UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM ATLACOMULCO

"Propuesta de prevención de ataques informáticos de una red LAN, mediante el escaneo de vulnerabilidades"

T E S I N A

Que para obtener el Título de:

Ingeniero en Computación

Presenta:

Janeth Segundo Galindo

Director de Tesina:

Mtro. José Antonio García Mejía

Atlacomulco, México; Septiembre del 2017

RESUMEN

El activo más importante en cualquier tipo de red es la información porque es la prioridad para cualquier tipo de usuario. Por lo tanto, el primer paso para iniciar la protección de la información es tener conocimiento acerca de las vulnerabilidades informáticas que pueden presentarse en una computadora, para ser capaces de prevenir ataques informáticos que provocan diferentes tipos de daños a la red como en el hardware o software.

La posibilidad de que los dispositivos sean víctima de un ataque informático ha aumentado rápidamente y los intrusos aprovechan esta situación para afectar la integridad, fiabilidad y disponibilidad de la información

Se realizó un caso de estudio en el cual se elaboró un conjunto de experimentos que simularon amenazas informáticas más comunes, para la obtención de resultados que retroalimentaran la propuesta de prevención para determinar cuál es la mejor forma de contrarrestar ataques informáticos en una red LAN.

No existe herramienta o método que proteja al 100% una computadora o red informática, pero es necesario seguir identificando riesgos, en el presente trabajo se realizó la detección de vulnerabilidades de una red LAN, mediante el uso de la herramienta de escaneo Nessus, para realizar la propuesta de prevención de ataques informáticos más comunes, con la finalidad de aumentar la seguridad informática.

Al final de la investigación, se mejoró el nivel de la seguridad, con la actualización del sistema operativo, software y el navegador, además del uso de antivirus, herramientas anti spyware, adware, phishing, y ransomware, así como el mejoramiento de las contraseñas.

ABSTRACT

The most important asset in any type of network is information because it is the priority for any type of user. Accordingly, the first step in initiating information protection is to have knowledge about informatics vulnerabilities that can be present on a computer, to be able to prevent computing attacks that provoke different types of damage to the network in hardware or software.

The possibility that the devices can be victims a computer attack has increased rapidly and intruders take advantage of this situation to affect the integrity, reliability and availability of the information.

A case study was made in which a set of experiments were developed that simulated the most common computer threats, to obtain results that feedback the prevention proposal to determine the best way to counteract computer attacks on a LAN

There is not a tool or a method that offers 100% of security for computers, but it is necessary to continue identifying risks. However; the following research proposes a LAN scan through a software called Nessus to detect vulnerability in the computers, having as a result a better security level.

At the end of the research the security level was improved, with the update of the operating system, software and the browser, in addition to the use of antivirus, tools anti-spyware, anti-adware, anti-phishing, anti-ransomware, and as well as improving passwords.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

Desde el inicio de las computadoras los intrusos informáticos han intentado aprovechar las debilidades o fallas en el sistema para causar diferentes ataques que pueden producir distintos tipos de daños en la información, software o el hardware y su modo de operación ha estado evolucionando a la par con la tecnología.

El incremento de ataques informáticos hacia las redes, se ha notado incluso más con el avance de las nuevas Tecnologías de la Información y Comunicación, con el objetivo de seguir intentando causar daños en contra de la integridad, disponibilidad y confidencialidad de la información.

Por lo tanto, el objetivo del presente trabajo de investigación es crear una propuesta de prevención de ataques que involucre el uso de diferentes métodos de prevención que ayuden a mejorar la seguridad informática de una Red de Área Local (LAN, por las siglas en inglés de Local Area Network).

La tesina está conformada por seis capítulos:

El capítulo 1 y 2, está compuesto por la introducción así como el planteamiento del problema donde se describen los objetivos, preguntas, justificación y los impactos de la investigación.

El capítulo 3 es el Estado del Arte donde se definen algunos conceptos concernientes a la información, seguridad de la red, sus elementos, clasificación, topologías, protocolos, medios de transmisión y dispositivos de conectividad, así como las vulnerabilidades de la red, las herramientas de escaneo, los diferentes tipos de amenazas, clasificación de ataques informáticos e intrusos de la red LAN y modo de operación.

En el capítulo 4 y 5 se describen los diferentes métodos de prevención de ataques informáticos y la herramienta de escaneo de vulnerabilidades “Nessus” asi como los simuladores de amenazas informáticas.

En el capítulo 6 denominado Metodología, se desarrolla el caso de estudio en la red LAN haciendo uso de los diferentes simuladores de amenazas informáticas y la herramienta de escaneo de vulnerabilidades.

En el capítulo 7 se realiza la discusión de los resultados obtenidos. Para finalizar con las conclusiones y recomendaciones para proyectos futuros.

Los ataques informáticos seguirán aprovechando cada vulnerabilidad que se encuentre en los sistemas, por lo tanto es necesario seguir en la búsqueda de nuevos métodos de prevención que se pueden emplear con la finalidad de disminuir las vulnerabilidades más comunes que se encuentren en las redes informáticas.

2 PLANTEAMIENTO DEL PROBLEMA

La protección de la información es la prioridad para cualquier tipo de usuario. De tal forma que el primer paso para iniciar la protección de la información es tener conocimiento acerca de las vulnerabilidades informáticas que se pueden presentar en cualquier tipo de red, así mismo de los ataques informáticos más comunes y la forma en la que el usuario puede proteger su información.

De acuerdo con el informe de 2014 de la OEA (Organización de los Estados Americanos) y Symantec sobre Tendencias de seguridad cibernética en América Latina y el Caribe, entre las principales amenazas y tendencias de ciberseguridad se reporta un crecimiento exponencial de las violaciones de datos con información personal. Asimismo, aumentan las prácticas que involucran ataques que restringen el acceso al sistema informático que infectan para luego exigir el pago de un rescate (ransomware), estafas en redes sociales, vulnerabilidades y riesgos en la computación móvil, programas maliciosos (malware), correo no deseado (spam) y robo de identidad dirigido a objetivos específicos (spear-phishing) [1].

Por esta razón es importante considerar el tema de la seguridad de una red LAN, ya que si existe alguna vulnerabilidad en la red, se puede utilizar para ocasionar alguna falla, que podría provocar problemas que generen un alto costo en lo relativo con la productividad, eficiencia o la perdida de datos que sean valiosas para el usuario, por este motivo la finalidad de este proyecto es la detección de vulnerabilidades más comunes que se puedan presentar en una red LAN que no cuente con un sistema de seguridad adecuado y realizar una propuesta eficaz de prevención de ataques informáticos que ayuden a minimizar daños a la red.

La protección de una red LAN es una de las principales responsabilidades del administrador, quien debe estar en constante búsqueda de vulnerabilidades y riesgos que pudieran existir, para proteger la seguridad de la información y ser menos propensa a tener ataques informáticos.

2.1 Definición del problema

Debido al crecimiento exponencial de ataques informáticos, la probabilidad de que intrusos informáticos aprovechen las vulnerabilidades de la red ha incrementado poniendo en riesgo la integridad, confidencialidad y disponibilidad de la información.

El trabajo de investigación está orientado al desarrollo de una propuesta de prevención de ataques informáticos mediante el uso de la herramienta Nessus cuya finalidad será escanear las vulnerabilidades de una red LAN. Se realizará un caso de estudio en el cual se elaborará un conjunto de experimentos que simulen amenazas, para la obtención de resultados y verificar cual es la mejor forma de contrarrestar ataques informáticos en una red LAN. No se profundizará en las características físicas y el sistema operativo del equipo de cómputo conectado a la red por lo que se realizará un enfoque en la seguridad de la información.

2.2 Objetivos de investigación

Objetivo General

- Realizar una propuesta de prevención de ataques informáticos para una red de área local (LAN) mediante el escaneo de vulnerabilidades usando herramientas de detección de vulnerabilidades.

Objetivos Específicos

- Realizar un estudio sobre los problemas de vulnerabilidades, ataques, amenazas y soluciones para mejorar el nivel de seguridad de una red LAN.
- Diseñar un conjunto de experimentos con simuladores de amenazas informáticas y realizar la detección de las vulnerabilidades.
- Analizar los factores principales que provocan que el equipo sea más vulnerable a los ataques informáticos.
- Desarrollar una estrategia para evitar y contrarrestar ataques informáticos en una red LAN.

2.3 Preguntas de investigación

- ¿Cuáles son los ataques más frecuentes en una red LAN?
- ¿Cuáles son los tipos de vulnerabilidades informáticas que ocasiona que una red sea más propensa a sufrir algún tipo de ataque informático?
- ¿Cuál es la mejor solución a la prevención de ataques informáticos?
- ¿Cómo se implementarán las recomendaciones de prevención de ataques informáticos?

2.4 Justificación

La falta de uso de métodos de prevención de ataques y medidas de seguridad en las redes es un problema que sigue en crecimiento, así como el internet y la tecnología; conforme a esto el número de atacantes es mayor por este motivo el fomentar una educación acerca de los tipos de ataques informáticos y vulnerabilidades a las que puede ser propenso una red, es de vital importancia puesto que el estar informados siempre será la mejor herramienta para la protección de la información, además de que es la clave para la disminución de los ataques informáticos.

Según un informe de la compañía de Panda Labs, en el 2017 Asia y Latinoamérica son las regiones con mayores infecciones, siendo México el séptimo país en tener un mayor índice de infección de ataques informáticos. El índice de ataques informáticos siguen en aumento siendo el caso del virus WannaCry que en su primera aparición en el 2017 afecto a 120,000 equipos en más de 150 países [2].

Es de suma importancia diseñar una propuesta de prevención de ataques informáticos mediante el escaneo de vulnerabilidades para que los administradores de red conozcan la forma en la que se puede prevenir estos ataques y disminuir los riesgos de la red.

2.5 Impactos

- Proporcionar una propuesta de solución para la prevención de ataques informáticos como herramienta para la reducción de vulnerabilidades de una red LAN.
- Disminuir el tiempo y costo que el responsable de la red LAN invierte en el mantenimiento correctivo de los equipos de cómputo.

3 ESTADO DEL ARTE

En este capítulo se presentarán los conceptos fundamentales que están relacionados a la seguridad de la red informática que está compuesta por diferentes dispositivos, medios de transmisión, protocolos, diseñada con distintas topologías para realizar la transmisión y almacenamiento de diferente tipo de información. Dependiendo del diseño físico y lógico de una red van apareciendo diferentes vulnerabilidades que pueden ser aprovechadas por intrusos para causar ataques informáticos. Por lo tanto es necesario hacer uso de herramientas y técnicas de escaneo de vulnerabilidades de la red, que en primer lugar ofrecen una perspectiva general sobre la seguridad informática, permitiendo conocer las fallas o riesgos que pueden afectar la red, para después poder tomar medidas de prevención en las áreas que cuenten con vulnerabilidades.

3.1 Definición de Información

La información es un conjunto de datos que proporcionan un significado o un mensaje y que son útiles para el usuario, de tal forma que la información puede ser utilizada para la toma de decisiones, resolver problemas o adquirir más conocimiento sobre algún fenómeno o tema en específico. La información puede ser clasificada en dos tipos [3]:

- **Información pública:** Es el conjunto de datos que son producidos en el marco de la actividad del servicio público, es información que cualquier persona tiene derecho a consultar, solicitar y recibir.
- **Información privada**: Conjunto de datos que la ley no permite divulgar ya que afecta la intimidad personal, la seguridad nacional o simplemente es excluida por la ley, por ejemplo contraseñas de correos electrónicos, datos personales o bancarios.

Sin importar el tipo de información con la que cuente el usuario es de vital importancia mantenerla segura para evitar que intrusos tengan acceso y hagan mal uso de estas, para evitar estar involucrados en situaciones poco favorables por el uso que se le puede dar a la información que fue sustraído del usuario o red.

3.1.1 Importancia de la Seguridad de la Información

El activo más importante de cualquier sistema o red informática siempre será la información ya sea perteneciente a una organización o cualquier tipo de usuario. Es

inevitable que siga en aumento la información que se encuentra en formato digital por el incremento de las tecnologías de información y telecomunicaciones, por esta razón, se debe de proteger ante cualquier tipo de amenaza informática que pretenda robarla, alterarla, destruirla y modificarla, o se realice la perdida accidentalmente de la información por lo que es necesario usar métodos y herramientas de protección.

Una vez que la información es sustraída es difícil poder recuperarla además deja de ser confidencial porque evidentemente el intruso que ha obtenido la información conoce todos los datos acerca de está y las puede emplear para realizar actos ilícitos, por este motivo la protección de la información es fundamental, una forma de mantenerla protegida es mejorar el nivel de seguridad con diferentes métodos de prevención, además de la realización continua de copias de seguridad y el almacenamiento redundante [4].

3.2 Definición de Seguridad Informática

La seguridad informática hace referencia a todas las medidas y controles que se deben establecer para el aseguramiento de los sistemas informáticos, impidiendo que intrusos internos o externos realicen procedimientos no autorizados sobre la red. La seguridad informática comprende la protección de [5]:

Aplicaciones: Para evitar algún problema de seguridad informática las aplicaciones se deben de descargar en fuentes confiables y actualizarlas frecuentemente.

Comunicaciones: Es necesario evitar la interceptación de la comunicaciones haciendo uso de canales de comunicación cifrada, además de tener un constante control de las conexiones para impedir conexiones no autorizadas.

Datos: Para mantener protegidos los datos es necesario realizar constantemente copias de seguridad, el cifrado de la información, realizar un almacenamiento redundante de datos y deshabilitar componentes que supongan la entrada o salida de información no autorizada.

Equipos: Para evitar el robo de equipos se debe de cifrar los contenidos críticos, controlar o evitar los intentos de conexión de equipos externos no autorizados, y realizar mantenimientos preventivos.

La seguridad informática trata de mantener seguro la: Integridad, Privacidad, Disponibilidad, Control y Autenticidad de la información, que se encuentra almacenada en una computadora.

En la Enciclopedia de la Seguridad informática, el autor Gómez Vieites Álvaro explica la definición de los siguientes conceptos [6]:

Integridad: Se encarga de garantizar que un mensaje o fichero no sea modificado desde su creación o durante su transmisión a través de una red informática hasta llegar al receptor.

Confidencialidad: Es la necesidad de garantizar que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, estas no podrán tener acceso al contenido del mensaje original.

Disponibilidad: Se encarga de garantizar la permanente disposición de los servicios a los que los usuarios deseen acceder.

Control: Permite asegurar que sólo los usuarios autorizados puedan decidir cuándo y cómo permitir el acceso a los servicios o información.

Autenticidad: Se encarga de garantiza que la identidad del creador de un mensaje o documento sea legítima.

Para poder definir a un sistema informático como seguro debe de cumplir con los tres principios básicos de la seguridad de la información de acuerdo al estándar ISO 27002 [7], es decir, mantener segura la integridad, confidencialidad y disponibilidad de la información, como se muestra en la Figura 3.1.

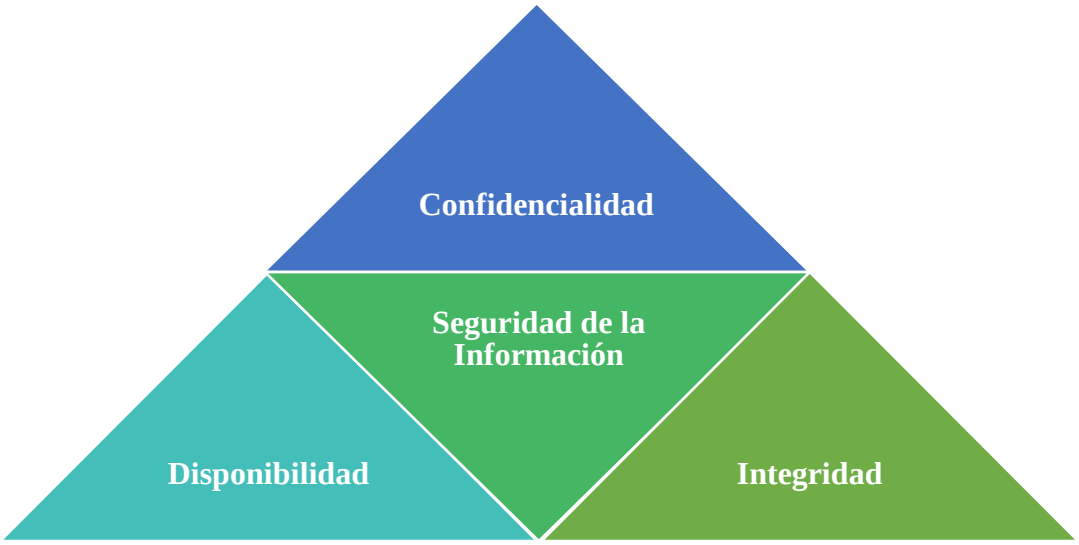


Figura 3.1.- Principios básicos de la seguridad de la información [7].

La finalidad de la seguridad informática es proteger el almacenamiento, procesamiento y transmisión de la información digital en cualquier tipo de red informática para que no pueda ser interceptada por ningún tipo de intruso informático [4].

