca en el análisis de modelos de seguridad a redes LAN lo cual genera la oportunidad de crear un modelo óptimo en base a la recolección de información en fuentes científicas para posterior implementación de este servicio en una empresa, tomando en cuenta que cuando se monta un servidor en una red local, se debe garantizar la seguridad de la red, que la misma no va a sufrir algún tipo de ataque o amenaza que pueda comprometer la información o confidencialidad de la organización, ya que un servicio de red en una empresa, la información y datos transmitidos a través de una red local son primordiales para un adecuado servicio dentro del mismo.

Capítulo 1: mediante este capítulo se da a conocer la utilidad de la creación de un modelo de seguridad para una red, los ámbitos de aplicación, justificando el porqué es importante dar solución a la necesidad planteada.

Capítulo 2: se detallan la definición del modelo de seguridad para una red local y su fundamentación teórica, además de los objetivos y diseño del modelo.

Capítulo 3: se establece el plan para evaluar el modelo de seguridad, obteniendo así los resultados de dicha evaluación para posterior establecer las conclusiones y recomendaciones del modelo implementado.

1. CAPITULO I. DIAGNOSTICO DE NECESIDADES Y REQUERIMIENTOS

1.1. ÁMBITO DE APLICACIÓN: DESCRIPCIÓN DEL CONTEXTO Y HECHOS DE INTERÉS

En el mundo moderno el internet genera gran relevancia por lo que vivir sin dichos servicios es imposible, en la actualidad alrededor del 80% de las personas a nivel mundial usan el internet de alguna u otra forma aunque con una tendencia al aumento cada año. [3]

Debido a esto se evidencia la necesidad de comunicación, el intercambio de recursos, entre otras funcionalidades y para ello se requiere el establecimiento de una red de computadoras que pueda conectar dispositivos como computadoras, impresoras y distintos dispositivos más para comunicarse entre los usuarios de computadoras y los recursos compartidos, para ello se destaca un tipo de aplicación de las redes informáticas que es la red de área local. [4]

Con el rápido desarrollo de la escala de las redes, las aplicaciones y los servicios se han enriquecido. Para promover la arquitectura dinámica, la seguridad de alto nivel y la alta calidad de servicio de la red, la separación hacia adelante de la arquitectura de la red de control es una tendencia de desarrollo de la tecnología de redes, por lo tanto es ahí donde se debe tener un adecuado control y aseguramiento en cuanto a la seguridad de una red de área local evitando así ataques frecuentes a la red causando perdida de información, problemas a la integridad o disponibilidad de la misma, entre otras. [5]

Por tal motivo la presente investigación es el desarrollo de un modelo el cual brinde y garantice un mayor control en cuanto a la seguridad de la red local, donde se neutralice en mayor medida los ataques que se puedan dar a la red garantizando una mayor fluidez de la conexión y asegurando la integridad, disponibilidad y confidencialidad de la información.

1.2. ESTABLECIMIENTO DE REQUERIMIENTOS

Los últimos años han visto el desarrollo de tecnologías exitosas de Internet de las cosas (IoT), comunicación global, entre otras, basadas en redes de datos habilitadas para IP. A

pesar de la creciente demanda de seguridad de las redes de servicios de datos, en una red de área local aún se presenta diferentes tipos de vulnerabilidades lo cual provoca perjuicios a la red. [6]

Es así que se plantea indagar en varios puntos y aspectos relacionados a una red de área local, de esa forma se puede evidenciar los principales aspectos a tomar en cuenta para el aseguramiento de una conexión optima dentro de una red local en una empresa, ayudando de esta manera su eficiencia y eficacia al momento de prestar sus servicios dentro de la misma, además de tener un control sobre la información que se opera en dicha organización.

Dentro de una red de área local se encuentran diferentes tipos a tomar en cuenta para la propuesta de un modelo basado en seguridad, como es el espacio físico o la misma red cableada, otras de las medidas es la virtualización de redes la cual se ha vuelto cada vez más importante en los últimos años ya que permite la creación de infraestructuras de red que se adaptan específicamente a las necesidades de distintas aplicaciones de red. [7]

En la actualidad, el uso de la red informática permite una mayor velocidad en el desarrollo de la tecnología, esto se puede ver en el creciente número de organizaciones o empresas que utilizan la red informática para facilitar el flujo de información dentro de la organización o la empresa, debido a esta situación se debe enfocar medidas de seguridad a este tipo de conexión ya que forma parte dentro de una red local en una empresa. [8]

1.3. JUSTIFICACIÓN DEL REQUERIMIENTO A SATISFACER

Mediante la elaboración del presente trabajo se ejecuta varias fases importantes para cumplir con el propósito y objetivos del mismo, donde se asume un tema importante en el área de las redes locales las cuales son bastante importantes porque permiten la transferencia de archivos entre ordenadores y como las mismas están conectadas a internet, aunque corren el riesgo de ser atacadas por ciberdelincuentes para robar datos o atacar con diferentes tipos de malware a nuestros equipos, precisamente eso se pretende mitigar o bajar significativamente este tipo de riesgo y se lo evidencia a lo largo de la elaboración del proyecto.

El propósito de esta investigación se enmarca en el análisis de modelos de seguridad a redes LAN lo cual genera la oportunidad de crear un modelo óptimo en base a la recolección de información en fuentes científicas para implementación de este servicio en una organización, para lo cual se realiza una comparativa que ofrecen los diferentes modelos existentes en cuanto a redes de área local y así tener conectividad de forma más segura.

Cumpliendo con los objetivos propuestos y según el alcance del proyecto se espera obtener un modelo óptimo en cuanto a seguridad de redes LAN lo cual permitiría aplicar dicho modelo en una empresa u organización luego de su correspondiente evaluación, la misma tendría múltiples beneficios para cualquier organización, ya que esta podría tener un control efectivo del tráfico de red lo cual se reflejará en la conexión directa al internet y tráfico de los datos que por la misma se comunican, proporcionando así, confiabilidad, confidencialidad y un servicio de calidad a sus clientes.

2. CAPÍTULO II DESARROLLO DEL PROYECTO

2.1. DEFINICIÓN DE UN MODELO PARA REDES DE ÁREA LOCAL

Modelo

Un modelo como tal es un sistema formal que promueve mecanismos consistentes y efectivos para definir e implementar controles. Los componentes deben centrarse en identificar el nivel actual de riesgo y tomar medidas para mitigarlo, como por ejemplo tomar en cuenta un modelo de seguridad centrándose en un área de investigación como la seguridad de una red. [9]

Redes de área local

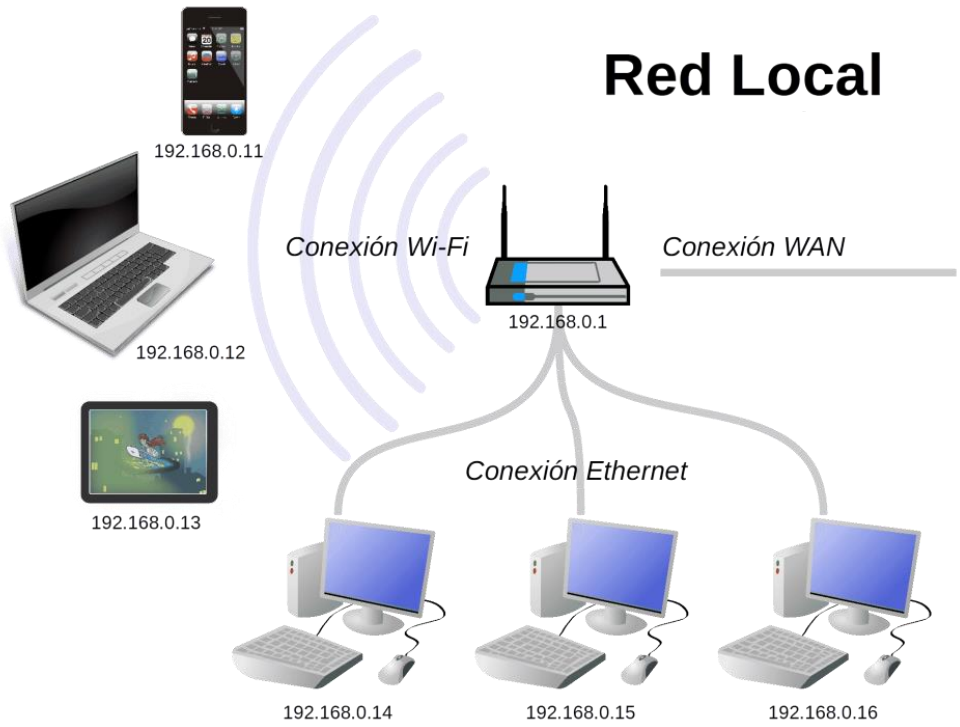
La necesidad de comunicación, el intercambio de recursos requiere el establecimiento de una red de computadoras que pueda conectar dispositivos como computadoras, impresoras y varios otros dispositivos para comunicarse entre los usuarios de computadoras y los recursos compartidos. Un tipo de aplicación de las redes informáticas es la red de área local.

Teniendo en cuenta una definición básica sobre una red local, se puede determinar como la interconexión entre varios ordenadores y periféricos, la misma indica que su extensión

está limitada físicamente a un entorno de unos pocos kilómetros, de tal manera que una red local se define a aquella que se expande en un área relativamente pequeña. Comúnmente se encuentra dentro de un edificio o un conjunto de edificios contiguos, de tal manera así sería adaptado a una pequeña o mediana empresa. [10]

Ahora bien, dentro de una LAN se debe aplicar cambios o configuraciones de ser necesario para armar un modelo óptimo que garantice la seguridad en dicha área local, para aquello se debe tomar en cuenta que existen diferentes tipos que conforma a una LAN, la cuales se mencionan a continuación para posteriormente usar ese conocimiento obtenido y así formar el modelo de seguridad antes mencionado para su posterior implementación en diferentes empresas que lo requieran.