3.2.1 Objetivos de la Seguridad Informática

Los principales objetivos de la seguridad informática en cualquier tipo de red son los siguientes [8]:

- Mantener protegida la información digital, el hardware y software de la red.
- Asegurar el adecuado uso de los recursos y de las aplicaciones del sistema.
- Identificar las vulnerabilidades con las que cuenta la red, para poder emplear métodos de prevención y de este modo poder proteger la información.
- Asegurar la confidencialidad, integridad y disponibilidad en los sistemas informáticos.
- Minimizar los riesgos, amenazas y vulnerabilidades que se encuentren en la red mediante uso de herramientas de protección.
- Contar con métodos eficaces de acciones de recuperación del sistema en caso de un incidente de seguridad.
- Evitar la fuga de información mediante el constante mantenimiento en la seguridad de la red informática.

3.3 Definición de red informática

Una red informática es aquella que está formada por un grupo de computadoras, periféricos, y otros dispositivos que se encuentran interconectados a través de uno o varios medios de transmisión, haciendo uso de protocolos y que en conjunto comparten los recursos e información.

Es necesario que una red cumpla con los siguientes criterios para que sea considerada efectiva y eficiente [9]:

Fiabilidad: Es medida por la exactitud de la entrega de la información, la frecuencia de fallos y el tiempo de recuperación de la red ante una falla en la red.

Rendimiento: Es medida por el tiempo de tránsito (duración en la que tarda un mensaje en ser enviado), y el tiempo de respuesta (duración que transcurre entre una petición y la respuesta). El rendimiento es relacionado a las siguientes dos métricas; ancho de banda que es la capacidad de un medio para transmitir datos y la latencia que es el tiempo que tarda un mensaje en llegar a su destino.

Seguridad Informática: Es el nivel de protección con el que se cuenta en la red, para ser capaz de proteger los datos frente a intrusos internos o externos que pretendan realizar acciones de monitoreo, modificación, intercepción y eliminación de la información. Además de contar con procedimientos de recuperación cuando se sufra alguna amenaza informática.

Con el uso de las redes informáticas la transmisión de la información es más rápida y eficaz tanto como su almacenamiento o el uso de diferentes tipos de software que facilitan muchas de las actividades cotidianas de los usuarios de la red. Pero si alguno de los criterios tiene alguna vulnerabilidad, existe la posibilidad que algún intruso trate de aprovecharlas para causar algún daño, por lo que es necesario estar en una constante mejora de la seguridad de la red.

3.3.1 Componentes de una red

Una red informática tiene dos tipos de componentes, físicos y lógicos [10]:

Componentes físicos

Los componentes lógicos de una red son:

- **Hardware:** Son un conjunto de componentes físicos que conforman la red (computadora, routers, switches, brigdes, hubs, servidor, etc.)
- **Medios de transmisión:** Es el conjunto de vías físicas a través de los cuales pasan las señales de transmisión de datos para tener comunicación (cable par trenzado, coaxial, fibra óptica).

Componentes lógicos

Los componentes lógicos de una red son:

- **Software:** Conjunto de programas que son utilizados para realizar diferentes actividades en la red (sistemas operativos, aplicación, servicio).
- **Protocolos:** Son el conjunto de reglas y normas que establecen la forma de intercambio de información a través de la red (tcp, udp, http, dns, ftp, etc).
- **Modelo de referencia OSI:** Está constituido por siete capas que sirven para describir el proceso de enviar y recibir datos a través de la red.
- **Modelo de referencia TCP/IP:** Constituido por cuatro capas, describen el proceso que se realiza en la transmisión de la información.

3.3.2 Elementos fundamentales de una red

Los elementos de una red son [10]:

Servidor: Permite a las computadoras conectadas a la red, comúnmente llamados clientes, compartir recursos e información, es el encargado de administrar los servicios de la red. Tiene que tener una suficiente capacidad de disco duro para el almacenamiento del software que sea requerido para el uso de la red, suficiente memoria RAM, y contar con ranuras de expansión disponibles para el futuro.

Sistema operativo de red: Es aquel que administra las operaciones de la red como el soporte de archivos, comunicaciones y el servicio para el soporte de equipo.

Estaciones de trabajo: Son el conjunto de computadoras que comparten los recursos del servidor y se interconectan a la red mediante una tarjeta de interfaz.

Tarjeta de interfaz de red: Para que las computadoras puedan tener comunicación a la red y al servidor, deben de contar con una tarjeta de interface de red o NIC (*Network Interface Cards*). Estos elementos son necesarios en el funcionamiento de la red, el uso de estos elementos depende del tamaño de la red y de su diseño.

3.3.3 Medios de transmisión de una red

Cualquier tipo de red informática debe hacer uso de diferentes medios de transmisión, que son la vía en la que el emisor y receptor se pueden comunicar, compartir información. Se pueden clasificar en guiados y no guiados [10,11]:

Medios guiados: Son aquellos que se necesitan para conectar entre si las estaciones de trabajo y diferentes dispositivos o nodos de la red para transmitir información. Existen diferentes factores que se necesitan verificar, al momento de elegir algún tipo de medio guiado:

- El rendimiento que se necesita en la red informática.
- El entorno en donde se va a realizar la instalación.
- La fiabilidad y facilidad de instalación.
- El tipo de dispositivo que se desea conectar.
- El costo o presupuesto con el que se cuenta.

Los diferentes tipos de medios guiados son:

Cable de par trenzado: Está compuesto de dos cables trenzados entre sí, para reducir el ruido, la diafonía y las interferencias eléctricas provenientes de líneas cercanas, son de cobre aislados por un material de pastico. Son el tipo de cable más utilizado por su bajo costo, además de ser flexibles y fáciles de conectar. Pero cuenta con la desventaja de solo poderse usar distancias limitadas(a menos de 100 metros), si se sobrepasa esta distancia la señal se pierde. Existen dos tipos de cable de par trenzado:

Cable sin blindaje (UTP, Unshielded Twisted Pair): Este cable está formado por dos conductores de cobre, cada uno cuenta con un aislamiento de plástico de color para su

identificación al momento de conectarlos ya sea por conexión directa (conexión de diferentes dispositivos) o cruzada (conexión de dispositivos iguales) y utilizan un conector RJ-45 de 8 conductores.

El cable UTP cuenta con diferentes categorías:

- Categoría 1: Son cables de par trenzado utilizados específicamente para el diseño de redes telefónicas. Con un intervalo máximo de velocidad de hasta 4Mbps en un intervalo de frecuencia menor a 100KHz.
- Categoría 2: Con características similares a los cables de categoría 1 pero funcionan en aplicaciones de voz y datos. Con un intervalo máximo de velocidad de 1 Mbps en un intervalo de frecuencias de 1 MHz.
- Categoría 3: Son cables que permiten aplicaciones de voz y datos, utilizado en redes de ordenadores, son utilizadas en redes LAN. Con un intervalo máximo de velocidad de hasta 10 Mbps en un intervalo de frecuencia de 16 MHz.
- Categoría 4: Es utilizada en redes con topología de anillo, con características similares a la categoría 3. Con un intervalo máximo de velocidad de hasta 16 Mbps en un intervalo de frecuencia de 20 MHz.
- Categoría 5: Es el cable más utilizado en redes LAN. Con un intervalo máximo de velocidad de hasta 100 Mbps en un intervalo de frecuencia de 100 MHz.
- Categoría 5e: Es una categoría 5 mejorada, que minimiza las interferencias. Con un intervalo máximo de velocidad de hasta 1000 Mbps en un intervalo de frecuencia de 100 MHz.
- Categoría 6: Con un intervalo máximo de velocidad de hasta 1000 Mbps en un intervalo de frecuencia de 250 MHz.
- Categoría 6a: Es una categoría 6 mejorada. Con un intervalo máximo de velocidad de hasta 10 Gigabits en un intervalo de frecuencia de 550 MHz.

Cable con blindaje (STP, Shielded Twisted Pair): Es un cable más protegido y menos flexible porque tiene una funda de metal o de malla entrelazada que rodea cada par de conductores aislados, evita que se infiltre el ruido electromagnético y elimina la interferencia. El cable STP usa los mismos conectores que el UTP, pero es necesario conectar el blindaje a tierra. Puede ser ocupado a un rango de distancia de hasta 500 metros

sin necesidad de hacer uso de un repetidor pero es demasiado costoso y difícil de instalar en comparación con el cable UTP

Cable coaxial: Es un cable que está formado por un conductor fijo sobre una funda de material aislante y una cubierta metálica en forma de malla como segundo conector. También llamado 10Base 2. Evita la radiación electromagnética y elimina la interferencia. Cuenta con un gran ancho de banda, es menos susceptible a interferencias, ofrece mayor frecuencia, mayor velocidad de transmisión en comparación con el cable de par trenzado, pero es más caro y pesado, además su instalación lleva más tiempo.

Existen dos tipos de cable coaxial:

Cable coaxial delgado: Este cable es medio flexible y fácil de instalar pero posee menor inmunidad frente a interferencias. Con un grosor de 6mm, puede ser utilizado en cualquier tipo de red. Puede ser instalado a una distancia de hasta 185 metros sin sufrir atenuación, con un intervalo máximo de velocidad de hasta 10Mbps.

Cable coaxial grueso: Este cable posee un conductor de mayor grosor de 13mm. También conocido como 10Base 5. Puede ser instalado a una distancia de hasta 500 metros permitiendo un máximo de 100 nodos sin sufrir atenuaciones en la red, con un intervalo máximo de velocidad de hasta 10Mbps.

Fibra Óptica: Es un delgado filamento hecho de silicio o cristal, con un alto índice de refracción de luz que transmite las señales en forma de luz. Puede ser instalado a una distancia de hasta 30 kilómetros sin sufrir atenuación Con un intervalo máximo de velocidad de hasta 1 Gbps. Su instalación y mantenimiento tienen un costo elevado, lo cual hace que solo sea empleado cuando la información es demasiada o es necesario cubrir largas distancias

Medios no guiados: Son aquellas que no necesitan ningún tipo de cable para transmitir información. Se basan en la propagación de ondas electromagnéticas a través del medio (aire, vacío). Se clasifican en:

Ondas de radio: Son multidireccionales, es decir que la información viaja en diferentes direcciones, capaces de recorrer grandes distancias y atravesar materiales sólidos. Son empleadas en las redes WiFi o Bluetooth.

Microondas: Transmiten los datos a través de radiofrecuencia con longitudes de onda del tipo microonda. Se utilizan en sustitución del cable coaxial o las fibras ópticas. La información viaja en línea recta por lo que el emisor y receptor deben de estar alineado cuidadosamente, tienen dificultades para atravesar materiales sólidos, rebotando en materiales hechos de metal, además está sujeto a interferencias provocadas por el ambiente (mal clima).

Infrarrojos: La comunicación se lleva a cabo mediante transmisores/receptores que modulan luz infrarroja no coherente. Este tipo de señal es barata y difícil de interceptar pero no cuentan con un gran rango de velocidad de transmisión además de no poder atravesar materiales sólidos.

Ondas de luz: Son el mismo tipo de ondas que utilizan las fibras ópticas, son unidireccionales es decir que solo viajan en una dirección, por lo que se pueden utilizar para comunicar dos edificios cercanos.

3.4 Dispositivos de conectividad de la red.

Los dispositivos de conectividad permiten que los equipos estén conectados entre sí y que puedan enviar datos o compartir la información en la red mediante algún medio externo de transmisión. Permiten la interconexión de varias redes, que se encuentren en la misma zona geográfica.

Algunos de los dispositivos de conectividad más usados en las redes informáticas son [12]:

Concentrador (Hub): Es un dispositivo que permite centralizar el cableado de la red, permite expandirla. Su función es recibir una señal que este solicitando ser transmitida de alguna de las estaciones de trabajo o segmento de la red y la emite por sus diferentes puertos. Es ocupado en las redes que cuentan con una topología en estrella porque usualmente es el nodo central.

Puente (Bridge): Dispositivo que realiza una interconexión de dos segmentos de la red o realiza una división de una red en segmentos, realizando la transmisión de datos de una red hacia otra de acuerdo a una dirección física de destino establecida para cada paquete, usando una tabla de direcciones MAC detectadas en cada segmento de los nodos que estén conectados, es decir; verifica las direcciones asociadas a cada paquete de información y

envía el paquete a su destino sin importar si tiene que pasar de un segmento a otro. Con el uso de este dispositivo se puede reducir notablemente el tráfico de los distintos segmentos conectados a él.

Conmutador (Switch): Dispositivo que realiza el envió de información a un usuario en específico sin necesidad de ser retransmitido al resto de los puertos. Son utilizados cuando se desea conectar múltiples redes convirtiéndolas en una sola, funcionan como un filtro en la red. Si son ocupadas en redes LAN mejoran su rendimiento y seguridad.

Enrutador (Router): Es un dispositivo de hardware o software de interconexión que interconecta segmentos de red o redes enteras. Es capaz de adaptar la estructura de información de una red a otra. Encamina la información por la ruta que considere más óptima además de reagrupar la información que viene por rutas distintas. Es utilizado para la creación de varias sub redes, permite el uso de varias clases de direcciones IP dentro de una misma red. Es usado en instalaciones más grandes ya que aumentan la seguridad y simplicidad, pero todo depende de la forma en la que sean configuradas. Permite conectar redes con diferentes topologías. Es usualmente ocupado para conectar una red LAN a Internet o entre sí mismas.

Modem: Dispositivo cuya función es modular y desmodular las señales, es decir; convierte las señales digitales en analógicas y viceversa para permitir la transmisión y recepción de una señal.

Repetidor: Es un dispositivo que es capaz de recibir una señal débil o de bajo nivel y regenerar la señal de transmisión con una potencia o nivel más alto, para que pueda ser enviada a distancias más largas sin degradación o con una degradación tolerable. Opera solamente de forma física para permitir que los bits viajen a mayor distancia a través de los medios.

La transmisión de la información usando diferentes tipos de dispositivos de conectividad depende del modelo de referencia que la red este ocupando (TCP/IP, OSI), este es el que proporciona una referencia común para mantener consistencia de conectividad en todos los tipos de protocolos y servicios de red. El modelo de referencia más ocupado actualmente es el Modelo OSI.

3.5 Modelo OSI (Open Systems Interconnection Reference Model)

El Modelo de Referencia de Interconexión de Sistemas Abiertos, fue diseñado en 1984, por la Organización Internacional para la Normalización (ISO). Está compuesto por siete capas como se muestra en la Figura 3.2, cada una realiza una función específica para poder permitir la interconexión y transmisión de datos dentro de una red [10].

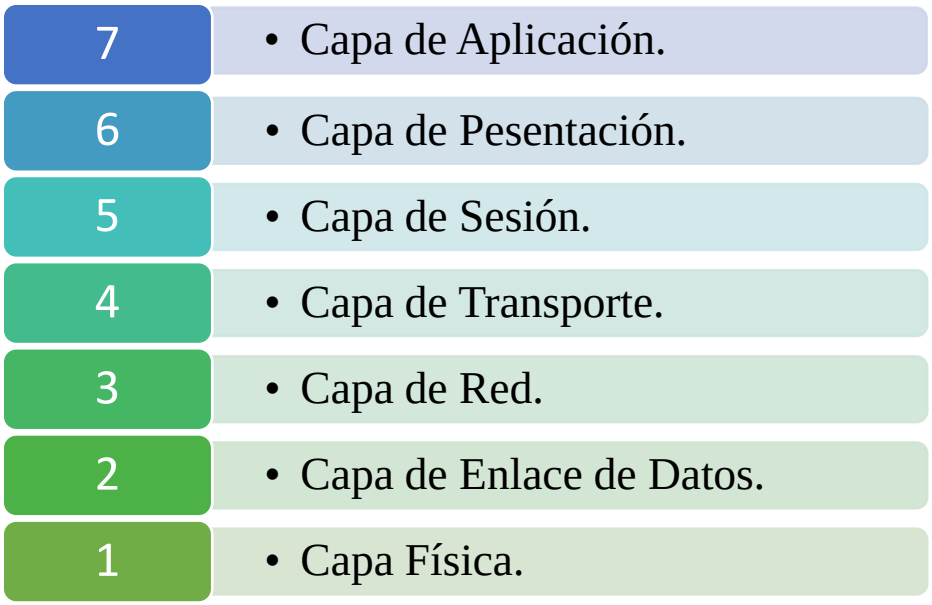


Figura 3.2.-Capas del Modelo OSI [10].

Capas del modelo OSI

1. **Capa física:** Transmite la información a un entorno físico, abarca los aspectos físicos como los cables, switch, topología y el resto de dispositivos que conforman el entorno físico de la red, por esto el usuario interactúa con esta capa.
2. **Capa de Enlace de datos:** Se encarga de desplazar los datos por el enlace físico de comunicación hasta el nodo receptor, mediante una entrega fiable y responsable. Además de realizar una detección de errores y si llegase a suceder un error realiza una retransmisión de los datos.
3. **Capa de Red:** Encamina y entrega los paquetes desde el origen al destino. También es el encargado de determinar la ruta que deben seguir los datos.
4. **Capa de Transporte:** Se encarga de controlar el flujo de datos, para que puedan entregar los paquetes en la secuencia establecida entre los nodos que establecen

una comunicación, mediante la supervisión del control del errores y el control del flujo de datos.

5. **Capa de Sesión:** Se encarga de establecer, almacenar, administrar y finalizar una conexión entre el emisor y receptor. Una vez establecida esta capa se encarga de ubicar puntos de control de secuencia de datos, para crear una tolerancia a los fallos mientras que exista una sesión de comunicación.
6. **Capa de presentación:** Esta capa es considerada el traductor del modelo OSI, toma los paquetes que se generan en la capa de aplicación y los convierte en un formato genérico que puedan leer todas las computadoras, además de comprimirlos para reducir su tamaño.
7. **Capa de Aplicación:** Se encarga de ofrecer al usuario acceso general a la red. Proporciona la interfaz y servicios que soportan las aplicaciones de usuario, como el correo electrónico, servicios de directorio, gestión de datos compartidos, el acceso y transferencia de archivos remotos, entre otros tipos de servicios para información distribuida.

El modelo OSI fue creado después del modelo TCP/IP cuya finalidad es hacer que la comunicación entre todas las computadoras de una red informática que esten usando algún protocolo sea compatible para poder realizar la transmisión de información, es decir, permite que los datos se traduzcan a un formato apropiado para la arquitectura de red a la que es enviada.

Modelo de protocolo TCP/ IP (Transmission Control Protocol/ Internet Protocol):

El modelo TCP/IP fue creado en 1972 por el departamento de Defensa de los Estados Unidos, utilizada en ARPANET. Describe un conjunto de normas de diseño e implementación de protocolos de red específicos que permite la transmisión de datos de una red a otra. Es la base actual del Internet y sirve para enlazar computadoras que utilizan diferentes tipos de sistemas operativos. Está compuesto por cuatro capas como se muestran en la Figura 3.3.

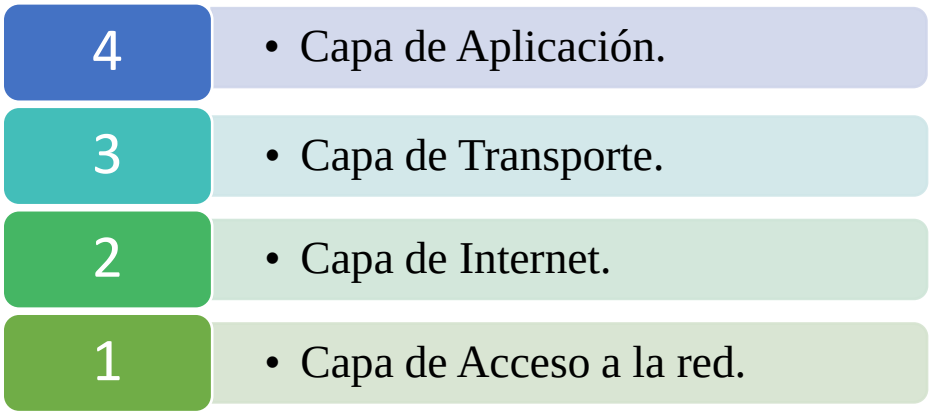


Figura 3.3.-Capas del modelo TCP/IP [13].

Cada capa realiza una función en específico que permite realizar la transmisión de datos en las redes informáticas [13]:

1. **Capa de acceso a la red**: Se encarga de especificar la forma en la que los datos deben transmitirse por la red.
2. **Capa de Internet:** Se encarga de proporcionar los datagramas (paquetes de datos), además de administrar las direcciones IP, por esta razón permite el enrutamiento de la información, la administración de la división de datagramas y el ensamblarlo cuando lleguen a su destino.
3. **Capa de Transporte:** Es responsable de brindar los datos de enrutamiento, junto con mecanismos que permitan conocer el estado de la transmisión de los paquetes. Permite que las aplicaciones que se están ejecutando en los equipos remotos puedan comunicarse.
4. **Capa de aplicación:** Incorpora aplicaciones de red estándar, que permiten la comunicación con las otras capas.

El modelo de TCP/IP tiene un alto grado de fiabilidad en la trasmisión de datos, realiza la conexión de la red de origen a la de destino, especificando cómo los datos deberían ser convertidos, direccionados, transmitidos, enrutados y recibidos por el destinatario. Es usado a nivel mundial para conectarse a Internet y a los servidores web.

3.6 Protocolos de red

Los modelos OSI o TCP/IP hacen uso de diferentes protocolos de red en cada una de sus capas, que son un conjunto de reglas normalizadas que permiten la correcta transmisión y comunicación de la información entre nodos en una red a través de un canal de comunicación. Un protocolo es capaz de definir, que se va a transmitir, en que forma y en qué tiempo se realizará la comunicación [10].

Un protocolo tiene asignada las siguientes tareas [14]:

- *Temporización:* Es el intervalo de tiempo que el protocolo destina para hacer el envío y recepción de los paquetes.
- *Semántica:* Es el significado de cada sección de bit, denominados campos, en los cuales se alberga información necesaria para la correcta comunicación y transmisión de la información.
- *Sintaxis:* Es la estructura del formato de los datos que se van a transmitir, determina el orden y la longitud de los campos dentro de cada paquete.

Los protocolos se caracterizan por ser [15]:

Directos: Es cuando la información pasa directamente entre el emisor y receptor sin la intervención de un agente activo.

Indirectos: El envío de información que se realiza entre dos entidades de diferentes redes se convierte en indirecto, intervienen elementos intermedios.

Monolíticos Sucede cuando el emisor tiene el control en una sola capa de todo el proceso de transferencia y contiene el mismo software para el proceso.

Estructurados: En un protocolo estructurado, existen varias capas que se coordinan y que dividen la tarea de comunicación.

Simétricos: Son aquellos donde los dos nodos que se comunican son semejantes, es decir ambos pueden ser emisores tanto como receptores.

Asimétricos: Es cuando una de los nodos tiene funciones diferentes de la otra, por ejemplo en clientes y servidores.

Estándares: Es utilizado para realizar una comunicación bastante organizada, que requiere de una serie de estándares para poder realizarla.

No Estándares: Es aquel que fue creado específicamente para un caso concreto, se usa para una comunicación en particular y que es necesario realizar su conexion con agentes externos.

Funciones de un protocolo de red

Las funciones de un protocolo se pueden agrupar en [15]:

- **Encapsulamiento:** Proceso en el cual se añaden los datos de información de control, son encapsulados en la PDU (Protocolo de Unidades de Datos).
- **Segmentación:** Proceso de dividir la información en bloques manejables.
- **Ensamblado:** Proceso inverso a la segmentación para recuperar el formato original de la información, para después ser entregados a la entidad de aplicación de destino.
- **Control de la conexión:** Realiza la administración del proceso de intercambio de información con sistemas orientados a la conexión o sin conexión. Se realiza mediante el hecho de que ambos extremos numeren y controlen las PDU tanto de entrada como de salida.
- **Entrada en orden:** Si dos entidades de host residen en diferentes host conectadas a través de la red, existe la posibilidad de que un PDU llegue con un orden diferente al de partida, por haber tomado diferentes rutas para llegar al destino.
- **Control de flujo:** Proceso que realiza la entidad receptora sobre la entidad emisora para evitar que la velocidad de la segunda desborde su capacidad de recibir datos y estos se pierdan, es decir, que delimita la velocidad o cantidad de datos que envía la entidad emisora.
- **Control de errores:** Son ocupadas para recuperar paquetes perdidos o deteriorados en los datos y de la información de control. Se implementan mediante dos funciones: detección de errores y la retransmisión.
- **Direccionamiento:** Este aspecto tiene que ver con la eficaz entrega de la PDU a las entidades que corresponda.

- **Multiplexación:** Realiza varias conexiones dentro de un solo sistema. Se puede realizar de modo ascendente (varias conexiones del nivel superior se comparten sobre una única conexión del nivel inferior) y de modo descendente (establece una única conexión del nivel superior utilizando varias conexiones del nivel inferior).
- **Servicios de transmisión:** Existen varios servicios que dependen de los servicios de transmisión, como por ejemplo: Prioridad (jerarquiza los mensajes a enviar), Calidad de servicio (velocidad en la entrega de los mensajes) y Seguridad (resguardo ante usuarios no autorizados).

Algunos de los protocolos más utilizados en algunas de las capas del modelo OSI o TCP/IP son [10]:

FTP *(File Transfer Protocol)*: El Protocolo de Transferencia de Archivos, se utiliza para compartir información además realiza la detección y corrección de errores solamente cuando se transfieren los archivos. Ocupado en la capa 7 del modelo OSI

TCP/ IP *(Transmission Control Protocol/ Internet Protocol)*: Protocolo de Control de Transmisión/ Protocolo de Internet, está compuesto por un conjunto de protocolos encaminados que puede ejecutarse en distintas plataformas de software y casi todos los sistemas operativos lo soportan como protocolo de red predeterminado. Es decir que su objetivo es permitir la comunicación entre nodos pertenecientes a una red.

ICMP *(Internet Control Message Protocol)*: El Protocolo de Mensajes de Control para Internet se encarga de facilitar o enviar los mensajes de error a los administradores del sistema, indicando que un paquete no puede llegar a su destino, si el encabezamiento lleva un valor no permitido, o si su tiempo de vida ha expirado. Ocupado en la capa 2 del modelo TCP/IP.

DHCP (*Dynamic Host Configuration Protocol*): El protocolo dinámico de configuración del host tiene la función de distribuir direcciones IP, las opciones de configuración a computadoras y estaciones de trabajo. Fue diseñado principalmente para ahorrar tiempo gestionando direcciones IP en redes de gran tamaño.

SMB *(Server Message Block):* Es un protocolo de Bloques de Mensajes del Servidor, cuya función es permitir que las aplicaciones de un equipo puedan leer, escribir archivos

y solicitar servicios desde los programas de un servidor en una red de equipos, por ejemplo realizar impresiones.

UDP *(User Datagram Protocol)*: El Protocolo de Datagrama de Usuario se limita a especificar los puertos de origen y destino para el envío del contenido del paquete, pero en ningún momento garantiza su entrega. Ocupado en la capa 4 del modelo OSI

SNMP *(Simple Network Managment)*: El Protocolo Simple de Administración de Red, es utilizado en la gestión de nodos de una red TCP/IP para controlar el estado de funcionamiento de los equipos o servicios.

HTTP *(Hypertext Transfer Protocol)*: El Protocolo de Transferencia de Hipertexto controla las transacciones entre un cliente de la web y un servidor de la web. Ocupada en la capa de aplicación del modelo OSI.

SMTP *(Simple Mail Transfer Protocol)*: El Protocolo Simple de Transferencia de Correo Electrónico, contiene un conjunto de reglas que rigen el formato para la transferencia de datos que se realizan en un envío de correo electrónico. Ocupado en la capa 7 del modelo OSI.

ARP *(Address Resolution Protocol)*: El protocolo de Resolución de Direcciones, permite asociar a un dispositivo de red, que a nivel físico posee una dirección física de red. Ocupado en la capa 3 del modelo OSI.

3.7 Clasificación de las redes informáticas

Las redes informáticas sin importar su clasificación hacen uso de un modelo de referencia con diferentes protocolos y se clasifican de acuerdo a la extensión geográfica que la red ocupe [16]:

- **Red PAN:** Red de Área Personal, tiene una extensión geográfica del alcance de una persona, que puede establecer comunicación con otros dispositivos en su propio entorno, por ejemplo conectar una computadora a una impresora.
- **Red LAN:** Red de Área Local, este tipo de red se caracteriza porque su extensión está limitada físicamente a un edificio, un cuarto, un salón, es decir que las redes LAN cubre un área geográfica relativamente pequeña. Se caracterizan por ser

capaces de compartir recursos (hardware, software y datos) entre las computadoras personales o de estaciones de trabajo. Las topologías más frecuentes en una red LAN son: estrella, bus y anillo. Cuentan con altas velocidades que pueden alcanzar de hasta 100 a 1000 Mbps, pueden transportar grandes volúmenes de datos con tiempos rápidos de respuesta. Suelen emplear medios de transmisión de datos mediante el uso del cable coaxial o UTP para la conexión de todas las maquinas.

- **Red CAN:** Red de Área Campus, la extensión geográfica de este tipo de red se delimita dentro de un campus (universitario, oficinas de gobierno, industrias), están formadas por una colección de redes LAN´s. Utilizan comúnmente tecnologías como Gigabit Ethernet para realizar la conexión a través de medios de comunicación como la fibra óptica.
- **Red MAN:** Red de Área Metropolitana, tiene una extensión geográfica mayor que la de una red LAN por ejemplo, una ciudad o un municipio. Con el uso de las redes MAN se puede realizar la interconexión de oficinas dispersas en una ciudad pero pertenecientes a una misma corporación. Están diseñada para clientes que necesitan una conexión de alta velocidad, normalmente a Internet, además las redes MAN pueden ser públicas o privadas.
- **Red WAN:** Red de Área Amplia tiene una extensión geográfica demasiado extensa, esta proporciona transmisión de información a larga distancia, por ejemplo alrededor de un país, una ciudad o incluso a nivel mundial.

  Contienen una gran colección de máquinas dedicadas a ejecutar los programas de usuarios. Una red WAN está conectada habitualmente a un enrutador que conecta a otros tipos de redes LAN o WAN.

3.8 Topologías de la red.

Es necesario que cada clasificación de red cuente con una topología, que se define como la construcción física o lógica de una unión de computadoras (nodos), periféricos entre otros dispositivos conectados entre sí mediante diferentes líneas de comunicación, es decir, hace referencia al modo en que están conectadas los nodos entre sí, que a su vez determina el tipo comunicación de la red.

En la Figura 3.4, se muestran algunas de las topologías de red que se describen a continuación [17]:

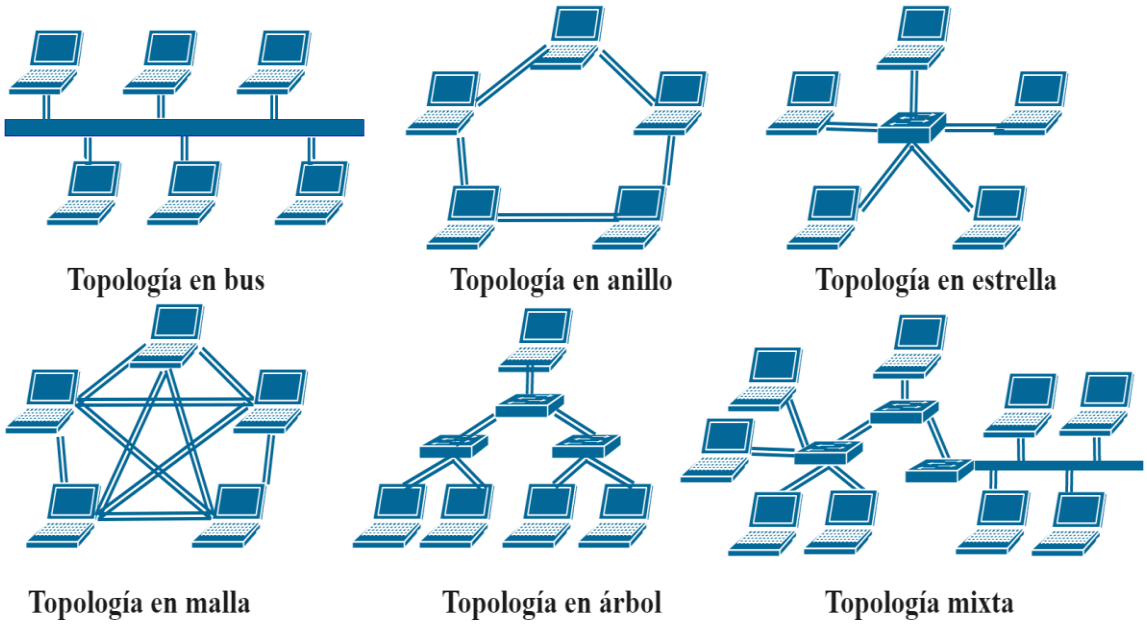


Figura 3.4.- Topologías de Red [17].

Topología en bus: También conocida como bus lineal**,** se caracteriza por que todos los nodos de la red están conectados entre sí por un mismo bus (cable backbone), por esta razón todos los nodos reciben la información que se transmite. La información circula por el bus en ambos sentidos y se mantiene de esta forma sin importar que algún nodo de la red falle. Se caracteriza por ser fácil de instalar, pero su desventaja radica en la dificultad de su reconfiguración y el aislamiento de fallas

Topología en anillo: Se caracteriza por que cada nodo está conectado al siguiente nodo, y el último nodo se conecta al nodo inicial. Para realizar el envió de información cada nodo examina si es el destinatario de la información enviada y de no ser así pasa al siguiente por lo tanto tiene que pasar por los nodos necesarios hasta que llegue a su destinatario, pero si algún nodo de la red se desconecta o sufre alguna falla ocasiona la ruptura de la conexión de la red, en esta topología la información circula en un solo sentido.

Una topología en anillo es fácil de instalar y reconfigurar, los fallos se pueden aislar de forma sencilla además no existe colisión de paquetes de datos. Existen dos tipos de anillos:

- *Anillos simples:* Se cuenta con un solo anillo y se realiza el envió de información en una sola dirección.
- *Anillos dobles:* Se cuentan con dos anillos y se realiza el envió de información en ambos direcciones, si alguno de los anillos falla, los datos se pueden transmitir mediante el otro anillo.

Topología en estrella: Se caracteriza por que todos los nodos de la red tienen en común un nodo central. La información tiene que circular por el nodo central para llegar a su destinatario. Las redes locales ocupan este tipo de topologías, suelen utilizar como nodo central un enrutador (router), conmutador (switch) o un concentrador (hub). Si un nodo de la red falla, no afecta la red, simplemente queda fuera de ésta, pero si el nodo central se daña toda la red falla.

Es fácil de instalar y configurar, también se conoce como topología en estrella expandida cuando se incluye un nuevo dispositivo que es conectado simplemente al nodo principal de la red.