Ilustración 1: *Red de área local*



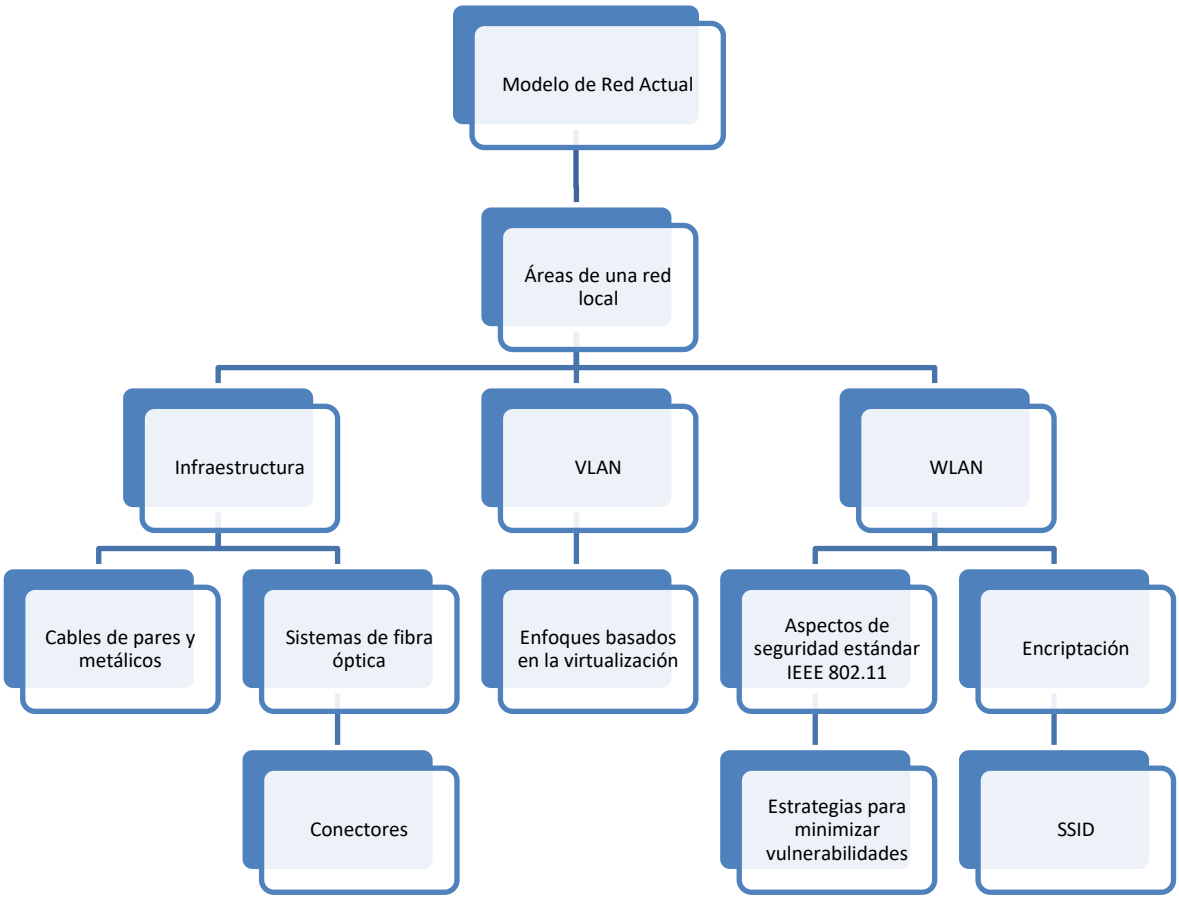
Fuente: [11]

Modelo para redes de área local

Si bien no existe un modelo como tal que permita asegurar una LAN tomando en cuenta todos los aspectos o áreas que la conforman, mediante el análisis de diferentes medidas de seguridad implementadas a redes locales y entrevistas con profesionales del área se pretende crear un modelo óptimo para la seguridad en la red local de una organización y/o empresa en base a la recolección de información en fuentes científicas para su posterior implementación, para ello se realiza una comparativa que ofrecen los diferentes modelos o medidas de seguridad que se aplican a una red local, así como tener en conocimiento las vulnerabilidades que existen y puedan afectar al correcto funcionamiento de la red y tráfico de la información, de esa forma se puede tomar los correctivos necesarios para la creación funcional del modelo.

2.2. FUNDAMENTACIÓN TEÓRICA DE UN MODELO PARA LAN

Ilustración 2: *Mapa conceptual de fundamentación teórica del modelo de red actual*



Fuente: *Elaboración propia*

Mediante el análisis de diferentes sistemas de seguridad a redes LAN se puede generar la oportunidad de crear un modelo óptimo para la seguridad en una red de área local para una organización y/o empresa en base a la recolección de información en fuentes bibliográficas así como experiencias compartidas por parte de gerentes o encargados en la parte del área de sistemas en diferentes empresas, para su posterior implementación, para ello se realiza una comparativa que ofrecen los diferentes tipos de seguridad a redes locales y así tener conectividad de forma más segura. [2]

Dentro de estas comparativas se obtienen varios aspectos a tomar en cuenta para la seguridad de las redes locales, donde destacan el espacio físico o infraestructura del área de sistemas, la red cableada en sí, entre otras.

2.2.1. Áreas de una red local

2.2.1.1. Infraestructura

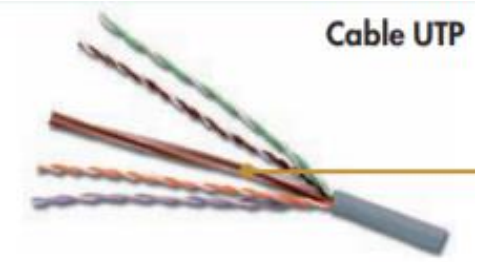
2.2.1.1.1. Cables de pares y metálicos

Los cables de pares están formados por pares de filamentos metálicos y constituyen el modo más simple y económico de todos los medios de transmisión, lógicamente estos presentan algunos inconvenientes principalmente al sobrepasar ciertas longitudes donde se debe restablecer el nivel eléctrico de la señal mediante el uso de repetidores. Además de la sensibilidad a interferencias y diafonías producidas por la inducción electromagnética. [12]

- **Cable UTP**

  UTP son las siglas de Unshielded Twisted Pair. Este es un cable de par trenzado sin cubierta metálica exterior, lo que lo hace susceptible a interferencias. Es importante mantener el número de pares. De lo contrario, el efecto trenzado se invalidará y la capacidad de transmisión se reducirá u obstaculizará significativamente. Este es uno de los tipos más utilizados de manera conveniente por su bajo costo y disponibilidad. Simplicidad de instalación. [12]

Ilustración 3: *Cable UTP*

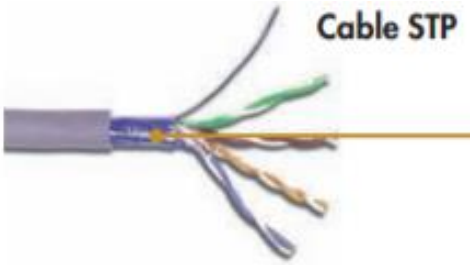


Fuente: [12]

- **Cable STP**

Similar al cable UTP, pero con un revestimiento metálico ligeramente mejorado para evitar interferencias externas. Esta chaqueta debe estar conectada a la tierra del equipo. [12]

Ilustración 4: *Cable STP*

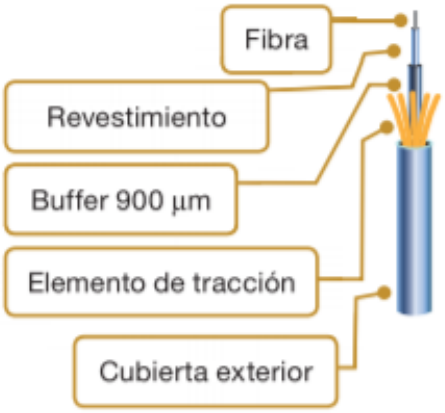


Fuente: [12]

2.2.1.1.2. Sistemas de fibra óptica

Según [12] la fibra óptica permite la transmisión de señales luminosas. La fibra, que suele ser de vidrio u otros materiales plásticos, es insensible a interferencias electromagnéticas externas, lo cual evidencia una mayor eficacia y eficiencia en comparación a los cables de pares trenzados. La luz ambiental es una mezcla de señales de muchas frecuencias diferentes y no es una fuente portadora óptica adecuada para la transmisión de datos.

Ilustración 5: *Propuesta de arquitectura*



Fuente: [12]

2.2.1.1.3. Conectores para fibra óptica

Los conectores más comunes utilizados en instalaciones de fibra óptica para redes de área local son los conectores ST y SC que se los presenta a continuación. [12]

- **Conector SC**

  Es un conector directo que expone las vulnerabilidades de seguridad de la red y se usa comúnmente en conmutadores Gigabit Ethernet. Para conectar la fibra al conector, es necesario pulir la fibra y alinear la fibra con el conector. [12]

- **Conector ST**

  Es un conector semejante al SC pero requiere un giro del conector para la inserción del mismo, dando así una mayor seguridad para la red debido a su dificultad para desmontarlo. Suele utilizarse en instalaciones Ethernet híbridas entre cables de pares y fibra óptica y al igual que el conector anterior se requiere un pulido y la alineación de la fibra. [12]

2.2.1.2. VLAN

La virtualización es un concepto bien establecido y las aplicaciones abarcan múltiples dominios de TI. Esta técnica permite crear múltiples plataformas virtuales en una única infraestructura física, lo que permite que arquitecturas heterogéneas se ejecuten en el mismo hardware. [7]

La necesidad de seguridad y conveniencia en la transmisión de datos requiere que todos los usuarios puedan crear redes más seguras tanto para la comunicación de datos como para compartir Internet. Siempre se requiere un desempeño laboral eficiente para poder trabajar rápidamente, a tiempo sin verse limitado por uno de los altos flujos de datos que están causando problemas a los dispositivos de red en el edificio. Al administrar las VLAN a través de una conexión LAN, puede analizar los problemas, especialmente desde el punto de vista de la comunicación de datos y la transmisión de datos lógicos. [4]

2.2.1.2.1. Enfoques basados en la virtualización

El enfoque de virtualización de máquinas implica la creación de una red virtual con un grupo de máquinas virtuales interconectadas. Los monitores de máquinas virtuales se

utilizan para crear instancias de enrutadores virtuales y establecer conexiones virtuales entre ellas, independientemente de su topología de red física. [7]

2.2.1.3. WLAN

Las redes inalámbricas son ampliamente reconocidas como una solución pública para el acceso rápido y fácil a la información a bajo costo. Wifi le permite acceder a información compartida sin conectarse a un punto de conexión fijo. Las WLAN combinan la comunicación de datos y el descubrimiento simple para enviar y recibir datos de forma inalámbrica. [13]

Por lo tanto se puede mencionar que la WLAN están diseñadas como una extensión de las Redes de Área Local (LAN) terrestres, para brindar conectividad de red con movilidad restringida que en muchos de los casos esta restricción puede ser evadida. [14]

2.2.1.3.1. Aspectos de seguridad del estándar IEEE 802.11

“IEEE 802.11 proporciona seguridad a través del cifrado y la autenticación. La autenticación se puede realizar a través de un sistema abierto. o clave compartida en modo ad hoc o en modo infraestructura.” [15]

2.2.1.3.2. Encriptación

En la actualidad el medio más eficiente de encriptación para redes inalámbricas es WPA2 aunque más adelante se menciona el tipo de encriptación WPA3 que brindará una mejor eficiencia a decir de los expertos en la materia, ambos reemplazando el WPA e introduce el CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), para reemplazar TKIP (el protocolo obligatorio en el WPA). CCMP proporciona una nueva forma de encriptación más segura basado en el cifrado por bloques AES. [16] Este es un cifrado de bloques diseñado por Joan Daemen y Vincent Rijmen. Tanto el bloque como la longitud de clave son extensibles a múltiplos de 32 bits. El cifrado AES es rápido, flexible y se puede aplicar a una variedad de sistemas operativos, particularmente dispositivos pequeños y tarjetas inteligentes, para mayor seguridad. [16]

2.2.1.3.3. Estrategia para minimizar vulnerabilidad en sistemas de información

"La seguridad en informática, considerada como el conjunto de técnicas aplicadas a los componentes de la red local, persigue el objetivo de minimizar
las vulnerabilidades presentes en los sistemas de información acordes a las políticas de la organización." [17]

La seguridad en informática es responsable de preservar los dispositivos conectados a la red, así como a la información administrada por esta. Los problemas de seguridad no deben perturbar la capacidad de una organización para realizar sus operaciones; este es el requisito básico de seguridad que deben tener las organizaciones.

2.2.1.3.4. SSID

El SSID como comúnmente se lo conoce al identificador de paquetes de servicio, se trata del nombre que identifica una red inalámbrica con respecto a otras. Por lo general, proporciona un único punto de acceso SSID para facilitar su uso por parte de los usuarios. Por lo tanto, los usuarios autenticados y autorizados tienen identidades diferentes y pueden conectarse a la red inalámbrica cuando y donde quieran y así obtener los mismos recursos de red accesibles, como ancho de banda y acceso. Control (LCA), entre otras, lo cual es una clara vulnerabilidad a la red. [9]

2.3. OBJETIVOS DEL MODELO

2.3.1. Objetivo General

- Proponer un modelo de red de área local con un enfoque de seguridad usando las mejores prácticas, garantizando así la integridad y disponibilidad de la infraestructura existente en una organización.

2.3.2. Objetivos Específicos

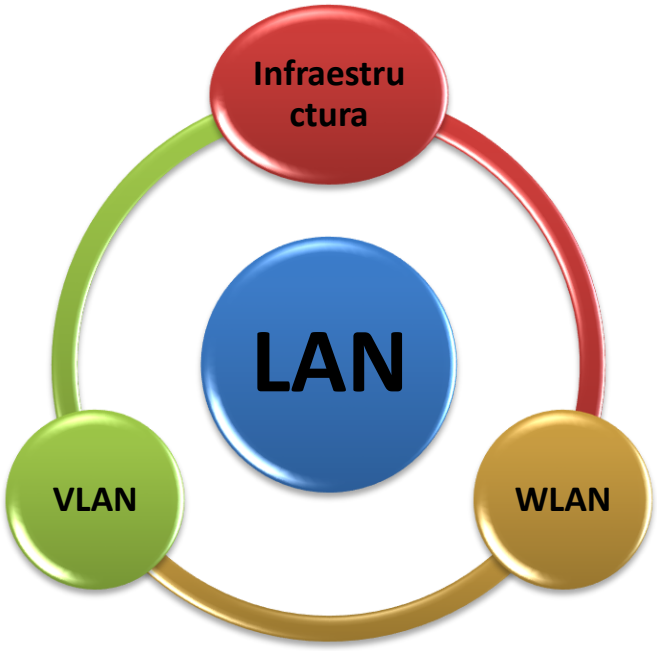
- Realizar un análisis sobre modelos de una red de área local mediante información bibliográfica y entrevistas con profesionales del medio.

- Identificar las vulnerabilidades existentes con respecto a seguridad en los modelos de una red de área local.
- Crear un modelo de red de área local que brinde seguridad a sus diferentes áreas que lo componen aplicando las mejores prácticas.

2.4. DISEÑO DEL MODELO

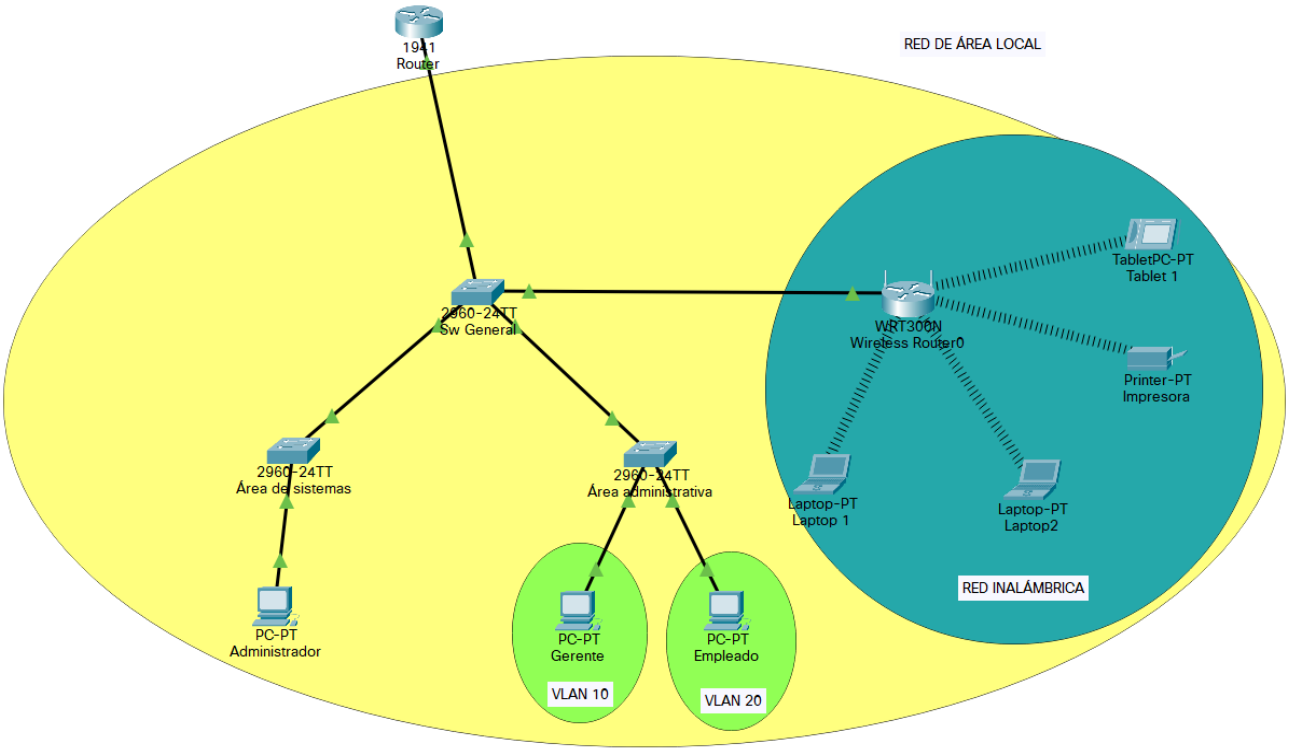
Como se indica en la documentación mostrada anteriormente mediante la información recopilada en fuente bibliográficas, estudios de seguridad para redes LAN en artículos científicos, datos obtenidos por entrevistas a diferentes empresas y departamentos de sistemas se muestra como tal, el modelo que usan diferentes empresas en una red local destacando las áreas que se abarca dentro de la misma.