Topología en malla: Se caracteriza por que todos los nodos de la red están conectados entre sí mismos La información circula en varios sentidos, por lo tanto si un nodo de la red falla se puede enviar la información por otro sentido. Para que la red falle en su totalidad todos los nodos de la red deberían de tener alguna falla, por lo tanto este tipo de topología no tiende a tener ninguna interrupción en las comunicaciones, pero es demasiado costosa de crear por el hardware que se necesita para conectar cada enlace además de la cantidad de cable que se necesita utilizar, sin contar que es complicada para instalar y configurar.

Topología en árbol: Se caracteriza por que los nodos de la red están conectados en forma de árbol. Está compuesto un nodo de enlace troncal, generalmente ocupado por conmutador (switch), y a partir de él se empezaran a ramificar los demás nodos permitiendo que se puedan conectar más dispositivos y por tanto se puede incrementar la distancia en la que puede viajar la señal entre dos dispositivos. Si el nodo principal falla también la red. Permite a la red aislar y prioriza la comunicación de diferentes nodos.

Topología mixta: Se caracteriza por ser una combinación de diferentes tipos de topologías conservando sus características. Para realizar la construcción y diseño de cualquier tipo de topología el administrador de la red debe de tener en cuenta determinar el costo, las necesidades de la organización, el flujo de datos que se necesita.

Para realizar la selección del tipo de topología para una red informática, es necesario considerar diferentes factores como el costo de mantenimiento, la capacidad de expansión, el número de computadoras a conectar, la infraestructura física donde se implementará, la facilidad de instalación y reconfiguración de la red.

3.9 Definición de Vulnerabilidad

En las diferentes clasificaciones y topologías de redes se pueden encontrar vulnerabilidades que de acuerdo con la Enciclopedia de la Seguridad informática el término de vulnerabilidad hace referencia a *"un estado viciado en un sistema informático que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas"* [18].

De acuerdo al estándar de la Organización Internacional para la Estandarización (ISO) 27001 "*La vulnerabilidad de un activo de seguridad es la potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información"* [19].

Por lo tanto, la vulnerabilidad informática: es un estado, elemento o falla que puede ser ocupado por intrusos para causar algún daño en el sistema o red informática.

Si un intruso hace uso de las vulnerabilidades encontradas en el sistema puede realizar diferentes actividades [18]:

- Ejecutar comandos haciéndose pasar como otro usuario.
- Tener acceso a información confidencial del sistema informático y del usuario.
- Eliminar, modificar, monitorear información confidencial.
- Realizar denegación de servicios.
- Realizar daños en el hardware o software.
- Aumentar el riesgo de que la red informática pueda tener más vulnerabilidades.

Las vulnerabilidades tienen un ciclo de vida que se origina desde que se detectan, para luego basarse en la forma en la que un intruso explota las vulnerabilidades encontradas en la red informática, hasta llegar al momento en el que administrador de la red o el programador de la aplicación realiza actividades para llegar a una solución para tratar de disminuirlas o eliminarlas, como se muestra en la Figura 3.5 [20].

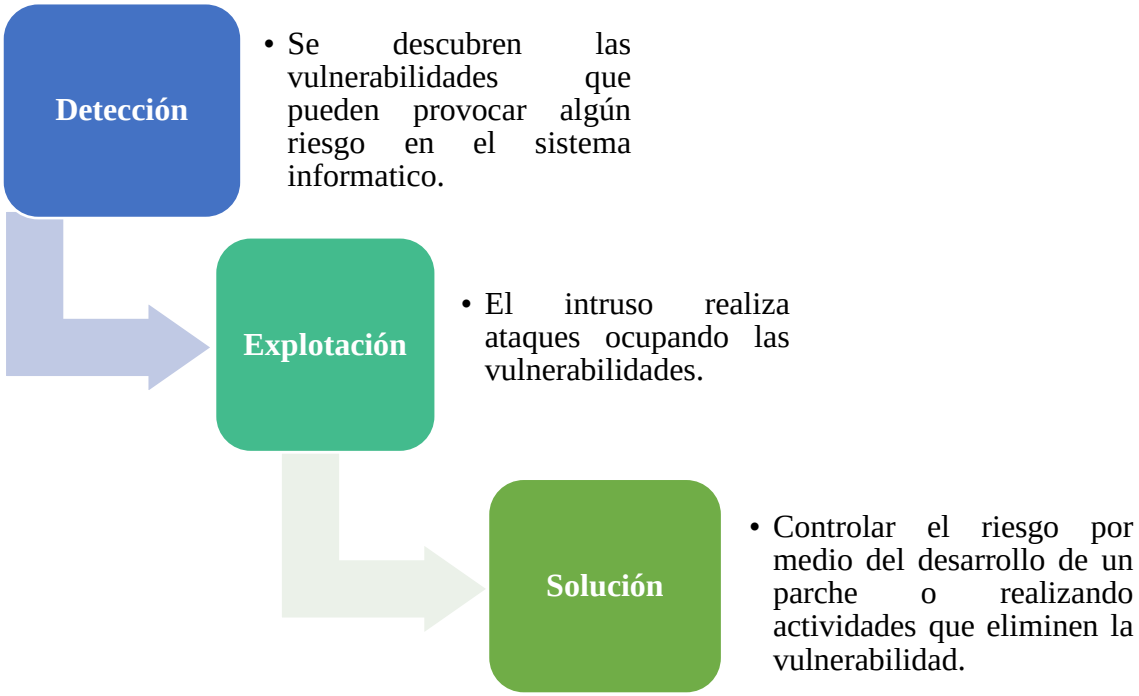


Figura 3.5.-Ciclo de vida de una vulnerabilidad [20].

La mayoría de las vulnerabilidades en un sistema pueden ser ocasionadas por fallas en el diseño o errores de programación e incluso por limitaciones tecnológicas, pero sin importar el tipo de vulnerabilidad estas pueden ser aprovechadas por los intrusos para causar cualquier tipo de daño.

3.9.1 Tipos de Vulnerabilidades Informáticas

Las vulnerabilidades que pueden presentarse un sistema o red informática deben de tenerse en cuenta para la correcta detección de las mismas. Se clasifican en [21]:

Comunicaciones o de red: Esta vulnerabilidad está presente al tener una serie de equipos de cómputo conectados entre sí existe la posibilidad de que un intruso acceda a solo uno de los equipos y posteriormente realizar su propagación en toda la red informática.

Emanaciones: Hace referencia a la posibilidad de interceptar radiaciones electromagnéticas para modificar o descifrar la información que es enviada y recibida de un receptor a un emisor.

Físicas: Son cualquier posible acceso físico desde las instalaciones hasta el equipo de cómputo que almacena información confidencial para substraerla, modificarla o eliminarla. Es un tipo de vulnerabilidad que se puede llevar a cabo por el mismo personal interno que hace mal uso de las políticas de acceso al sistema informático y medios físicos de almacenamiento de información.

Humanas: Son el tipo de vulnerabilidades más comunes en cualquier sistema, porque la falta de capacitación o información genera que los usuarios realicen actividades como el mal uso del equipo de cómputo o políticas de seguridad que den pauta a otros tipos de vulnerabilidades.

Hardware: Es la posibilidad de que alguna pieza física en el sistema informático falle (por un mal diseño, funcionamiento y uso), provocando daños o problemas mientras que se intenta arreglar la falla.

Naturales: Posibilidad de que el sistema informático sufra daños o perdidas causados por el ambiente o desastres naturales, como incendios, tormentas, inundaciones, terremotos. Este tipo de vulnerabilidad se presenta por la falta de medidas de prevención o auditorias de seguridad que revele algún tipo de deficiencia en el espacio geográfico en el que se encuentre ubicada la red informática.

Software: Tiene vulnerabilidades conocidas como bugs que hace referencia a un error o defecto en el software provocando que deje de funcionar correctamente. Esta vulnerabilidad es ocupada frecuentemente por intrusos informáticos para lograr acceder al sistema.

Las vulnerabilidades son aprovechadas por intrusos para causar daños físicos y lógicos a un sistema informático, para disminuirlas es necesario realizar la detección de estás, mediante pruebas de infiltración, para mejorar la seguridad y confidencialidad de la información.

3.9.2 Pruebas de Infiltración para el escaneo de vulnerabilidades

Existen algunas pruebas de infiltración que se realizan por *pentesters* o analistas de seguridad que son los encargados de detectar vulnerabilidades [22].

Test de Caja Negra: Este tipo de pruebas se realiza ignorando el funcionamiento interno de un sistema, es decir, el código fuente, se centra en realizar pruebas sobre la interfaz gráfica del software, trata de obtener un conjunto diferente de salidas dependiendo de las entradas que realiza.

Test de Caja Blanca: Se centra en el funcionamiento interno para verificar que líneas de código en específico funcionan tal como fueron diseñadas

Test de Caja Gris: En este tipo de pruebas los analistas de seguridad tienen conocimientos sobre algunos aspectos del funcionamiento de sistema y de otros no, mediante esta prueba se busca encontrar vulnerabilidades que permitan a un intruso acceder o infiltrarse en la red informática.

3.9.3 Herramientas para el escaneo de vulnerabilidades

Al realizar pruebas de infiltración usualmente se hace uso de diferentes herramientas para el escaneo de vulnerabilidades informáticas, como se muestra en la Tabla 3.1 [23,24].

Tabla 3.1.- Herramientas para el escaneo de vulnerabilidades.

Herramienta	Definición
Nessus	Es un herramienta que detecta las vulnerabilidades que se puedan presentar por fallas de seguridad además de detectar vulnerabilidades también sugiere como minimizarlas o eliminarlas. Puede generar informes de los escaneos que se han realizado.
Nmap	Es un escáner para auditorías de seguridad en red que escanea los servicios TCP, UDP, ICMP, RPC, así como el sistema operativo de la máquina remota.

OpenVAS	Es una herramienta que ofrece una solución completa y potente de escaneo de vulnerabilidades y gestión de vulnerabilidades.
SAINT Network Vulnerability Scanner:	Es un escáner de vulnerabilidades de red que realiza pruebas de infiltración permitiendo explotar las vulnerabilidades encontradas en un sistema informático.
Acunetix Web Vulnerability Scanner:	Realiza el escáner de seguridad Web, además de analizar y generar informes, incluye una base de datos para gestionar todas las plataformas principales del servidor web.
GFI LANguard Network Security scanner:	Es una herramienta que sirve para realizar la exploración de vulnerabilidades de red y también sirve para realizar auditorías informáticas de seguridad.
MCAfee Vulnerability Manager:	Realiza una monitorización activa y pasiva, que permiten conocer los puntos en los que se debe centrar los esfuerzos de programación.
Nexpose Vulnerability Manager:	Realiza pruebas de vulnerabilidades, además de dar una respuesta de como disminuir o eliminar las vulnerabilidades que se encuentren.
QualysGuard Web Application Scanning WAS	Es una herramienta en la nube que permite realizar pruebas funcionales y de infiltración para aplicaciones web.
WebSite Security Audit- WSSA	Permite examinar páginas web, aplicaciones y servidores web mediante la realización de pruebas de vulnerabilidades de código.
Retina Web Security Scanner	Realiza el escaneo de sitios web, aplicaciones web complejas para hacer frente a las vulnerabilidades de aplicaciones.
Fortify Static Code Analyzer:	Proporciona análisis de código estático automatizado para ayudar a los desarrolladores a eliminar las vulnerabilidades que presentan y poder crear software de seguridad.

Las herramientas de detección de vulnerabilidades realizan principalmente diferentes tipos de escaneos:

- **Escaneo de red:** Es de uso general, usualmente utilizada para detectar vulnerabilidades en la red.
- **Escaneo de puertos:** Realiza la identificación de puertos abiertos o de gran vulnerabilidad que pueden ser utilizados para que un intruso entre a la red.
- **Escaneo de seguridad de aplicaciones web:** Analiza los principales riesgos en las aplicaciones web para poder corregirlos y evitar ataques.
- **Escaneo de base de datos:** Encuentra vulnerabilidades en las bases de datos.

Realizar pruebas de infiltración mediante el uso de herramientas de escaneo es necesario para obtener información relevante acerca de los puntos vulnerables que podrían ser ocupados por diferentes intrusos que pretendan realizar algún tipo de ataque informático, por lo tanto dicha información ayuda a conocer las vulnerabilidades del sistema después con el uso de métodos de protección y prevención mejorar el nivel de seguridad en la red.

3.10 Definición de Ataques informáticos

En la actualidad los dispositivos electrónicos (smartphones, tablets, laptops, desktops) están conectados a través de Internet, motivo por el cual los equipos de los usuarios son propensos a sufrir ataques informáticos en cualquier tipo de red.

Un ataque informático es aquel que trata de aprovechar alguna falla o debilidad en el hardware o software, con el objetivo de causar algún tipo de daño o problemas específicamente a un sistema informático o red.

3.10.1 Clasificación de los tipos de Ataques Informáticos

Los ataques informáticos se pueden clasificar en dos categorías como [25]:

Ataques físicos: Se caracteriza por que la red puede sufrir algún tipo de daño causado por el entorno en el que se encuentre ubicada u ocasionada por el hombre. En esta categoría se puede encontrar con la amenaza de sufrir desastres naturales, que son eventos que ocasionan la pérdida de bienes, servicios, información, y alteraciones en el ambiente en el que suceden, por ejemplo:

- **Incendio:** Pueden ser ocasionados por la falla de instalaciones eléctricas defectuosas, uso inadecuado de materiales inflamables, por la falta de revisión y mantenimiento a las instalaciones. Algunas de las recomendaciones para minimizar el riesgo de un incendio en una red son:
    - El área en la que se encuentren las computadoras debe evitar tener combustibles o inflamables.
    - Contar con mecanismos de ventilación y detección de incendios.
    - Revisar que la topología de la red no sobrecargue los enchufes con demasiadas clavijas, distribuir las cargas equitativamente.
    - Tener un reglamento de seguridad que prohíba ingerir alimentos, bebidas y fumar dentro de la instalación.
    - Antes de realizar alguna reparación de la instalación eléctrica, desconectar el interruptor general y compruebe la ausencia de energía, para evitar algún incidente.
- **Inundación:** Puede ser ocasionada por la falta de drenajes naturales o artificiales provocando la invasión de agua por excesos de escurrimiento superficial en la instalación.
- **Terremotos:** Son ocasionados por fenómenos sísmicos, en ocasiones son producidos a gran escala provocando la pérdida de vidas humanas, aparatos e información, pero la mayoría de las veces son producidos a una escala menor que solo es detectada por instrumentos muy sensibles.
- **Disturbios o sabotaje:** Son ocasionados por personas que hacen uso de las computadoras, con el objetivo de causar algún daño en la red, para evitar la pérdida de información ocasionada por el sabotaje se recomienda el constante respaldo de la información en el sistema.

Ataques lógicos: Se caracteriza por que la red puede sufrir algún tipo de daño en el software o en la pérdida de información. En esta categoría se pueden clasificar en dos:

- **Ataques pasivos:** Caracterizada por obtener información mediante la monitorización de la red sin modificar la comunicación. Su principal objetivo es el análisis del tráfico

para conocer todo lo que pasa por la red y la intercepción de datos para tener conocimiento de la información que se tiene guardada, que envía o recibe el usuario.

  - **Intercepción:** Proceso en el cual un intruso (persona, organización o software) capta la información que un emisor envía a un receptor, por lo tanto el intruso puede obtener información privada (contraseñas, claves bancarias) que suelen ser ocupados para otros fines. La intercepción es un ataque pasivo por lo que es difícil reconocer si algún usuario está siendo atacado al no producirse ninguna alteración en el sistema. Un método de prevención es el cifrado de la información que se envía a través de la red. Este ataque es contra la confidencialidad del usuario o red.

- **Ataques activos:** Se caracteriza por que existe una modificación en el flujo de datos que se transmite [26].
  - **Interrupción:** Proceso en el cual un intruso destruye algún recurso del sistema o no permite que el usuario acceda a los recursos de la red (software, hardware), además de poder inhabilitar el acceso a la información, es decir que no se permite operar de forma normal el sistema. Este ataque es contra la disponibilidad de la información o red.
  - **Modificación**: Proceso en el cual un intruso no solo ingresa sin autorización, sino que también puede realizar una alteración en la información que se envía o recibe a través de la red o realiza cambios en algún software provocando que funcione de forma diferente. Este ataque es contra la integridad del usuario o red.
  - **Suplantación de identidad:** Proceso en el cual un intruso trata de hacerse pasar por una identidad diferente, provocando diferentes daños por que el intruso puede acceder a los recursos privilegiados de la red con la identidad que fue robada. Este ataque es contra la autenticidad del usuario o red.

En la Tabla 3.2 se muestra los tipos de ataques informáticos más comunes que pueden vulnerar cualquier tipo de red, causando daños en el hardware, software o en la información que es almacenada en la computadora [25, 8].

Tabla 3.2.- Tipos de ataques informáticos

Ataque	**Tipo**	**Definición**
Interceptación	***Scanning***	Es un método que se basa en la búsqueda de canales de comunicación susceptibles de ser explotados para la interceptación de información que sea de utilidad para el intruso.
	Sniffing	Método que se basa en el robo de información sin realizar ninguna modificación sobre la misma haciendo uso de Sniffers, que son analizadores de paquetes que monitorizan toda la información que pasa a través de una red.
	Snooping– Downloading	Además de realizar la intercepción de tráfico de red, ingresa a la información o software guardado en la red, realiza la copia de los datos y de este modo los analiza para después realizar actos ilícitos con la información.
Interrupción	***DoS* (Denegación de Servicios)**	Método que se basa en dejar inaccesible algún servicio o recurso de una red durante un período indefinido de tiempo. Se realiza provocando la pérdida de conexión de la red por la saturación generada a partir de un aumento del tráfico.
	***DDoS* (Denegación de Servicios Distribuida)**	Este tipo de ataque se realiza a un conjunto de ordenadores infectados llamados bots o zombies que son controlados de forma remota.
	Man in the middle	En este tipo de ataque un intruso intercepta la comunicación entre dos partes sin que estas sean conscientes de su presencia. Por lo tanto el intruso es

		capaz de leer, modificar, insertar o eliminar mensajes entre ellos.
	Tampering o Data Diddling	Se realiza una alteración desautorizada de los datos o el software instalado, pueden llegar a borrar cualquier información que puede generar incluso la baja total del sistema o red.
	Pharming	Este tipo de ataque se basa en la falsificación del DNS (Sistema de nombres de Dominio) para así redirigir a la víctima a una página web falsa (idéntica a la original), con la finalidad de obtener información del usuario y generar alguna actividad ilícita.
Suplantación de identidad	***Spoofing-Looping***	Este tipo de ataque se basa en actuar en nombre de otros usuarios, es decir suplantar la identidad de terceros, usualmente para realizar tareas de Snooping o Tampering Tipos de Spoofing: • IP Splicing–Hijacking: Suplanta la identidad de un usuario mediante la interceptación de una sesión establecida. • Web Spoofing: El intruso crea un sitio web falso para obtener la información que desea de un usuario.
	Obtención de Contraseñas	Este tipo de ataque ocupa la "fuerza bruta" para obtener las contraseñas que le permitan ingresar a los sitios, sistemas, cuentas, aplicaciones, que el intruso desee.
	BackDoors	Permite al intruso saltarse los métodos habituales de autentificación por medio de las puertas traseras de algún software.

Cualquier tipo de red es vulnerable a sufrir ataques informáticos cuando la seguridad informática no está en constante actualización y mantenimiento. Es necesario mantener seguros o actualizar los dispositivos de conectividad que se emplean, usualmente son ocupados como medio de intrusión que podrían provocar daños a nivel software o hardware en la red.

3.10.2 Modo de operación de los ataques informáticos

Los ataque informáticos tienen un modo de operación cuya finalidad es causar algún daño en la red informática, como se muestra en la Figura 3.6 [25,27].

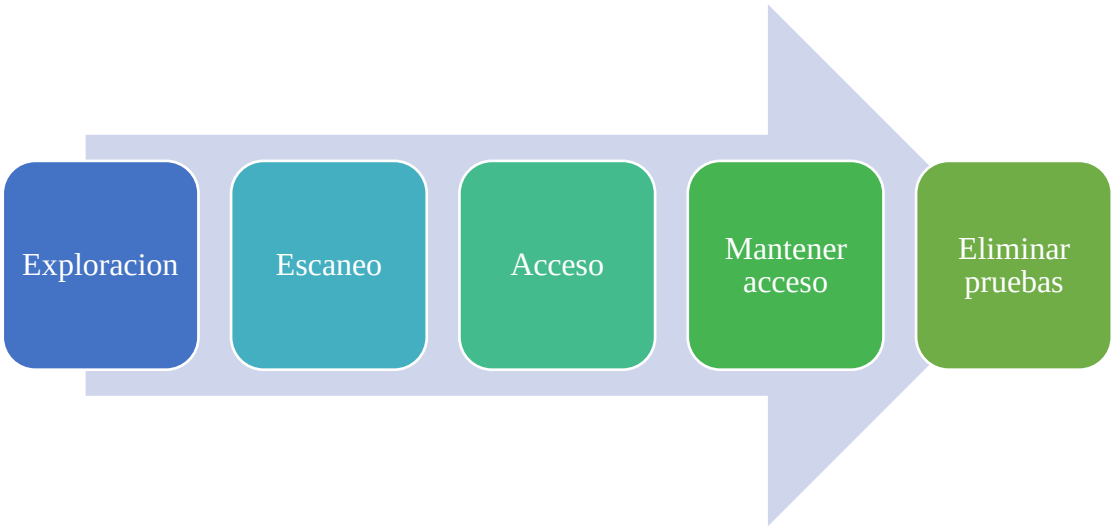


Figura 3.6.- Modo de operación de los ataques informáticos [25].

Exploración: Realiza el análisis de la red o sistema informático para poder ingresar de manera no autorizada.

Escaneo: Realiza la búsqueda de las vulnerabilidades de la red que pueden ser utilizadas para acceder a la red informática

Acceso: Ingresa de forma ilícita a la red informática mediante el aprovechamiento de las vulnerabilidades que fueron encontradas en el escaneo de la red.

Mantener el acceso: Para realizar daños en el software, hardware en el sistema o red informática, además de realizar la recopilación de información confidencial de algún usuario o de la organización.

Eliminar pruebas: Realiza la eliminación de datos, huellas o información que pueda evidenciar que existió algún tipo de ataque informático.

El modo de operación de los ataques informáticos permite que los intrusos que las generan puedan ocultar su identidad al eliminar las pruebas del ataque realizado, después de haber obtenido información confidencial o haber ocasionado daños al hardware de la red.

3.11 Definición de amenazas

Para que un intruso realice ataques informáticos hace uso de las diferentes amenazas, que se puede definir como cualquier elemento, circunstancia o acción que tiene potencial de causar algún daño en el sistema o red informática [25].

3.11.1 Clasificación de las amenazas

Algunas de las amenazas que pueden ocasionar daños en cualquier tipo de red informática se muestran en la siguiente Tabla 3.3 [28,29].

Tabla 3.3.- Tipos de amenazas informáticas.

Amenazas	Definición
Virus/ Código Malicioso	Es todo programa o fragmento del mismo que genera algún tipo de problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con el normal funcionamiento del mismo.
Adware (Advertising Malware)	Son programas que ejecutan pantallas emergentes para mostrar publicidad además de redirigir solicitudes de búsqueda a sitios web de publicidad y realiza la recopilación datos de una computadora (sitios a los que el usuario accede) para poder crear propaganda personalizada basada en los gustos del usuario.
Backdoor (Puerta trasera)	Son utilizados para evitar la autentificación al intentar acceder a algún sistema.

Bombas Lógicas	Es un código insertado intencionalmente en un software, que permanece oculto hasta que se cumplen con los requisitos necesarios para realizar su ejecución y causar algún daño al sistema.
Dialer	Son programas cuyo objetivo es tratar de establecer conexión telefónica con un número de tarificación especial sin realizar ningún previo aviso al usuario.
Exploits	Son programas creados para tratar de aprovechar las vulnerabilidades que se encuentren en una red y software para realizar algún ataque informático.
Gusanos	Son programas que se auto duplican y que se alojan en diferentes ubicaciones en la computadora, causando diferentes daños en el sistema o red informática.
Hijackers	Son programas que modifican la configuración del explorador y complementos además de ser capaces de instalar spyware
Hoax	Son mensajes cuyo objetivo es engañar y molestar al usuario por que contienen falsas alarmas de virus o de cualquier otro tipo de alerta. Ocupan la suplantación de identidad para poder manipular información que obtienen del usuario.
Ingeniería Social	Tratan de obtener información confidencial mediante la manipulación de las personas convenciéndolas de ejecutar acciones que revele todo lo necesario para superar las barreras de seguridad.
Ingeniería Social Inversa	Trata de obtener información cuando el usuario cae en alguna trampa que el intruso género para obtener la información confidencial que necesitaba.
Joke	Es un programa que simula que la computadora está siendo atacada por un virus informático, su objetivo es crear algún efecto molesto.

Keyloggers	Es un programa cuyo objetivo es registrar todas las teclas que un usuario presiona en su computadora; de este modo puede obtener información confidencial y que sean de utilidad para el atacante.
Phishing	El intruso hace uso de la suplantación de identidad para obtener información confidencial y poder generar fraudes informáticos.
Ransomware	El objetivo de esta amenaza es restringir el acceso al sistema operativo y exige el pago de un rescate para eliminar la restricción, para que el usuario pueda acceder a su información nuevamente.
Rootkit	Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos para poder acceder ilícitamente a un sistema informático. Sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema.
Spyware	Son aplicaciones cuyo objetivo es recolectar información del equipo y usuario para luego enviarlas sin permiso del propietario a un intruso que realiza actos ilícitos con la información que obtuvo.
Stealers	Son programas que se introducen a través de internet con el objetivo de obtener las contraseñas de un usuario y enviarlas a una computadora remota para que un intruso realice actividades ilícitas con fines de lucro.
Trashing	Es la recolección información confidencial a través de material desechado con la finalidad de obtener datos que sirvan como información para cometer fraudes.
Troyano	Son programas no auto replicable cuyo objetivo es realizar acciones de eliminación, bloqueo, modificación, copia de datos no autorizadas por el usuario. Existen diferentes tipos de troyanos:

	• *Trojan-Banker* (Troyano Bancario): Diseñados para robar datos bancarios de sistemas de banca online, sistemas de pago electrónico y tarjetas de débito o crédito. • *Trojan-DDoS:* Diseñados para realizar ataques DoS contra una dirección web específica. • *Trojan-Downloader:* Son programas de descarga de troyanos, su objetivo es descargar e instalar nuevas versiones de programas maliciosos en el ordenador, incluidos troyanos. • *Trojan-Dropper:* Son programas que se utilizan para instalar troyanos y virus. • *Trojan-FakeAV:* Es un programa que simula la actividad de software antivirus. Su objetivo es extorsionar al usuario a cambio de la detección y eliminación de amenazas, aunque estas no existan realmente. • *Trojan-GameThief:* El objetivo de este programa es robar los datos de la cuenta de usuario de los jugadores online. • *Trojan-Ransom:* Su objetivo es modificar los datos de la computadora para evitar que funcione correctamente y que el usuario no pueda acceder a datos específicos. • *Trojan-Spy:* Son programas cuyo objetivo es espiar las actividades que se realizan en la computadora y de este modo obtener información confidencial. • *Trojan-Mailfinder:* Son programas cuyo objetivo es recopilar las direcciones de correo electrónico de la computadora.

Las amenazas informáticas están en aumento, ocupando diferentes medios para ocasionar daños en la red. Según el informe de seguridad 2016 de Cisco [30], las extensiones maliciosas de navegador pueden ser una fuente importante de filtración de datos de las empresas y son un problema muy extendido. Se calcula que más del 85% de las organizaciones analizadas sufre el problema de las extensiones maliciosas de navegador.

3.11.2 Historia de las Amenazas informáticas

Es importante conocer cuál ha sido la evolución de las amenazas informáticas a través de la historia, con el avance de la tecnología se incrementan continuamente las amenazas que siempre están en constante búsqueda de vulnerabilidades informáticas que se pueden encontrar en los diferentes tipos de redes.

Las principales amenazas informáticas que han ocurrido a través del tiempo se describen a continuación [31]:

- 1939, el científico matemático John Louis Von Neumann, escribió "Teoría y organización de autómatas complejos", donde se mostraba que era posible desarrollar programas que tomasen el control de otros.
- 1949 – 1950s, Core War fue un juego mediante el cual se propagó uno de los primeros software con características maliciosas que afectaba la memoria de las computadoras y podía auto replicarse, fue una sencilla aplicación que competía con el resto de los programas que se ejecutaban en una computadora con el fin de obtener el control absoluto de la memoria del equipo.
- 1971, Creeper fue creado por Bob Thomas fue especialmente escrito para atacar al sistema operativo Tenex. Cuando Creeper llegaba a una computadora, por lo general por intermedio de los nodos de la ARPANET, el malware se auto ejecutaba y mostraba el siguiente mensaje: "Soy la enredadera, atrápame si puedes"
- 1982, Elk Cloner fue el primer virus informático conocido que tuvo una expansión real y no como un concepto de laboratorio. Rich Skrenta, un estudiante de instituto de 15 años, lo programó para los Apple II en 1982. se propagaba infectando los disquetes del sistema operativo de los computadores Apple II.
- 1985, Los primeros troyanos se presentaban disfrazados, por que el virus se escondía bajo una imagen de programa de mejora de gráficos llamado EGABTR, y por la imagen del famoso juego llamado NUKE-LA, para de este modo acceder al sistema e infectarlo.
- 1987, Virus Brain fue el primer virus que provocó mayores infecciones en la época, el cual comenzó a circular en el año 1986, y para 1987 había logrado extenderse por todo el mundo.

- 1988**,** Gusano Morris, considerado el primer gusano, durante las primeras horas de su aparición afectó aproximadamente el 10% de todas las máquinas conectadas a Internet. Su creador Robert Tappan Morris fue la primera persona condenada por la justicia bajo el delito de fraude y abuso informático.
- 1989, el virus Dark Avenger también conocido como "vengador de la oscuridad", se propagó por Europa y Estados Unidos.
- 1990, Mark Washburn crea "1260", el primer virus polimórfico, que mutaba en cada infección.
- 1992, aparece el conocido virus Michelangelo sobre el cual se crea una gran alarma sobre sus daños y amplia propagación, aunque finalmente fueron pocos los ordenadores infectados.
- 1994, Good Times, fue el primer virus broma.
- 1995, aparece Concept con el cual comienzan los virus de macro. Y ese mismo año aparece el primer virus escrito específicamente para Windows 95.
- 1999, el virus "Melissa" utilizaba la técnicas de ingeniería social, llegaba con el mensaje "Aquí está el documento que me pediste… no se lo enseñes a nadie". Causó una de las infecciones masiva más importante de la historia, causando daños de más de 80 millones de dólares a empresas norteamericanas.
- 200, virus "I love you" se autocopiaba y escondía en diversos ficheros, añadía registros, remplazaba archivos, se auto enviaba vía correo y copiaba contraseñas a través de una aplicación auto instalable
- 2001, Sircam es un virus informático de correo electrónico que tiene la capacidad de enviarse a todos los contactos de la libreta de direcciones de Microsoft Outlook, por lo que su propagación se produce rápidamente. Su objetivo es obtener datos privados, y agotar el espacio libre del disco duro.
- 2002, el virus Bugrear podía desactivar los programas de seguridad de la computadora, además de abrir una puerta trasera en el equipo infectado.
- 2003, SQL Slammerizafird aprovecho una falla en la base de datos del servidor SQL de Microsoft, saturando archivos en todo el mundo

- 2004, MyDoom el virus creaba una puerta trasera para acceder al sistema operativo, buscaba distribuirse a través de las cuentas de correo, una vez infiltrado no se tiene arreglo.
- 2006, Zhelatin, Nuwar o Peacomm era capaz de convertir el computador en un "zombie", vulnerable al control remoto de parte del que envía el ataque.
- 2012, el virus DNSChanger modifica la configuración de la conexión a Internet para que toda petición de carga se dirija hacia servidores de nombres falsos.
- 2017, el virus WannaCry en su primera aparición afecto a 120,000 equipos en más de 150 países.

Este tipo de amenazas informáticas seguirán surgiendo, utilizando nuevos medios y métodos de ataque, de igual forma en la que el número de intrusos informáticos aumentara, por lo tanto es necesario seguir empleando métodos de prevención y protección que permitan mantener segura la información, el software y hardware de la red informática.

3.12 Clasificación de los intrusos en las redes

Un intruso se define como una persona que intenta entrar a la red de una organización o de otra persona sin ninguna autorización, cuya finalidad es causar algún daño al software, hardware o recopilar información confidencial.

Existen diferentes tipos de intrusos que pueden ocupar las vulnerabilidades de la red para causar algún tipo de daño con fines específicos en la red informática, como se muestra en la Tabla 3.4 [4.5].

Tabla 3.4.- Tipos de Intrusos informáticos.

Intruso	Definición
Cracker	Persona que accede a un sistema o red informática sin autorización con fines personales, cuyo principal objetivo es causar algún daño en el sistema informático y obtener información confidencial para realizar actos ilícitos con fines de lucro.
Ciberterrorista	Es un cracker que puede efectuar cualquier ataque informático con la finalidad de satisfacer intereses políticos y económicos

Creadores de virus y programas dañinos	Son personas que utilizando sus conocimientos en tecnologías de información y telecomunicaciones que desarrollan programas dañinos y virus, la distribución se realiza a través del Internet para que estos se propaguen y pueden causar diferentes daños en las redes
Hacker	Persona experta en tecnologías de información y telecomunicaciones que accede a un sistema o red informática sin autorización, su objetivo es buscar fallas que puedan ser solucionadas por él, para poner a prueba sus conocimientos o avisarle al fabricante de los errores y riesgos con los que cuenta el sistema. Aunque no tratan de hacer ningún daño al sistema, el hacker tiene acceso a información confidencial y en muchas ocasiones crea puertas traseras que otros tipos de intrusos pueden ocupar.
Intrusos remunerados	Personas que acceden a un sistema por órdenes de terceros para obtener información confidencial o causar algún daño en el sistema.
Lamers	También conocidos como "Scriptkiddies"o "Click-kiddies", son personas sin un amplio conocimiento en las tecnologías de información, que adquieren diferentes herramientas o programas para realizar diferentes ataques a un sistema informático, para observar los resultados y daños causados.
Phreakers	Son personas que se dedican a realizar sabotajes en redes telefónicas y de este modo poder realizar llamadas gratuitas.
Personal interno y ex-empleados	Este tipo de personas en ocasiones por falta de conocimiento pueden provocar incidentes en la red o sin intención crean algún tipo de vulnerabilidad que es aprovechada por los intrusos externos. En caso de los ex-empleados al tener conocimiento del tipo de seguridad con la que cuenta la organización, pueden actuar en su contra, al obtener, eliminar o modificar información confidencial.
Piratas informáticos	Se dedican a robar programas, aplicaciones o contenidos digitales para realizar actividades con fines de lucro, además de infringir la legislación sobre la propiedad intelectual.