Ilustración 6: *Modelo de Red de área local*



Fuente: *Elaboración propia*

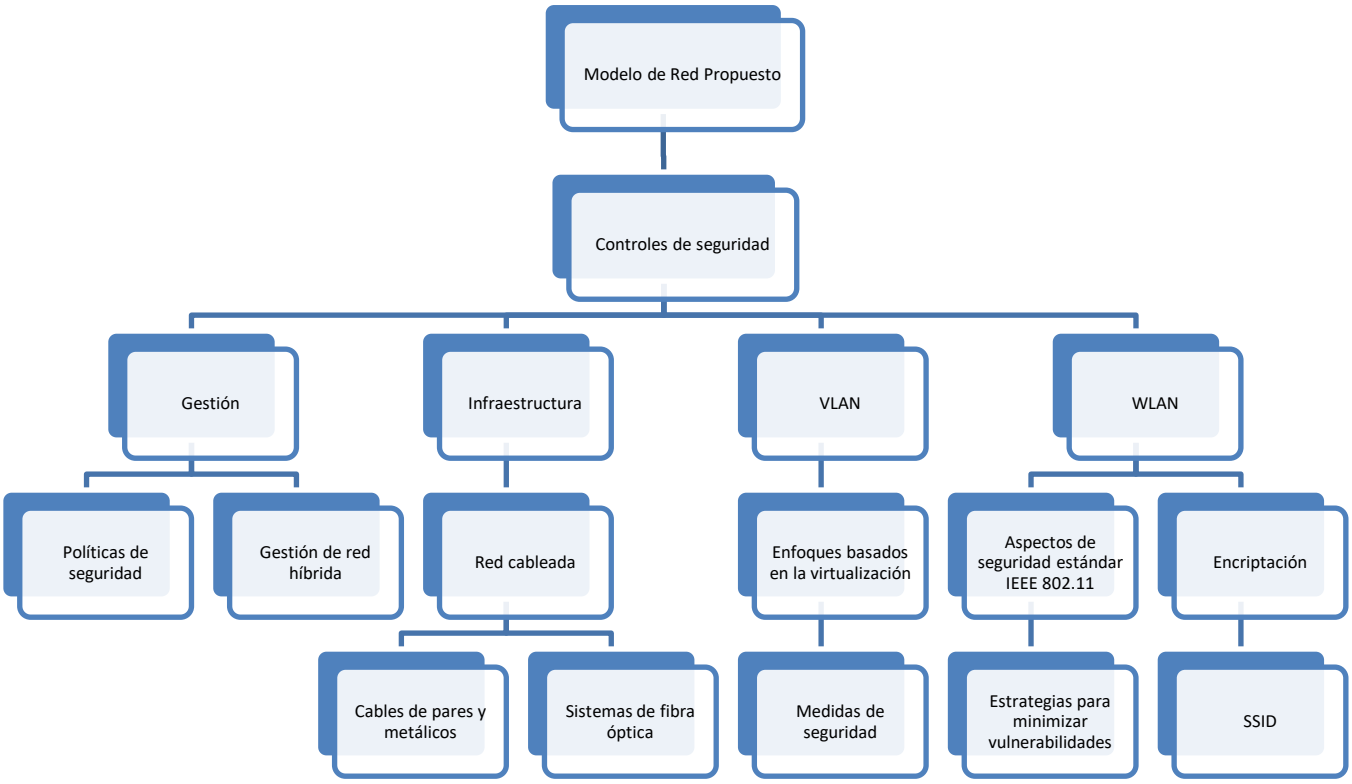
Ilustración 7: *Modelo lógico de una LAN*



Fuente: *Elaboración propia*

2.5. FUNDAMENTACIÓN TEÓRICA DEL MODELO DE SEGURIDAD PARA LAN

Ilustración 8: *Mapa conceptual de fundamentación teórica del modelo de red propuesto*



Fuente: *Elaboración propia*

2.5.1. Controles de seguridad

En la actualidad por el auge de la conexión y comunicación mediante redes, la propagación del malware de red en Internet es un desafío de red complejo y dinámico. Esta suposición se establece en muchos casos, como el malware informático que se propaga por Internet. Por lo tanto, se debe considerar tomar en cuenta este tipo de vulnerabilidades y contrarrestarlas mediante los debidos controles. [9]

2.5.1.1. Gestión

2.5.1.1.1. Políticas de seguridad

Mediante las políticas de seguridad se puede asegurar los sistemas de gestión de la información de amenazas internas o externas, ya sean intencionales o no, para garantizar la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

Muchos profesionales del medio mencionan políticas propias de la empresa donde destacan medidas como la de controles rutinarios del área de sistemas así como el de tener un control para el ingreso al mismo y manipulación del sistema de la organización, esto no es suficiente y por tal razón se debe considerar otras estrategias de control.

Para dicho propósito se establecen medidas sugeridas en la ISO 27001, la cual es un estándar desarrollado por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información en una empresa u organización. [18]

Políticas de seguridad de la información

Políticas para la seguridad de la información: El conjunto de pautas de seguridad de la información debe ser definido, aprobado, publicado por la gerencia y comunicado a los empleados responsables y a terceros. [18]

Control de Acceso

Política de control de acceso: en cuanto respecta al control de acceso se debería establecer, documentar y revisar una política de control con base en los requisitos del negocio y de seguridad de la información. [18]

Política sobre el uso de los servicios de red: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados anteriormente en un área en específico. [18]

Gestión de acceso de usuarios: Mediante este punto se pretende asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a los servicios de la organización, se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. [18]

Así como nos indica la norma en la gestión de derechos de acceso privilegiado, donde se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado. [18]

Seguridad física y del entorno

Áreas seguras: Se debe evitar el acceso físico no autorizado, el daño y la interferencia con la información y las instalaciones de procesamiento de información de una organización. [18]

Seguridad de las comunicaciones

Gestión de la seguridad de las redes: en este punto se debe asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información. Así mismo las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones. [18]

2.5.1.1.2. Gestión de red Híbrida

Mediante este tipo de gestión se pretende una combinación entre una red alámbrica y una red inalámbrica, se implementa para facilitar, tanto la estabilidad como la versatilidad de la red. [10]

De esta forma se elimina todas las deficiencias de las redes cableadas e inalámbricas optimizándola de mejor forma, ya que debido a la transmisión inalámbrica de datos entre cada dispositivo y los hosts de servicios remotos, se necesita la transmisión de datos con seguridad y que mejor forma que combinando estos dos tipos de redes. [19]

Establecer medidas de seguridad dentro de una red de área local tomando en cuenta el concepto de una gestión de red híbrida, es considerar no solo la conexión inalámbrica sino la conexión y el espacio físico, es decir la infraestructura de la red en sí.

Según [20] la mitigación de riesgos debe ser considerada por todos los que desempeñan un papel en el mercado. La mitigación del riesgo comienza con la prevención de la amenaza, por lo tanto se pueden tomar algunas medidas preventivas.

Mediante conversatorios formales e informales con encargados y administradores en departamentos de sistemas en diferentes empresas se pudo evidenciar que estos profesionales de la seguridad informática y redes no toman los controles necesarios pero que una de las opciones que se maneja en la mayoría de empresas es que cuentan con un área específica para el control de sistemas dentro de la misma logrando una mayor facilidad de vigilancia en dicha área.

Considerando los aspectos antes mencionados, se puede determinar que la confidencialidad, integridad, disponibilidad, identificación, autenticación, privacidad y

confianza se analizan como características de seguridad por lo que debe dársele la importancia necesaria. [20]

A medida que aumenta el acceso a Internet, aumenta la demanda de diferentes niveles de ataque y protección en entornos cableados e inalámbricos, por ello el uso de redes híbridas para una mayor seguridad de una red local. [21]

2.5.1.2. Infraestructura

2.5.1.2.1. Red cableada

Según [22] la comunicación inalámbrica es más propensa a pérdidas aleatorias que la comunicación por cable debido al ruido y la movilidad, lo cual conlleva a que una red cableada genera una mayor seguridad en cuanto al aseguramiento de la información, para ello a continuación se describe los principales medios de transmisión y las acciones para mejorar su seguridad.

2.5.1.2.1.1. Cables de pares y metálicos

Considerando el uso de este tipo de cables lo más recomendable sería la implementación del cable STP ya que como se mencionó anteriormente tiene una mejora con respecto al cable UTP por su revestimiento lo cual da como resultado, un cable mejor blindado, aunque menos flexible que los cables anteriores. [12]

2.5.1.2.1.2. Sistemas de fibra óptica

Si bien la fibra óptica es un método mejorado en cuanto a rendimiento y velocidad, la misma cuenta con diferentes tipos de conectores, según el estudio realizado, el conector ST es el conector más adecuado si de seguridad se trata, ya que necesita un giro del conector para su inserción presentando así una mayor dificultad para desmontarlo. [22]

2.5.1.3. VLAN

Mediante la aplicación de una VLAN se genera una medida de seguridad para la red local ya que analiza los diferentes problemas que se pueden dar en la transmisión y comunicación de los datos.