Script kiddie	Son personas que están en aprendiendo a convertirse en cracker o hacker, por lo cual realizan diferentes ataques sin conocer muy bien lo que están haciendo o el resultado que obtendrán.
Sniffers	Su objetivo es buscar y recopilar mensajes que circulan por Internet, para obtener información confidencial y ocuparlas con fines de lucro.
Spammers	Se encargan del envío masivo de mensajes de correo electrónico sin autorización y sin ser solicitados a través del internet, esto ocasiona el colapso de los servidores y la sobrecarga de los buzones de entrada de los correos electrónicos de los usuarios.

3.13 Triangulo de la Intrusión en la red.

Los intrusos informáticos para realizar cualquier tipo de ataque informático deben de tener en cuenta tres aspectos [27]:

Oportunidad: Ocupan las fallas y vulnerabilidades en la seguridad de cualquier tipo de red informática.

Medio: Deben de tener los conocimientos o herramientas necesarias para poder realizar un ataque informático.

Motivo: Son los objetivos personales del intruso para realizar el ataque informáticos. Algunos de los motivos más comunes de los intrusos son:

- *Financieros:* Realizan ataques para poder obtener información confidencial para posteriormente venderlas y obtener una remuneración monetaria
- *Diversión:* Realizan diferentes tipos de ataques en las redes informáticas solo para pasar el rato
- *Ideología:* Realizan ataques a organizaciones especificas porque van en contra de sus ideas personales.
- *Búsqueda de reconocimiento:* Destacar entre un grupo de personas que se dediquen a realizar las mismas actividades ilícitas

En conjunto estos tres aspectos como se muestra en la Figura 3.7, componen el triángulo de la intrusión en la red informática.

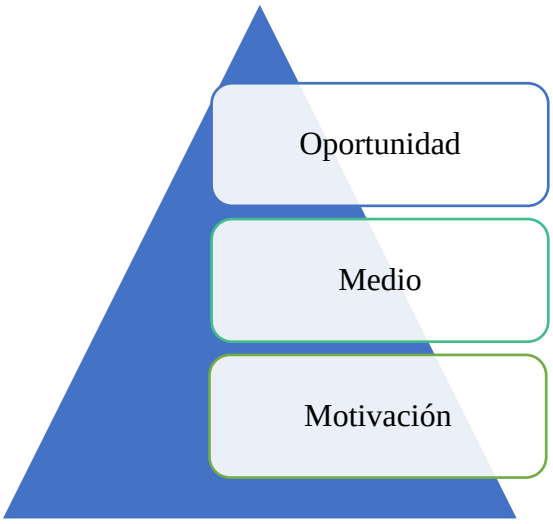


Figura 3.7.-Triángulo de la intrusión [27].

Los intrusos informáticos al cumplir con estos tres aspectos, realizan diferentes ataques que dañan el sistema informático y provocan la perdida de información, de acuerdo al informe de Kaspersky Lab en el primer trimestre del 2017, neutralizaron 479 528 279 ataques lanzados desde recursos de Internet ubicados en 190 países del mundo. Se neutralizaron intentos de ejecución de programas maliciosos que roban dinero mediante el acceso a cuentas bancarias en los equipos de 288 000 usuarios [32]. Por otro lado los ataques informáticos siguen aumentado en los dispositivos móviles, por la poca seguridad de las contraseñas que se utilizan en las diversas cuentan que los usuarios tienen y los sitios web a los que acceden. Además el incremento de intrusos en la red pone en riesgo la seguridad de la información. Por este motivo es necesario realizar la protección de los dispositivos que se encuentran en la red mediante métodos de prevención.

4 METODOS DE PREVENCIÓN DE ATAQUES INFORMÁTICOS

Con las constantes amenazas que existen en cualquier red informática, es necesario hacer uso de las diversas medidas de prevención y herramientas de defensa para mantener segura la información, el software o hardware de la red. Hasta el momento no existe ninguna aplicación o herramienta que brinde el 100% de protección, debido a las diversas amenazas potenciales a las que se expone diariamente la red. Algunos de los métodos de prevención se describen a continuación [4, 5, 10]:

Actualización del Sistema Operativo

Es una medida preventiva para mejorar la seguridad, por lo tanto, es necesario realizar una constante actualización del Sistema Operativo, porque en cada actualización se proporcionan muchas revisiones para el equipo, además de agregar nuevas funciones, eliminan funciones desactualizadas, se actualizan controladores, en ocasiones se corrigen problemas con el calentamiento del equipo o los mecanismos de interacción con las memorias, se proporcionan correcciones de errores de programación o se realiza el soporte a nuevas tecnologías y principalmente reparan vulnerabilidades que fueron detectadas para evitar que un intruso pueda producir ataques informáticos.

Cualquier tipo de actualización debe de instalarse lo antes posible, de modo que se disminuye el tiempo en el que los intrusos puedan ocasionar algún daño, para realizar la actualización solo es necesario estar conectado a Internet.

Sin importa el sistema operativo con el que se cuente es necesario realizar actualizaciones, que pueden ser programados para que se realicen durante periodos de inactividad o en el momento que el usuario o administrador de la red crea conveniente.

Actualización del software y el navegador

El objetivo de cualquier tipo de actualización es mejorar la seguridad a medida en que se van descubriendo vulnerabilidades, además de mejorar la funcionalidad. Las amenazas informáticas suelen aprovechar los agujeros que existen en el software y navegador para infectar al dispositivo, los fabricantes al detectar dicha vulnerabilidad corrigen el

programa a través de actualizaciones. Es recomendable activar las actualizaciones automáticas del software que se encuentre instalado en la computadora, además del navegador y sus complementos (*plugins*).

Copias de seguridad

La mayoría de los malwares realizan acciones destructivas, dirigidas a ocasionar un mal funcionamiento del sistema operativo, además de causar daño o eliminación de archivos críticos del sistema. El realizar copias de seguridad de la información que se encuentre en la computadora es un método de prevención para tener un respaldo en caso de ser víctimas de cualquier tipo de ataque informático. Es recomendable realizar copias de seguridad periódicamente para mantener actualizada la información que respaldada.

Es importante seleccionar información que sea de vital importancia para la realización de la copia de seguridad, si se copian demasiados archivos se puede agotar rápidamente la capacidad de almacenamiento disponible, se pueden realizar copias de seguridad de la información a fuentes externas como CD, DVD, discos duros, memorias USB o en servicios de almacenamiento en la nube, de esta manera, ante una pérdida o robo de la información ya sea por daños de los archivos o por acción de amenazas informáticas, será mucho más sencillo y rápido recuperar la información, por lo cual se ha demostrado que las copias de seguridad son un elemento fundamental en materia de seguridad.

Utilizar contraseñas seguras

El uso de contraseñas genera una barrera que se interpone entre la información confidencial con la que cuenta el usuario y los intrusos informáticos, el robo de contraseñas es el método más extendido para acceder a la información que esta almacenada en el equipo y/o servicios en línea [30], por ejemplo, datos bancarios, personales, o que tengan acceso a datos corporativos.

Crear contraseñas seguras es otro método de prevención a la perdida de información, para crearlas de modo seguro se deben de tener en cuenta las siguientes características:

- No debe de tener menos de ocho dígitos.

- Se debe crear con la mezcla de letras en mayúsculas, minúsculas, con números y caracteres especiales.
- No debe contener el nombre de usuario o información personal.
- Evitar el uso de palabras demasiado obvias o simples.
- Es recomendable hacer el cambio periódicamente la contraseña.
- No se debe de utilizar la misma contraseña para diferentes servicios o cuentas.
- No se debe compartir la contraseña con nadie.

Al introducir la contraseña es importante que la página sea correcta, en muchas ocasiones la página accedida puede parecer idéntica a la legítima y sin embargo se estaría tratando de una suplantación (phishing).

Firewall

Monitorea el tráfico entrante-saliente de la red, para permitir o bloquear algún tipo de tráfico específico en base a un conjunto definido de reglas de seguridad establecido. Es decir que establece una barrera entre la red interna protegida y la red externa que no son de confianza.

Un firewall puede ser hardware, software o ambos, y su principal objetivo es proteger al equipo de accesos de intrusos que puedan obtener información confidencial del usuario e incluso denegar servicios de la red.

El tipo de reglas y funcionalidades que se pueden construir en un firewall son las siguientes:

- Administrar el acceso a los servicios privados de la red.
- Registrar todos los intentos de entrada y salida de la red.
- Realizar un filtro de direcciones, es decir, realizar un filtro de paquetes en función de su origen, destino y número de puerto.
- Realizar un filtrado de protocolo, se realiza un filtro de determinados tipos de tráfico en la red en función del protocolo utilizado.

- Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso que superen un determinado límite. De este modo es posible evitar algunos ataques de denegación de servicio.
- Controlar las aplicaciones que pueden acceder a Internet.
- Crear una regla que detecte los puertos que están siendo ocupados para el monitoreo de la red.

El firewall ayuda a manejar una variedad de aspectos en el punto de acceso a la red pública manteniendo a los intrusos fuera, mientras que la red interna ofrecer normalmente sus servicios y otros ofrecidos por Internet, además de controlar el acceso de usuarios eternos a los recursos de la red interna..

Antivirus

Es un programa que es instalado en una computadora o un dispositivo móvil como herramienta de protección ante diferentes tipos de amenazas informáticas. La función del antivirus es detectar cualquier tipo de malware, impidiendo su ejecución además de tomar diferentes medidas de prevención como eliminar el archivo que este infectado, o ponerlo en cuarentena para evitar daños al sistema y a la información. Realiza la detección de malware de dos formas:

- **Detección por firma:** Cada malware tiene en específico un código de firma que lo identifica que está almacenado en un diccionario de malware conocido, cuando el antivirus realiza un análisis del equipo en busca de las características de las firmas existentes y si existe algo que coincida con el patrón del diccionario el programa intenta neutralizarlo.
- **Detección por comportamiento:** Se encarga de monitorear el comportamiento del software que se encuentra instalado en la computadora, verificando que no se comporte sospechosamente, por ejemplo: que esté tratando de acceder a información privilegiada o modificar archivos u otros programas, si el antivirus detecta que se está comportando sospechosamente le advierte al usuario para que él pueda tomar alguna decisión acerca del software que está generando problemas.

Aunque existen diferentes tipos de antivirus, y cada uno tiene su propio método de actuar cuando se localiza un virus, y puede variar en función de si el antivirus detecta el virus durante un escaneo automático o una búsqueda manual.

Es necesario actualizar periódicamente el antivirus, de ese modo se actualiza el diccionario de malware conocido, ya que el antivirus solo protege al sistema de lo que reconoce como dañino.

Software Anti-spam

Es un software que es instalado en la computadora con la finalidad de prevenir el spam (correo basura) permitiendo bloquear y eliminar todos los correos no solicitados en la bandeja de entrada del correo electrónico.

Existen diferentes tipos de software anti-spam que tienen diversas maneras de configuración, administración y automatización en la detección de correo basura. Una ventaja de usar este tipo de softwares es que la lectura de correos electrónicos es más rápida y seguro porque no se pierde tiempo verificando, eliminando o reenviando a cuarentena los correos no solicitados. Se debe de realizar una actualización continua para que las firmas de spam se mantengan actualizadas.

Software Anti-spyware

Este tipo de software permite prevenir que el software intruso a la red puedan monitorear y recolectar la información de la actividad que el usuario realice en internet para después enviarla a una entidad externa, que a su vez empezara a generar de manera automática la reproducción de páginas publicitarias para realizar una propaganda de productos y servicios.

El software anti-spyware también impide que los diferentes tipos de spyware existentes disminuyan el rendimiento de la computadora provocando la lentitud de los programas que se estén ejecutando.

El riesgo de ser atacados por algún tipo de spyware es alto, cualquier tipo de usuario que haga uso del internet puede ser propenso a este tipo de amenaza, por lo que es recomendable usar cualquier tipo de software que pueda detectar y eliminar spyware.

Software Anti-adware

Para prevenir que en una computadora se instalen programas de adware cuya finalidad es generar anuncios publicitarios o redirigir las solicitudes de búsquedas a sitios publicitarios que pueden contener virus, por lo general no revela su presencia por lo que es necesarios realizar la instalación de cualquier tipo de software anti-adware de la preferencia del usuario para su detección y eliminación.

Es tipo de amenaza es uno de los más frecuentes, afectan a una gran cantidad de usuarios que al estar navegando en internet, visualizan publicidad indeseada en las páginas web a las que acceden.

Software Anti-phishing

Este tipo de software trata de identificar si existe contenido de phishing en los sitios web y correo electrónico en los que el usuario accede, para ayudar a prevenir que el usuario sea engañado.

La mayoría de los amenazas de phishing son muy difíciles de identificar fácilmente ya que los intrusos que los generan los elaboran con los datos reales de las paginas falsificadas, por este motivo es recomendable ocupar este tipo de software que permite bloquear sitios web conocidos por distribuir este tipo de contenido.

Software Anti-ransomware

Este tipo de software permite prevenir que la computadora sea víctima de ransomware que es un tipo de amenaza que encripta la información que se tiene almacenado en el sistema informático restringiendo el acceso a ella, y para recuperarla pide a cambio un rescate económico.

El software anti-ransomware funciona encriptando la información del equipo para impedir su acceso a cualquier intruso anticipándose al daño que puede causar. Además de crear

una carpeta con contenidos y nombres aleatorios que utiliza como señuelo en una carpeta de usuario, la cual posiciona de manera que si llegase a existir una amenaza, este empezará el secuestro de datos por dicha carpeta. Con la monitorización de su actividad puede detectar cualquier anomalía y enviar rápidamente una alerta al usuario.

Acceder a sitios seguros

Es necesario que al acceder a sitios web, el usuario lo haga de modo seguro para evitar ser víctimas de diferentes amenazas informáticas, el usuario solo debe de acceder a páginas que tienen algún sello o certificado que garanticen su calidad y fiabilidad. Por lo tanto siempre se puede navegar en páginas que cuenten con el protocolo HTTPS activado.

La mayoría de las páginas que son seguras, en la barra del navegador que se esté utilizando, debe aparecer un icono de un candado cerrado. Por medio de este icono se puede acceder a un certificado digital que confirma la autenticidad de la página.

Fomentar una educación de prevención informática

Aunque no exista ningún método que brinde una completa seguridad de la red, es necesario tratar de fomentar una educación de prevención informática, de este modo se harían uso de los diferentes métodos de prevención antes mencionadas con mayor frecuencia, por lo cual, es recomendable que el administrador de la red les proporcione a los usuarios información acerca de los métodos de prevención que existen, orientándolos en las interrogantes que les surjan.

5 NESSUS Y SIMULADORES DE AMENAZAS INFORMÁTICAS

En este trabajo de investigación se realizará un caso de estudio, en el cual se hará uso de herramienta Nessus para el escaneo de vulnerabilidades y el uso de los simuladores de amenazas informáticas que se describen a continuación:

5.1 NESSUS

Es una herramienta de escaneo de vulnerabilidades de red y de diferentes Sistemas Operativos, fue desarrollado por Renaud Deraison en 1998, e incluye su propio lenguaje de programación llamado NASL (Nessus Attack Scripting Language) [33].

En la plataforma de análisis de vulnerabilidades de Nessus los usuarios pueden programar diferentes tipos de escaneos, utilizar asistentes para crear políticas, programar escaneos y enviar resultados por correo electrónico, puede ser utilizado en modo consola o grafico dependiendo del sistema operativo en la que se instaló.

Nessus está diseñado en un modelo clásico de cliente-servidor que cuenta con su propio protocolo de comunicación., el servidor realiza el escaneo y prueba ataques, mientras que las tareas de control, generación de informes y presentación de datos son realizadas por los clientes.

Actualmente existen dos versiones de Nessus; “Home” y “Professional”, la primera es libre, permite escanear la red doméstica personal o redes LAN, con las mismas evaluaciones de alta velocidad, profundidad y comodidad de exploración que los usuarios que adquieren la versión Professional, con la diferencia de que esta última proporciona acceso a soporte técnico, le permite realizar comprobaciones de cumplimiento o auditorías de contenido.

Las características clave de Nessus son [23]:

- Detección de Malware.
- El descubrimiento de activos es realizado a una alta velocidad.

- Realiza una evaluación de vulnerabilidad, dependiendo del nivel de riesgo (critica, alta. mediana y bajo).
- Es capaz de realizar un escaneo y auditoría de plataformas virtualizadas y de la nube.
- Está en continua actualización y mejora a partir de las vulnerabilidades que se van encontrando en las redes escaneadas.
- Basa su arquitectura en un conjunto de plugins para la realización de varias simulaciones de ataques.
- Realiza el escaneo el puertos e identificación de servicios mediante Nmap
- Los resultados del escaneo pueden ser exportados como informes en varios formatos (xml, html, LaTex).