La VLAN se debe a las limitaciones de la red local. (VLAN) Al utilizar la tecnología VLAN para administrar la distribución y regulación del tráfico de datos, el conmutador de administración puede agrupar interfaces (puertos) en todos los grupos requeridos por la red. [4]

2.5.1.3.1. Enfoques basados en la virtualización

Teniendo en cuenta que en un entorno virtualizado, diferentes redes virtuales pueden operar sobre la misma infraestructura física, se deben tomar algunas medidas de seguridad para asegurar una VLAN. [23]

Dichas medidas a tomar en cuenta se detallan en los siguientes apartados:

2.5.1.3.2. Medidas de seguridad

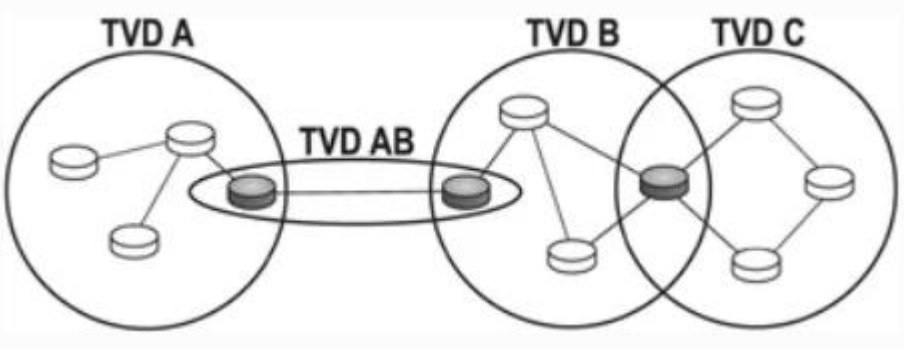
- **Dominios virtuales de confianza**

  El control de acceso utiliza mecanismos de autenticación y autorización para autenticar las identidades de las entidades en la red e imponer diferentes niveles de privilegio a cada entidad, de esta forma se aborda esta medida mediante dominios virtuales de confianza. [7]

  El marco utiliza un dominio virtual de confianza (TVD) para proporcionar las medidas de seguridad anteriores. Cada TVD representa un dominio distinto que consta de "elementos de virtualización" y los canales de comunicación entre estos elementos. Como sugirió Cabuk, los elementos de virtualización son estaciones de trabajo virtuales. [7]

  A continuación, en la siguiente ilustración se muestra los TVD en una infraestructura de red virtual:

Ilustración 9: *Cable STP*



Fuente: [7]

El marco utiliza un dominio virtual de confianza (TVD) para proporcionar las medidas de seguridad anteriores. Cada TVDgh

- **Autenticación**

  El propósito de la autenticación es verificar que las entidades alrededor de la red sean las solicitadas. En un entorno de red virtual, la autenticación exitosa es difícil debido a factores como la federación de redes virtuales, la movilidad de enrutadores y los enlaces virtuales, por tal razón se debe hacer frente a estas dificultades mediante los siguientes enfoques. [7]

  Basado en certificado: Como se mencionaba anteriormente acerca de los TVD, la autenticación necesaria para soportar el control de acceso se proporciona mediante certificados digitales. Estos certificados garantizan la identidad de las entidades conectadas a la red. El sistema también utiliza una red privada virtual (VPN) para autenticar entidades a través de una conexión de red. [7]

  Basado en clave: El sistema tiene una arquitectura que proporciona enrutamiento eficiente, aislamiento de recursos adecuado y canales de comunicación seguros entre enrutadores y monitores de máquinas virtuales (VMM). [7]

  Por razones de rendimiento, el enrutador virtual copia la información de enrutamiento al VMM (en este caso, el hipervisor). Este proceso lo realiza un módulo de separación de planos, que separa el plano de datos (que contiene reglas de enrutamiento) y el plano de control (responsable de crear reglas de enrutamiento). Esto mejora enormemente el rendimiento, ya que no es necesario enviar paquetes al enrutador virtual de acuerdo con las reglas de la tabla de enrutamiento del hipervisor. [7]

  Sin embargo, el proceso de copia de la información de enrutamiento debe autenticarse de manera que un enrutador malintencionado no pueda comprometer el plano de datos de otro enrutador.

Claro está que para evitar que los enrutadores malintencionados entren en los enrutadores pudiendo afectar el plano de datos de otros enrutadores, es necesario autenticarse el proceso de copia de la información de enrutamiento.

Como se logra evidenciar, la seguridad de una red no significa necesariamente un mayor costo, control o riesgo para los usuarios, sino más bien un equilibrio entre el rendimiento, el control y la respuesta a incidentes como se lo demuestra en los enfoques antes mencionados.

- **VLAN y VPN**

  Debido a que las máquinas virtuales que pertenecen a diferentes TVD se pueden alojar en la misma máquina física, sería necesario asegurar un aislamiento adecuado, evitando que un TVD acceda a datos que pertenecen a otro TVD, he ahí la propuesta de implementar una combinación de VLAN y VPN. [7]

  Las VLAN se utilizan para identificar paquetes que pertenecen a diferentes redes y para garantizar que los dispositivos habilitados para VLAN enruten los paquetes a la interfaz de red correcta para proporcionar un aislamiento adecuado. Sin embargo, el canal físico incorrecto puede requerir un mayor nivel de seguridad. Por eso la utilización de una VPN para proteger los datos con criptografía de extremo a extremo. [7]

- **Cortafuegos y subredes**

  Otra medida es restringir el tráfico haciendo uso de reglas de firewall para evitar comunicaciones entre diferentes redes virtuales. Además de utilizar firewalls para este propósito, también se emplean la división en subredes (es decir, cada red virtual está vinculada a una subred única) proporcionando así una capa adicional de seguridad contra la divulgación de información no autorizada. [7]

  Como se logra evidenciar, la seguridad de una red no significa necesariamente un mayor costo, control o riesgo para los usuarios, sino más bien un equilibrio entre el rendimiento, el control y la respuesta a incidentes como se lo demuestra en los enfoques antes mencionados. [24]

La capacidad de crear VLAN se considera una característica importante de la conmutación Ethernet. Una VLAN es un clúster virtual de nodos y dispositivos de red que se conectan a la conmutación Ethernet

La capacidad de crear VLAN es una característica importante de los conmutadores Ethernet. Una VLAN es una colección virtual de nodos y dispositivos de red para lo cual era necesario implementar las medidas de seguridad antes mencionadas. [25]

2.5.1.4. WLAN

2.5.1.4.1. Aspectos de seguridad del estándar IEEE 802.11

Una estación de red o un punto de acceso (AP) puede otorgar permiso a cualquier estación que solicite conexión en el sistema de autenticación abierto, o solo a aquellas incluidas en una lista predefinida. Sólo aquellas estaciones que tengan una clave de encriptación apropiada serán autenticadas en un sistema de clave compartida.

El cifrado representa un medio eficaz para evitar poner en peligro los datos transmitidos en las transmisiones inalámbricas. 802.11 especifica una capacidad de cifrado opcional denominada WEP; esto establece un nivel de seguridad similar al de las redes cableadas que utilizan el cifrado de los datos transportados por las señales de radio. WEP utiliza el algoritmo RC4 desarrollado por RSA Data Security. WEP también se utiliza para evitar que usuarios no autorizados obtengan acceso a WLAN (es decir, proporciona autenticación); tal propósito no se establece explícitamente en 802.11 pero se considera una característica importante de WEP. [15]

2.5.1.4.2. Encriptación

Recientemente se da a conocer Wi-Fi Protected Access en su tercera versión mejor conocido como WPA3 como nuevo estándar para el mismo protocolo, mucho más seguro y avanzado. Sin embargo, pueden surgir problemas de compatibilidad durante la migración que pueden durar años. [26] [27]

Una mejora significativa entre WPA2 y WPA3 es la reacción ante los ataques de fuerza bruta es decir, un tipo de vulnerabilidad que comprueba continuamente si hay ataques aleatorios hasta que se ejecuta el ataque apropiado, haciendo este tipo de aleatoriedad

más complicado en WPA3, además de que el proceso de autenticación presenta una mejora significativa, ya que es más complicado y requiere de mucho más tiempo de intentos, puesto que cada clave requiere de interacción con la red Wifi. [28]

2.5.1.4.3. Estrategia para minimizar vulnerabilidad en sistemas de información

Para tomar en cuenta que tipo de medidas tomar en una red se debe antes que nada identificar y analizar las vulnerabilidades comunes de seguridad cibernética.

Como por ejemplo existe denegación de servicio (DoS) la cual es un tipo de ataque que se enmarca en hacer que una máquina o un recurso de red sean inaccesibles para los usuarios previstos. Esto se debe a eventos que debilitan o inhabilitan la capacidad de la red para funcionar como se esperaba. [29]

Otro tipo de ataque es el software malicioso En este ataque, el atacante despliega programas de software maliciosos para conseguir acceso no autorizado a los sistemas informáticos aprovechando sus vulnerabilidades de seguridad que existieran pero que se puede contrarrestar. [29]

2.5.1.4.4. SSID

En cuanto al SSID, se debe tener un control adecuado de este identificador, como mencionaban algunos profesionales del área consultados de diferentes empresas, muchos coinciden en medidas como el de ocultar el SSID o múltiples SSID que podrían resolver el problema, aunque este último podría confundir a los usuarios que no saben qué SSID se pueden conectar.