Nessus también ofrece un conjunto de posibilidades de autenticación de usuarios, para garantizar que usuarios no autorizados no utilicen los recursos de la red para realizar exploraciones de puertos o de vulnerabilidades de forma ilegıtima. A través del uso de contraseñas de usuario, o bien mediante el uso de técnicas criptográficas, el cliente Nessus realizara un proceso de autenticación contra el servidor, para garantizar que el usuario que se conecta a dicho servicio es un usuario legıtimo.

La mayoría de las alertas generadas por Nessus después de la exploración de vulnerabilidades en la red son [20]:

- Utilizar servidores no actualizados o mal configuradas y que presentan deficiencias de seguridad.
- Deficiencias de seguridad relacionadas con la implementación del protocolo TCP/IP.
- Instalación de puertas traseras, troyanos, demonios de DDoS u otros servicios extraños.
- Instalación de servicios ilegítimos o sospechosos en los equipos de la red.
- Utilización de aplicaciones CGI (Common Gateway Interface) desde servidores web mal configuradas o mal programadas y que suponen una brecha de seguridad contra el sistema que las alberga.

5.2 Simuladores de amenazas informáticas.

Para elaborar el conjunto de experimentos del caso de estudio se hará uso de los siguientes simuladores de amenazas informáticas [34, 35, 36].

5.2.1 Simulador de virus EICAR

También conocido como el archivo de prueba EICAR, fue desarrollado en 1996 por el Instituto Europeo para la investigación de los Antivirus Informáticos, cuya finalidad es probar la funcionalidad del software antivirus, es decir, que se debe de detectar durante los procesos de escaneo.

Este simulador no implica ningún riesgo para la seguridad de la red en el cual se implementa, es de gran ayuda para verificar si las barreras que el antivirus que se tiene instalado en una computadora sirven para proteger la información, además es útil para verificar si el antivirus está realizando correctamente su trabajo de detección de amenazas informáticas.

El archivo de prueba EICAR consiste en 68 caracteres ASCII, cuya descripción está incluida en las bases de datos antivirus permitiendo al software antivirus identificarla en los objetos de escaneo. Los caracteres son:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Al ejecutar, descomprimir o intentar descargar este simulador el antivirus que se tenga instalado y que este monitoreando el sistema operativo debe de detectarlo generando una advertencia de virus, de la misma forma en la que responderían ante un verdadero virus, aunque el código es totalmente inofensivo, lo reportan como malware con el nombre: "EICAR-AV-Test".

Por otro lado para simular como pueden ser transmitidos los virus informáticos se puede anexar el archivo del simulador en un correo electrónico y verificar así la protección que tiene en la computadora.

En caso de no contar con ningún tipo de protección el simulador de virus EICAR se ejecutara ocasionando la aparición de una ventana DOS con el siguiente mensaje de texto:

EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

Al final se debe de borrar el archivo de EICAR que se generó para evitar que cualquier tipo de antivirus empiece a generar falsas alarmas después de detectarlo.

5.2.2 Simulador RanSim (Ransomware Simulator)

Es un software desarrollado por KnowBe4 que simula amenazas de ransomware que es aquella que toma el control del sistema operativo, encriptando los archivos para después exigir un pago para rescatar la información cifrada. RanSim simula diez tipos de amenazas cuya finalidad es verificar y comprobar que la computadora este protegida ante estos tipos de amenazas o que el sistema de seguridad sea eficiente por lo cual realizar una advertencia acerca del estado de la seguridad en sistema operativo.

El instalar este simulador es seguro, no genera ningún problema en el sistema, en ningún momento actúa como un ransomware verdadero. Analiza el comportamiento de la computadora en los siguientes 10 escenarios [37]:

- **InsideCryptor** – Cifra los datos y sobrescribe los originales.
- **LockyVariant** – Simula una de las incontables variables del ransomware Locky.
- **Mover** – Cifra los datos en una carpeta diferente a la original y elimina los originales.
- **Replacer** – Remplaza el contenido de los archivos originales.
- **Streamer** – Cifra todos los datos y los agrupa en un solo fichero.
- **StrongCryptor** – Cifra los datos y borra los originales de forma segura.
- **StrongCryptorFast** – Cifra los datos y borra los originales.
- **StrongCrytptorNet** – Cifra los datos, borra los originales y simula una conexión HTTP.
- **ThorVariant** – Simula una de las incontables variables del ransomware Thor.
- **WeakCryptor** – Utiliza un cifrado débil para cifrar los datos y elimina los originales.

RanSim crea un listado de archivos que son más vulnerables a través de un gráfico de sectores. También muestra la lista de amenazas que pueden atacar con éxito el sistema y la partición del disco que afectarán a la mayoría.

5.2.3 Trojan Simulator

Es un programa que simula ser un troyano que se está instalando en el equipo, su finalidad es verificar cómo se comporta el software de seguridad que se tiene instalado en el sistema en una situación real.

El simulador de Troyano está disponible en diferentes sistemas de Windows, actualmente una gran cantidad de antivirus ya puede detectar Trojan Simulator. El proceso de instalación es sencilla, al ejecutarlo, se instalará el troyano de demostración en su sistema. El troyano de demostración simula un verdadero servidor de troyanos ocultando su ventana principal y escribiendo una entrada de inicio automático en el registro. Al hacer clic en el botón Desinstalar, se quita la entrada de inicio automático del registro y, a continuación se descarga el servidor de troyanos de demostración de la memoria. Al desinstalarlo se eliminan todos los archivos que fueron generados por el simulador, para no generar problemas o falsas advertencias generadas por el antivirus.

6 METODOLOGÍA

En este capítulo se describirá el caso de estudio que se realizó para lograr alcanzar los resultados de la investigación. Con el uso de la herramienta de detección de vulnerabilidades "Nessus" y los simuladores de amenazas informáticas.

6.1 Requerimientos o especificaciones

- Contar con una red LAN para la implementación de la propuesta de prevención de ataques informáticos.
- Instalación del software Nessus, que realiza una detección de vulnerabilidades en diferentes sistemas operativos además de generar reportes y especificar el nivel de riesgo de cada una de ellas.
- Recolección de simuladores de amenazas informáticas para el caso de estudio que se realizara en una red LAN.

6.2 Diseño e implementación

Al realizar el caso de estudio en la red LAN, se tomó un muestra de computadoras con diferentes métodos de protección (diferentes tipos de antivirus, firewall) y otra muestra sin ninguna protección. Después se realizó la instalación o ejecución de los simuladores de amenazas informáticas, para observar el modo en que respondían los métodos de protección con los que contaban las computadoras en ese momento ante los simuladores de amenazas.

Resultados del Simulador de virus EICAR

El primer simulador de amenaza informática con el que se realizó el caso de estudio fue Simulador de virus EICAR, a continuación se muestran los resultados que proporcionan las computadoras de la red con los siguientes métodos de protección:

Firewall

Con el uso del firewall, al insertar el dispositivo USB no realiza una detección de virus en el dispositivo, pero al tratar de ejecutar el simulador EICAR, el firewall despliega el siguiente mensaje que se muestra en la Figura 6.1.

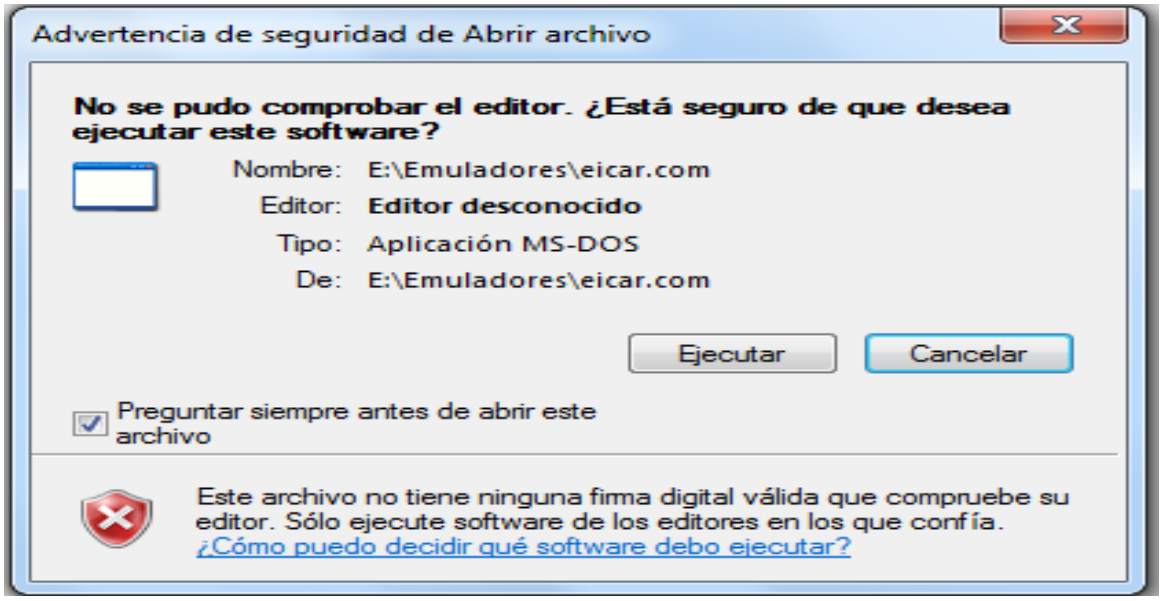


Figura 6.1.- Mensaje de advertencia de seguridad.

El firewall advierte que se puede estar instalando un archivo no seguro, por lo tanto advierte al usuario que este archivo puede ocasionar daños en el sistema informático.

Antivirus

En la Figura 6.2 se muestra que con el uso de antivirus, desde el inicio en el que se inserta el dispositivo USB, se detecta que existe software malicioso.

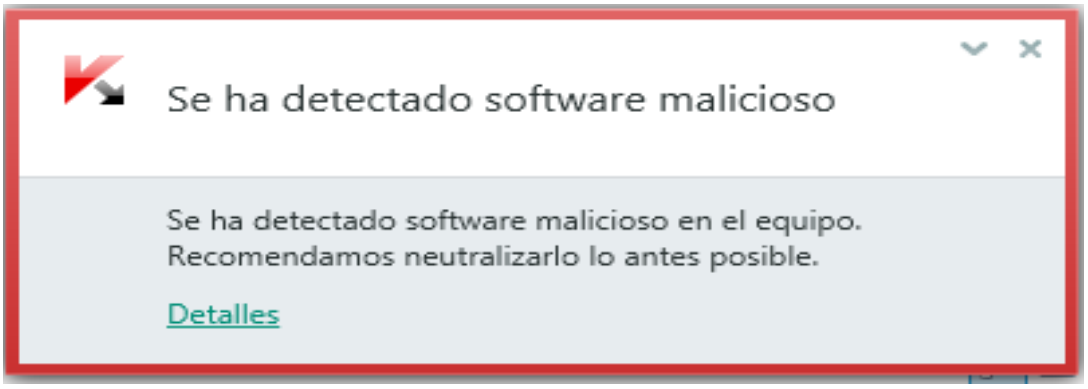


Figura 6.2.- Mensaje de detección de software malicioso.

Además si se trata de acceder o ejecutar el simulador, el antivirus no lo permite como se muestra en la Figura 6.3.

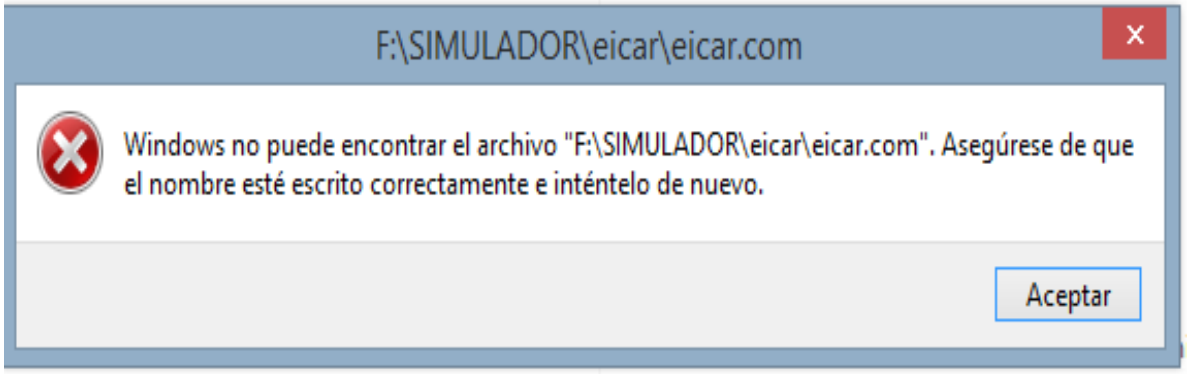


Figura 6.3.- Mensaje de Windows

En la Figura 6.4 se muestra como el antivirus realiza la eliminación del simulador y de este modo protege el sistema.

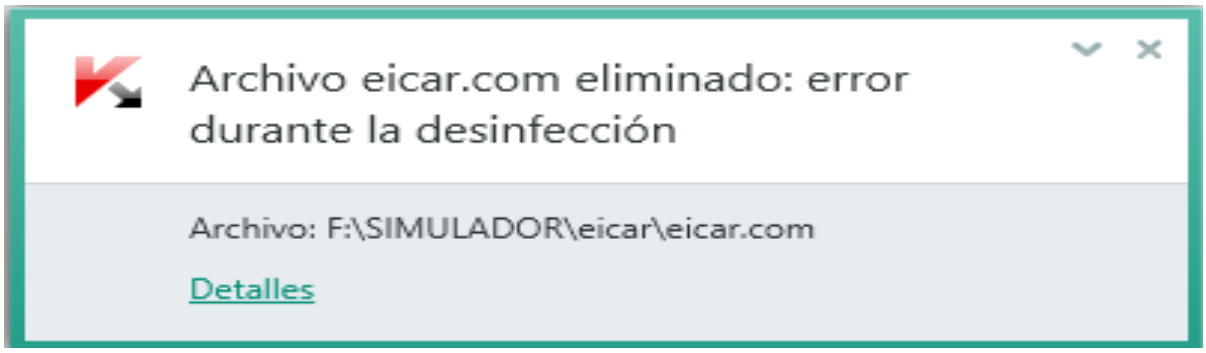


Figura 6.4.- Eliminación del simulador EICAR.

El uso de antivirus proporciona un nivel más alto de seguridad en la computadora, realiza como actividad complementaria la eliminación del archivo malicioso, vitando que este se propague por el sistema intentando causar daños.

Windows Defender y sin ningún método de protección

Al dar clic en el simulador EICAR para abrirlo en las computadoras que contaban con Windows Defender y las que no contaban con ningún método de protección, se ejecutaba sin ningún problema como se muestra en la Figura 6.5.

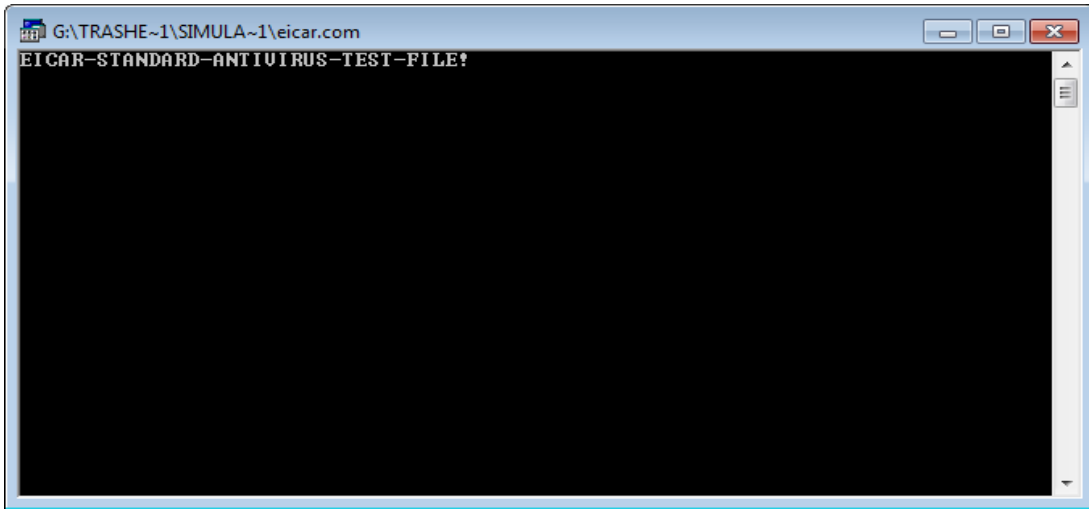


Figura 6.5.- Mensaje que se muestra al ejecutar el simulador EICAR.

La finalidad del simulador EICAR es desplegar una ventana con un mensaje, para demostrar que si no se tiene ningún método de protección en el sistema, se tienen demasiadas vulnerabilidades y por lo tanto es fácil que un intruso ejecute cualquier tipo de ataques en contra del sistema informático.

El simulador se ejecuta en las computadoras que cuentan con Windows Defender, aun cuando se realice actualización del antivirus, este no contiene en su base de datos un registro que demuestre que el simulador EICAR es una amenaza, se entiende que lo mismo puede suceder con otros registros de amenazas informáticas, por eso es recomendable hacer uso de otro tipo de antivirus.