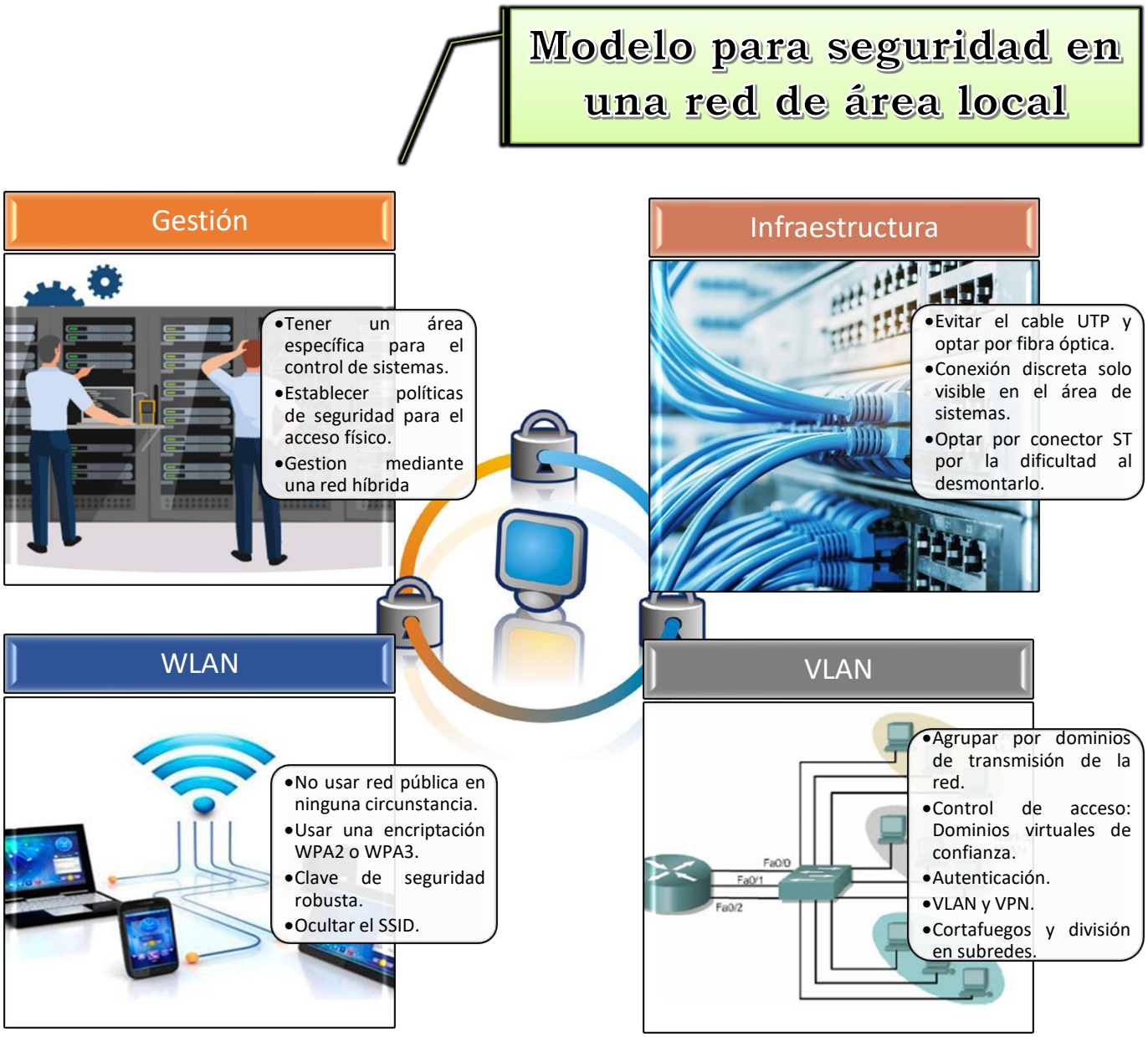
Mediante el análisis del tráfico de red se pueden detectar posibles ataques, en especial que buscan atacar la disponibilidad de la información lo cual generaría una pérdida para la empresa, en base a esta situación se debe tomar las medidas correspondientes. [30]

Una contramedida de seguridad según la información abordada previamente, es ocultar el SSID ya sea usando el tipo de encriptación WPA2 o WPA3 según la configuración de los equipos lo permita, además de contar con una clave robusta (combinación entre letras, números y caracteres especiales).

2.6. DISEÑO DE MODELO DE SEGURIDAD PARA LAN

Como se lo detalla en el documento tomando en cuenta la información recopilada en fuente bibliográficas, estudios de seguridad para redes LAN en artículos científicos, datos obtenidos por entrevistas a diferentes empresas y departamentos de sistemas se toma en cuenta varios aspectos y áreas para crear el modelo de seguridad obteniendo como resultado el siguiente modelo.

Ilustración 10: *Propuesta de modelo de seguridad en una red local*



Fuente: *Elaboración propia*

3. CAPÍTULO III EVALUACIÓN DEL MODELO

3.1. PLAN DE EVALUACIÓN

Entrevista para evaluación del modelo de seguridad para una red local

El modelo de análisis y evaluación que se empleará en el proceso de la investigación es una encuesta con preguntas objetivas usando escala de Likert con 5 niveles de satisfacción detallando las áreas del modelo propuesto, para su posterior análisis estadístico.

Pregunta 1: ¿Existe alguna norma de seguridad para redes de área local impuesta por el estado que se utiliza en su empresa?

Tabla 1: Resultados de pregunta 1

SI	
NO	

Fuente: *Elaboración propia*

Pregunta 2: ¿En su empresa aplican alguna norma o medida de seguridad para redes de área local?

Tabla 2: Resultados de pregunta 2

SI	
NO	

Fuente: *Elaboración propia*

Si la respuesta es “Si”, menciónelas: ……

Pregunta 3: Según el modelo propuesto ¿Consideraría que los controles de seguridad en cuanto a la gestión de una LAN garantizan la operatividad de la misma?

Tabla 3: Resultados de pregunta 3

Nivel Eficiencia	
Totalmente de acuerdo	0
De acuerdo	0

Ni acuerdo, ni desacuerdo	0
En Desacuerdo	0
Totalmente en desacuerdo	0

Fuente: *Elaboración propia*

Pregunta 4: ¿Consideraría que los controles de seguridad en cuanto a la infraestructura de una LAN aseguran la operatividad de la misma?

Tabla 4: Resultados de pregunta 4

Nivel Eficiencia	
Totalmente de acuerdo	0
De acuerdo	0
Ni acuerdo, ni desacuerdo	0
En Desacuerdo	0
Totalmente en desacuerdo	0

Fuente: *Elaboración propia*

Pregunta 5: ¿Consideraría que los controles de seguridad enfocados a la VLAN de una LAN garantizan la operatividad de la misma?

Tabla 5: Resultados de pregunta 5

Nivel Eficiencia	
Totalmente de acuerdo	0
De acuerdo	0
Ni acuerdo, ni desacuerdo	0
En Desacuerdo	0
Totalmente en desacuerdo	0

Fuente: *Elaboración propia*

Pregunta 6: ¿Consideraría que los controles de seguridad en cuanto a la WLAN de una red de área local aseguran la operatividad de la misma?

Tabla 6: Resultados de pregunta 6

Nivel Eficiencia	
Totalmente de acuerdo	0
De acuerdo	0
Ni acuerdo, ni desacuerdo	0
En Desacuerdo	0
Totalmente en desacuerdo	0

Fuente: *Elaboración propia*

Pregunta 7: En líneas generales ¿Usted considera que los puntos antes descritos ayudarían con la seguridad en una LAN mitigando así en gran parte las vulnerabilidades que pueda tener la misma?

Tabla 7: Resultados de pregunta 7

Nivel Eficiencia	
Totalmente de acuerdo	0
De acuerdo	0
Ni acuerdo, ni desacuerdo	0
En Desacuerdo	0
Totalmente en desacuerdo	0

Fuente: *Elaboración propia*

Pregunta 8: ¿Considera que el modelo propuesto abarca todas las áreas que conforman una LAN?

Tabla 8: Resultados de pregunta 8

SI	

NO	

Fuente: *Elaboración propia*

En caso de que su respuesta es “NO”, menciónelas: ……

3.2. RESULTADOS DE LA EVALUACIÓN

A continuación se presenta la tabulación de los resultados como evaluación del modelo de seguridad de una red de área local propuesto.

Pregunta 1: ¿Existe alguna norma de seguridad para redes de área local impuesta por el estado que se utiliza en su empresa?

Resultados:

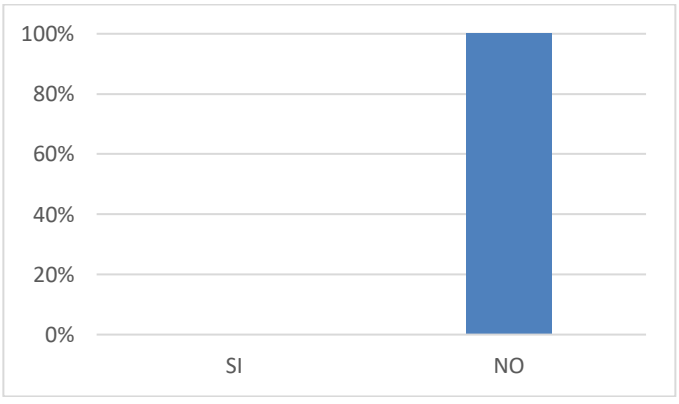
Tabla 9: Resultados de pregunta 1

SI	0%
NO	100%
TOTAL	100%

Fuente: *Elaboración propia*

Gráfico:

Ilustración 11: *gráfico de representación de la pregunta 1*



Fuente: *Elaboración propia*

Según la representación gráfica, se puede evidenciar que el 100% de las empresas encuestadas mencionan que no existe ninguna norma impuesta por el estado específicamente para una LAN.

Pregunta 2: ¿En su empresa aplican alguna norma o medida de seguridad para redes de área local?

Resultados:

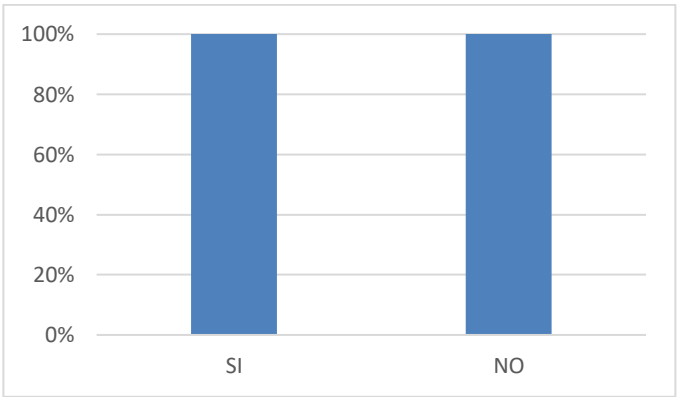
Tabla 10: Resultados de pregunta 2

SI	50%
NO	50%
TOTAL	100%

Fuente: *Elaboración propia*

Gráfico:

Ilustración 12: *gráfico de representación de la pregunta 2*



Fuente: *Elaboración propia*

Si la respuesta es "Si", menciónelas: Claves, Firewall, Roles de usuario, Estructuración de red cableada, Seccionado de red.

Según nos presenta la gráfica, la opinión está dividida en un 50 y 50 puesto que una parte de las empresas si cuentan con medidas de seguridad para su red local y otras no, destacando algunas medidas tomadas como es las claves de acceso, firewall, roles de usuario, entre otras.

Pregunta 3: Según el modelo propuesto ¿Consideraría que los controles de seguridad en cuanto a la gestión de una LAN garantizan la operatividad de la misma?

Resultados:

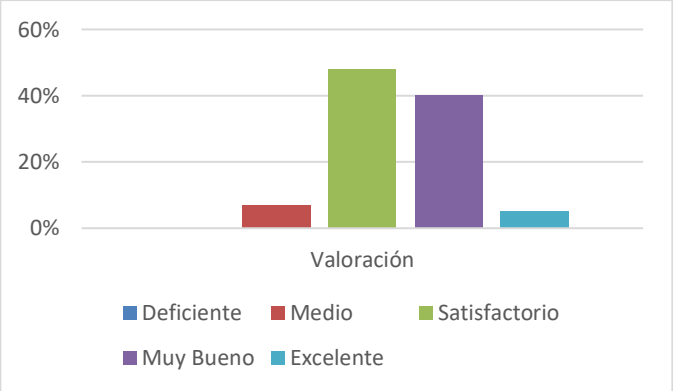
Tabla 11: Resultados de pregunta 3

Nivel Eficiencia	
Totalmente de acuerdo	25%
De acuerdo	75%
Ni acuerdo, ni desacuerdo	0
En Desacuerdo	0
Totalmente en desacuerdo	0
Total	100%

Fuente: *Elaboración propia*

Gráfico:

Ilustración 13: *gráfico de representación de la pregunta 3*



Fuente: *Elaboración propia*

Según la representación gráfica donde consta cinco niveles de satisfacción, nos indica que en esta área los controles son muy satisfactorios ya que el 25% de los encuestados dan como totalmente de acuerdo dichos controles y otro 75% respondieron que están de acuerdo.

Pregunta 4: ¿Consideraría que los controles de seguridad en cuanto a la infraestructura de una LAN aseguran la operatividad de la misma?

Resultados:

Tabla 12: Resultados de pregunta 4

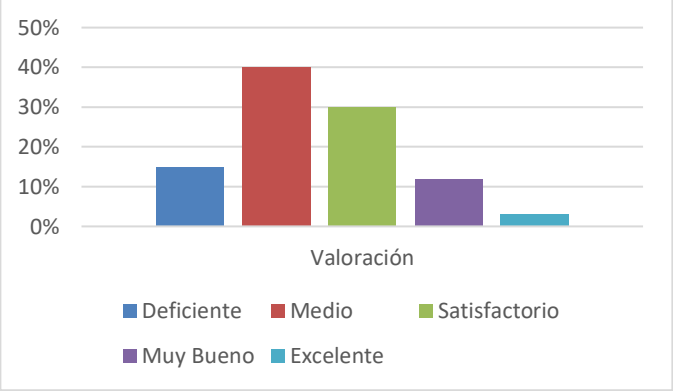
Nivel Eficiencia	
Totalmente de acuerdo	25%
De acuerdo	25%
Ni acuerdo, ni desacuerdo	50%

En Desacuerdo	0
Totalmente en desacuerdo	0
Total	100%

Fuente: *Elaboración propia*

Gráfico:

Ilustración 14: *gráfico de representación de la pregunta 4*



Fuente: *Elaboración propia*

Según nos presenta la gráfica igualmente con sus niveles de satisfacción, se puede detectar que en esta área los controles son adecuados aunque según las empresas encuestadas hay un ligero cambio a comparación de la anterior pregunta, ya que el 25% de los encuestados dan como totalmente de acuerdo, otro 25% dan como de cuerdo y el 50% restante no están ni de acuerdo ni en desacuerdo.

Pregunta 5: ¿Consideraría que los controles de seguridad enfocados a la VLAN de una LAN garantizan la operatividad de la misma?

Resultados:

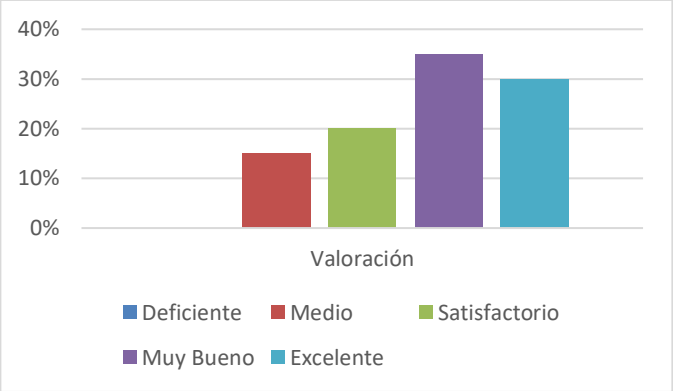
Tabla 13: Resultados de pregunta 5

Nivel Eficiencia	
Totalmente de acuerdo	25%
De acuerdo	50%
Ni acuerdo, ni desacuerdo	25%
En Desacuerdo	0
Totalmente en desacuerdo	0
Total	100%

Fuente: *Elaboración propia*

Gráfico:

Ilustración 15: *gráfico de representación de la pregunta 5*



Fuente: *Elaboración propia*

Según la información representada se visualiza que en cuanto a controles de la VLAN las empresas dan como correcto dichas medidas, donde el 25% de los encuestados dan como totalmente de acuerdo, otro 50% dan como de acuerdo y el 25% restante expresan que no están ni de acuerdo ni en desacuerdo.

Pregunta 6: ¿Consideraría que los controles de seguridad en cuanto a la WLAN de una red de área local aseguran la operatividad de la misma?

Resultados:

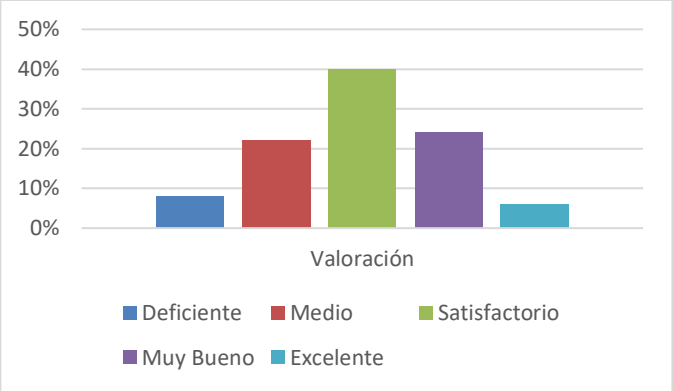
Tabla 14: Resultados de pregunta 6

Nivel Eficiencia	
Totalmente de acuerdo	50%
De acuerdo	50%
Ni acuerdo, ni desacuerdo	0
En Desacuerdo	0
Totalmente en desacuerdo	0
Total	100%

Fuente: *Elaboración propia*

Gráfico:

Ilustración 16: *gráfico de representación de la pregunta 6*



Fuente: *Elaboración propia*

Según la información representada gráficamente se evidencia que en cuanto a controles de una WLAN las empresas expresan un nivel de satisfacción alto en cuanto a dichas medidas, ya que el 50% de los encuestados dan como totalmente de acuerdo mientras el otro 50% dan como de acuerdo a dicha gestión.

Pregunta 7: En líneas generales ¿Usted considera que los puntos antes descritos ayudarían con la seguridad en una LAN mitigando así en gran parte las vulnerabilidades que pueda tener la misma?

Resultados:

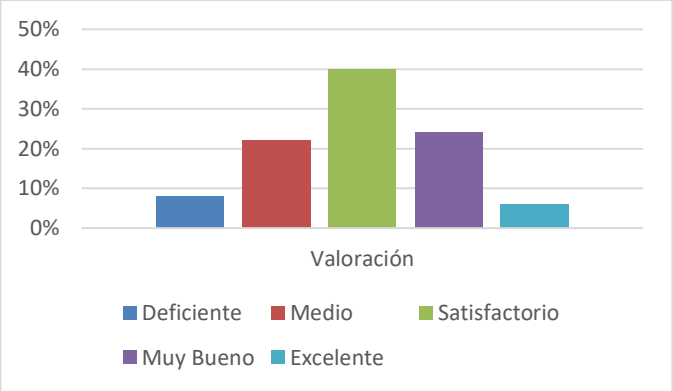
Tabla 15: Resultados de pregunta 7

Nivel Eficiencia	
Totalmente de acuerdo	0
De acuerdo	50%
Ni acuerdo, ni desacuerdo	50%
En Desacuerdo	0
Totalmente en desacuerdo	0
Total	100%

Fuente: *Elaboración propia*

Gráfico:

Ilustración 17: *gráfico de representación de la pregunta 7*



Fuente: *Elaboración propia*

Según la información representada se logra evidenciar que en líneas generales acerca del modelo propuesto los profesionales encuestados dictaminan un agrado sobre los controles mencionados mostrando así que un 50% responden que están de acuerdo con dichas medidas mientras el otro 50% no están ni de acuerdo ni en desacuerdo.

Pregunta 8: ¿Considera que el modelo propuesto abarca todas las áreas que conforman una LAN?

Resultados:

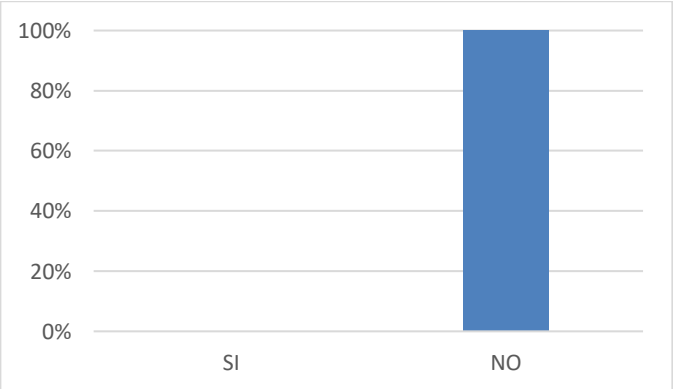
Tabla 16: Resultados de pregunta 8

SI	100%
NO	0
TOTAL	100%

Fuente: *Elaboración propia*

Gráfico:

Ilustración 18: *gráfico de representación de la pregunta 8*



Fuente: *Elaboración propia*

Según la representación gráfica, se logra evidenciar que el 100% de las empresas encuestadas mencionan que el modelo propuesto abarca todas las áreas que conforma una red de área local.

3.3. CONCLUSIONES

- Como resultado del presente trabajo se crea una propuesta de un modelo de red de área local con un enfoque a la seguridad para lo cual se usa las mejores prácticas que incluye información de revistas científicas así como consultas a expertos del área en sistemas, para garantizar la integridad y disponibilidad de la infraestructura existente en una empresa.
- Se realiza un análisis sobre temas relacionados a modelos de una red de área local, para lo cual se interpreta información relevante de fuentes bibliográficas y entrevistas con profesionales capacitados del tema.
- Se pudo conocer algunas medidas que se toman en cuenta en diferentes empresas o sitios sobre la seguridad de su red local, lo cual permitió identificar las vulnerabilidades que existen en modelos actuales de una red de área local.
- Se ha logrado crear un modelo de red de área local, dicha propuesta planteada pudo ser revisado y evaluado por diferentes profesionales encargados en la seguridad de una LAN en una organización, la cual evidencia que dichos controles brindan seguridad en las diferentes áreas que a la red antes mencionada la componen aplicando las mejores prácticas.

3.4. RECOMENDACIONES

- Es necesario familiarizarse con los diferentes controles que se aplican por cada área de la red local del modelo propuesto para futuras actualizaciones del mismo, ya que se pueden agregar o quitar diferentes controles o incluso puede variar las partes que conforman la red de área local según sea el caso.

- Se debe tomar en cuenta implementar el modelo propuesto luego de la evaluación correspondiente para así tener una mayor certeza de la funcionalidad que ejerce dicha propuesta en una red de área local de una empresa.
- Enfocar el modelo propuesto en otros tipos de infraestructura de red, como por ejemplo en las redes de área metropolitana o redes de área extensa.
- Presentar el modelo a diferentes profesionales en seguridad de redes mediante grupos o conferencias lo cual puede generar una evaluación más acertada de dicha propuesta.

BIBLIOGRAFÍA

[1] P. Veeraraghavan, D. Hanna y E. Pardede, «Building Scalable and Secure Multicast Delivery Infrastructure in a Local Area Network,» vol. 8, nº 10, p. 1162, 2019.

[2] C. Robledo Sosa, Redes de Computadoras, ESIME-Zacatenco, 2016.

[3] K. G. Pincay Romero, «Características de la conectividad a internet en el cantón Pasaje,» *Revista Universidad y Sociedad,* vol. 13, nº 3, pp. 150-160, 2021.

[4] R. Gatra, R. Akbar, B. Sugiantoro y N. Asyhab, «VLAN-based LAN Network Management Comparison using Cisco and Brocade,» *IJID REVISTA INTERNACIONAL DE INFORMÁTICA PARA EL DESARROLLO,* vol. 7, nº 2, pp. 45-49, 2019.

[5] S. Wang, J. Wu, W. Yang y L.-h. Guo , «Novel architectures and security solutions of programmable software-defined networking: a comprehensive survey,» *Frontiers of Information Technology & Electronic Engineering,* vol. 19, nº 12, p. 1500–1521, 2018.

[6] J. Han y D. Kim , «Security offloading network system for expanded security coverage in IPv6-based resource constrained data service networks,» *Wireless Networks,* vol. 26, p. 4615–4635, 2020.

[7] L. R. Bays, R. R. Oliveira, M. P. Barcellos y L. P. Gaspary, «Virtual network security: threats, countermeasures, and challenges,» *Journal of Internet Services and Applications,* vol. 6, nº 1, 2015.

[8] M. S. Bahry y B. Sugiantoro, «Analysys and Implementation IEEE 802.1Q to Improve Network Security,» *IJID (INTERNATIONAL JOURNAL ON INFORMATICS FOR DEVELOPMENT),* vol. 6, nº 2, pp. 7-11, 2018.

[9] L. Lan, K. L. K. Ryan, R. Guangming y X. Xiaoping, «Malware Propagation and Prevention Model for Time-Varying Community Networks within Software Defined Networks,» *SECURITY AND COMMUNICATION NETWORKS,* vol. 2017, p. 8, 2017.

[10] C. Caztro, «SlideShare,» 28 Octubre 2017. [En línea]. Available: https://es.slideshare.net/kaztro93/tipos-de-redes-locales. [Último acceso: Agosto 2021].

[11] admin, «conmutadoresyrouters,» 19 Abril 2020. [En línea]. Available: https://www.conmutadoresyrouters.com/conmutadores/. [Último acceso: Agosto 2021].

[12] A. Abad Domingo, «Redes Locales,» de *Redes Locales*, Madrid, 2018, pp. 32-36.

[13] S. Suroto, «WLAN Security: Threats And Countermeasures,» *JOIV: INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION*, vol. 2, nº 4, pp. 232-238, 2018.

[14] J. Araújo y K. Silva, «A Performance Evaluation of WLAN-Femtocell-LTE beyond the Capacity Crunch. Does Femtocell have to overcome WLAN or can they coexist in HetNets?,» *Journal of Microwaves, Optoelectronics and Electromagnetic Applications (JMOe),* vol. 15, nº 04, 2016.

[15] O. Sarmiento, F. Guerrero y D. Rey Argote, «Fundamentos prácticos de seguridad en redes inalámbricas IEEE 802.11,» *g. Investig.*, vol. 28, nº 2, pp. 89-96, 2008.

[16] W. Méndez Moreno, D. Mosquera Palacios y E. Rivas Trujillo, «WEP, WPA and WPA2 encryption protocols vulnerability on wireless networks with Linux platform,» *Revista Tecnura*, vol. 19, pp. 79-87, 2015.

[17] O. Salamanca, «Sistema de gestión de seguridad para redes de área local para empresas desarrolladoras de software,» *Revista Venezolana de Información, Tecnología y Conocimiento*, vol. 13, nº 3, pp. 114-130, 2016.

[18] «ISO 27001,» 2017. [En línea]. Available: https://normaiso27001.es/. [Último acceso: Agosto 2021].

[19] M.-S. Jian y J. M.-T. Wu, «Hybrid Internet of Things (IoT) data transmission security corresponding to device verification,» *Journal of Ambient Intelligence and Humanized Computing,* 2021.

[20] A. Jurcut, T. Niculcea, P. Ranaweera y N.-A. Le-Khac , «Security Considerations for Internet of Things: A Survey,» *SN Computer Science*, vol. 1, nº 193, 2020.

[21] J. R. Beulah y D. S. Punithavathani, «A Hybrid Feature Selection Method for Improved Detection of Wired/Wireless Network Intrusions,» *Wireless Personal Communications,* vol. 98, pp. 1853-1869, 2018.

[22] T. Saedi y H. El-Ocla, «Improving Throughput in Lossy Wired/Wireless Networks,» *Wireless Personal Communications*, vol. 114, p. 2315–2326, 2020.

[23] L. H. Costa y V. Costa, «Vulnerabilities and solutions for isolation in FlowVisor-based virtual network environments,» *Journal of Internet Services and Applications,* vol. 6, nº 18, 2015.

[24] M. G. Moreira Santos y P. A. Alcívar Marcillo, «Security in the data link layer of the OSI model on LANs wired Cisco,» *JOURNAL OF SCIENCE AND RESEARCH,* vol. 3, nº CITT2017, pp. 106-112, 2018.

[25] S. A. Alabady, F. Al-Turjman y S. Din, «A Novel Security Model for Cooperative Virtual Networks in the IoT Era,» *International Journal of Parallel Programming,* vol. 48, pp. 280-295, 2018.

[26] M. Jacovic, K. Juretus, N. Kandasamy, J. Savidis y K. R. Dandekar, «Physical Layer Encryption for Wireless OFDM Communication Systems,» *Journal of Hardware and Systems Security,* vol. 4, pp. 230-245, 2020.

[27] A. G. Paz, D. B. Casanova y E. R. Fuentes Gari, «Propuesta de Protocolos de Seguridad para la Red Inalámbrica Local de la Universidad de Cienfuegos,» *UNIVERSIDAD Y SOCIEDAD,* vol. 8, nº 4, 2017.

[28] R. Nazir, A. A. Laghari, K. Kumar, S. David y M. Ali , «Survey on Wireless Network Security,» *Archives of Computational Methods in Engineering,* 2021.

[29] M. Humayun, B. Niazi, N. Z. Jhanjhi y M. Alshayeb, «Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study,» *Arabian Journal for Science and Engineering,* vol. 45, pp. 3171-3189, 2020.

[30] B. Alotaibi y K. Elleithy, «Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions,» *Wireless Personal Communications,* vol. 90, pp. 1261-1290, 2016.

[31] W. Li, X. Mingshan y Q. Fazhi, «Security Mechanism for user access to Single SSID WLAN,» *EPJ WEB OF CONFERENCES,* vol. 245, nº 07009, 2020.