Resultados del Simulador RanSim

El segundo simulador de amenaza informática que se utilizó fue Simulador RanSim (Ransomware Simulator), al instalarlo este empieza a generar diferentes amenazas de ransomware y verifica que tan vulnerable es el sistema dependiendo del método de protección que se esté ocupando en ese momento, a continuación se muestran los resultados que proporcionan las computadoras de la red LAN:

Firewall

Al utilizar como método de protección el firewall, con el simulador RanSim en primer lugar permite su instalación y al ejecutarlo este demuestra que el sistema es

completamente vulnerable a diferentes amenazas de ransomware, como se muestra en la Figura 6.6.

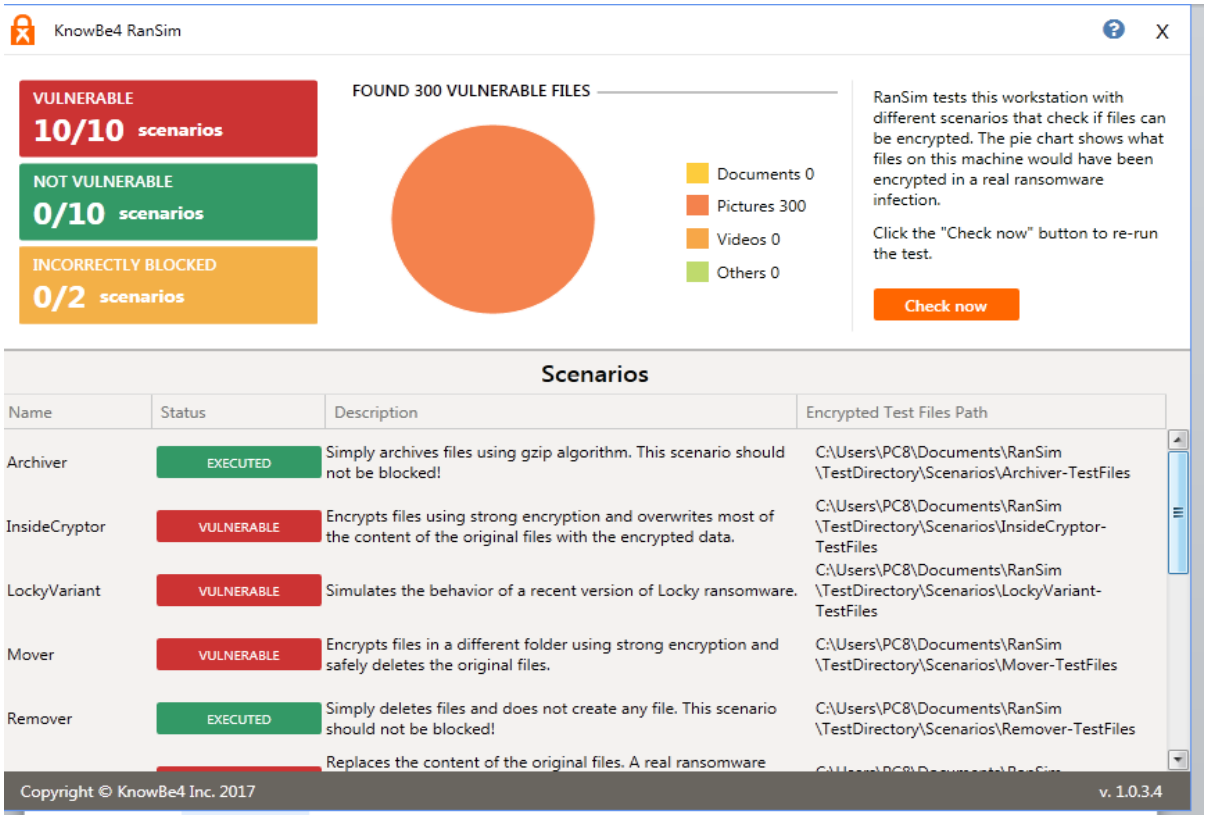


Figura 6.6.- Resultados del simulador RanSim.

Antivirus

Cuando se intenta instalar el simulador RanSim, en primer lugar el antivirus bloquea su ejecución, denegándole a Windows acceso al archivo del simulador, como se muestra en la Figura 6.7.

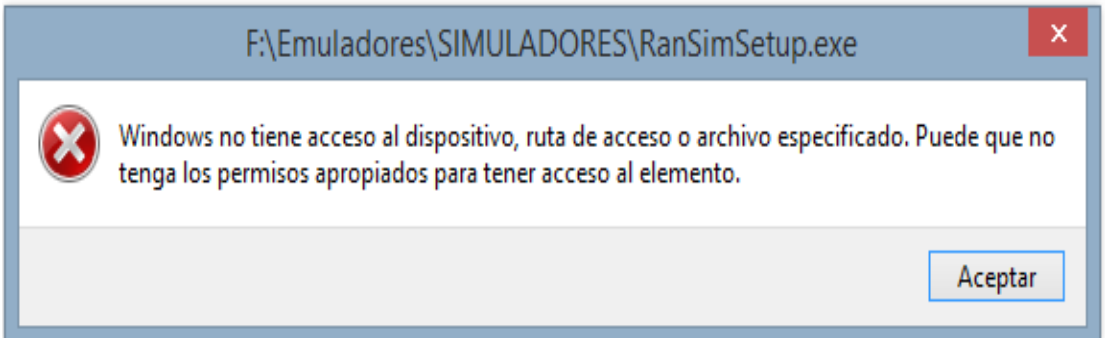


Figura 6.7.-Mensaje de Windows.

Después despliega un mensaje en el que se indica que se ha bloqueado acciones sospechosas de la aplicación, como se observa en la Figura 6.8.

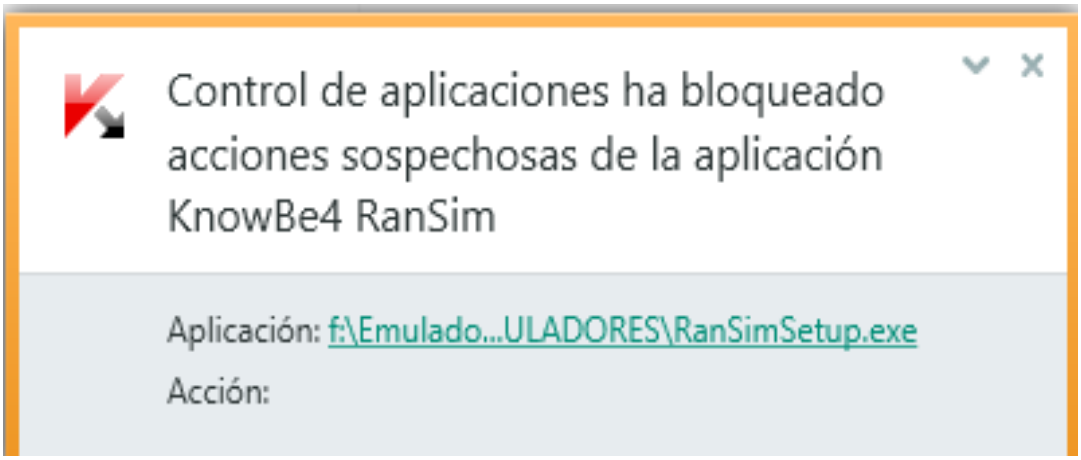


Figura 6.8.- Mensaje de bloqueo del simulador RanSim.

Finalmente el antivirus elimina el simulador porque esta lo está identificando como una aplicación maliciosa como se muestra en la Figura 6.9.

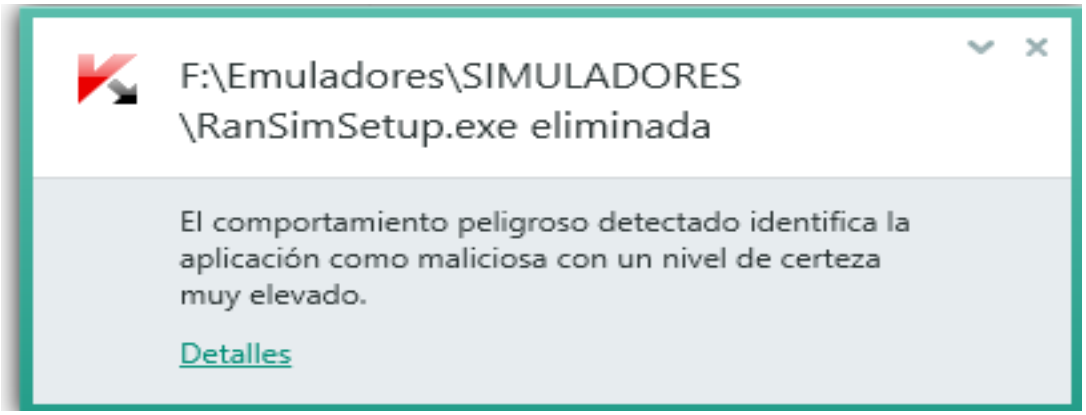


Figura 6.9.- Mensaje de eliminación del simulador RanSim.

Por lo tanto el uso del antivirus como método de protección no permite la ejecución de software malicioso que pueda dañar el sistema y realiza su correcta eliminación sin permitir en ningún momento que este se instale.

El antivirus mejora la protección del sistema evitando que sea vulnerable a las constantes amenazas que existen en una red informática, por esta razón es necesario estar realizando su constante actualización.

Windows Defender

Al utilizar Windows Defender este permite que se ejecute el programa pero al obtener los resultados del simulador RanSim, se muestra que de las diez amenazas de ransomware generadas solo en un escenario no se encuentra vulnerabilidad.

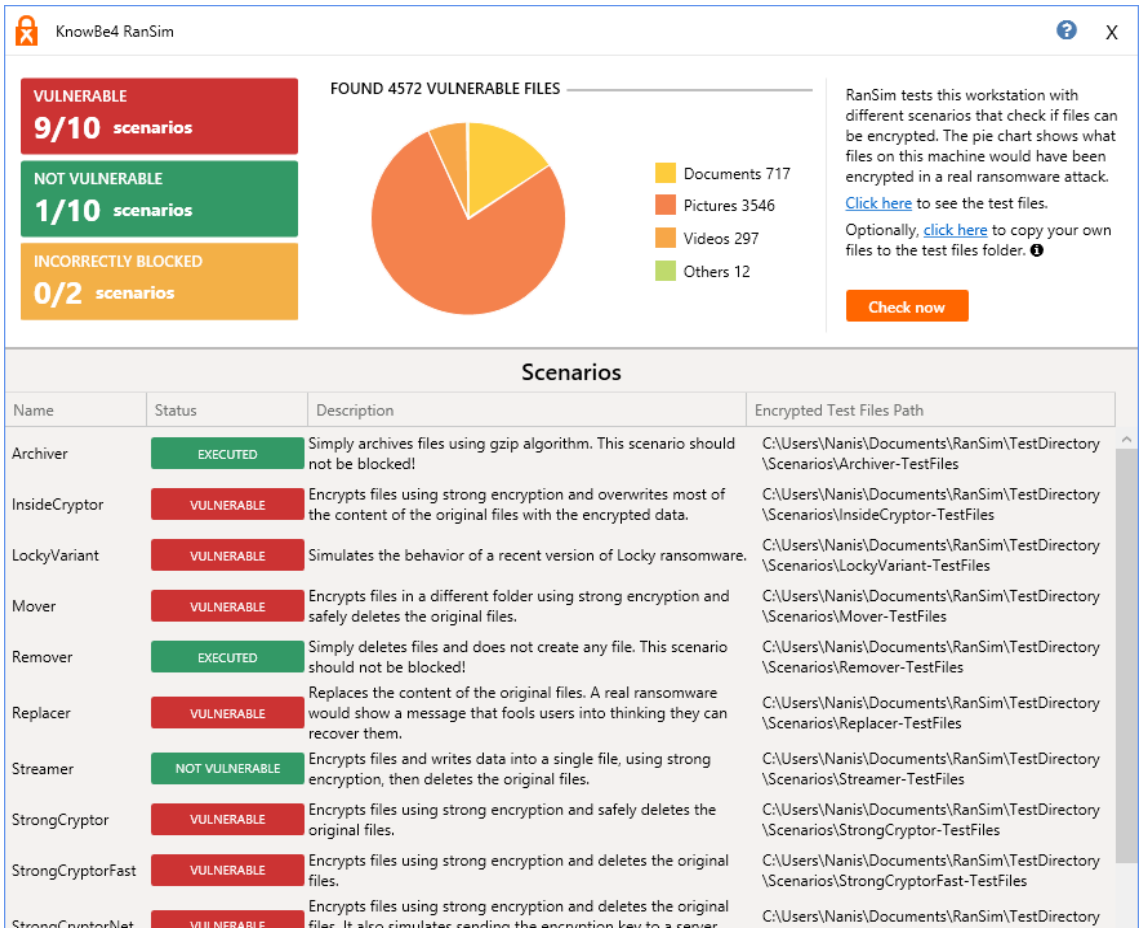


Figura 6.10.-Resultados del simulador RanSim.

En la Figura 6.10, se muestra que no se es vulnerable al momento de que un intruso pretenda cifrar archivos o escribe datos dentro de un archivo, pero por otro lado para mejorar que los resultados cambien es mejor ocupar más métodos de protección ante la amenaza de ransomware.

Sin ningún método de protección

Al intentar instalar el simulador RanSim en las computadoras que no contaban con ningún método de protección, este se instalaba con facilidad a diferencia de cuando se intenta

realizar la misma acción en las computadoras que contaban con antivirus, y al ejecutarse muestra que el sistema es completamente vulnerable a diferentes amenazas de ransomware como se puede observar en la Figura 6.11.

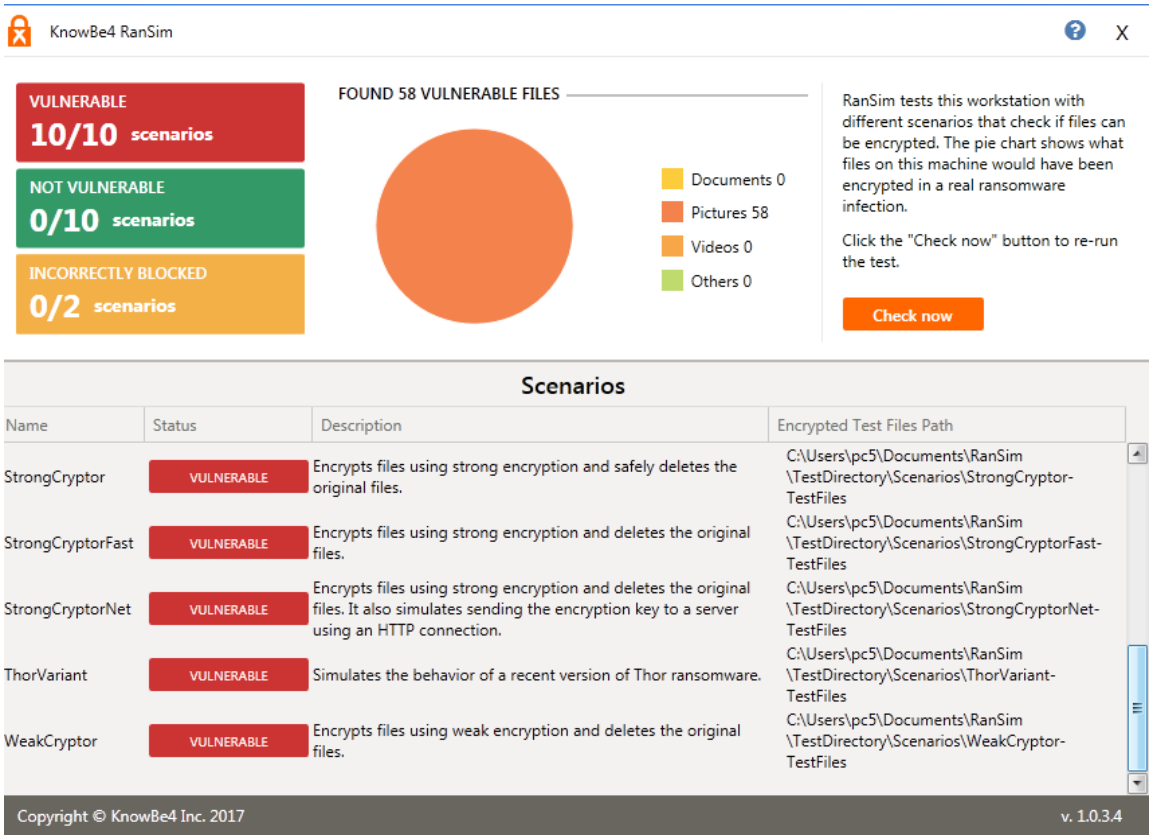


Figura 6.11.- Resultados del simulador RanSim.

El no contar con ningún método de prevención en el caso del simulador RanSim hace que la computadora sea un objetivo fácil para intrusos que deseen provocar ataques al sistema informático, en primer lugar a diferencia del uso del antivirus se pueden instalar amenazas fácilmente sin permiso del usuario, para después provocar diferentes ataques que dañen por completo el hardware, software y la información confidencial de la red.

Resultados del Simulador de Troyano

El último simulador de amenaza informática con el que se realizó el caso de estudio fue Trojan Simulator, a continuación se muestran los resultados que proporcionan las computadoras de la red con los siguientes métodos de protección:

Firewall

Con el uso del firewall, al insertar el dispositivo USB no realiza una detección de virus en el dispositivo, pero al tratar de ejecutar el simulador de troyano el firewall despliega el siguiente mensaje que se muestra en la Figura 6.12.

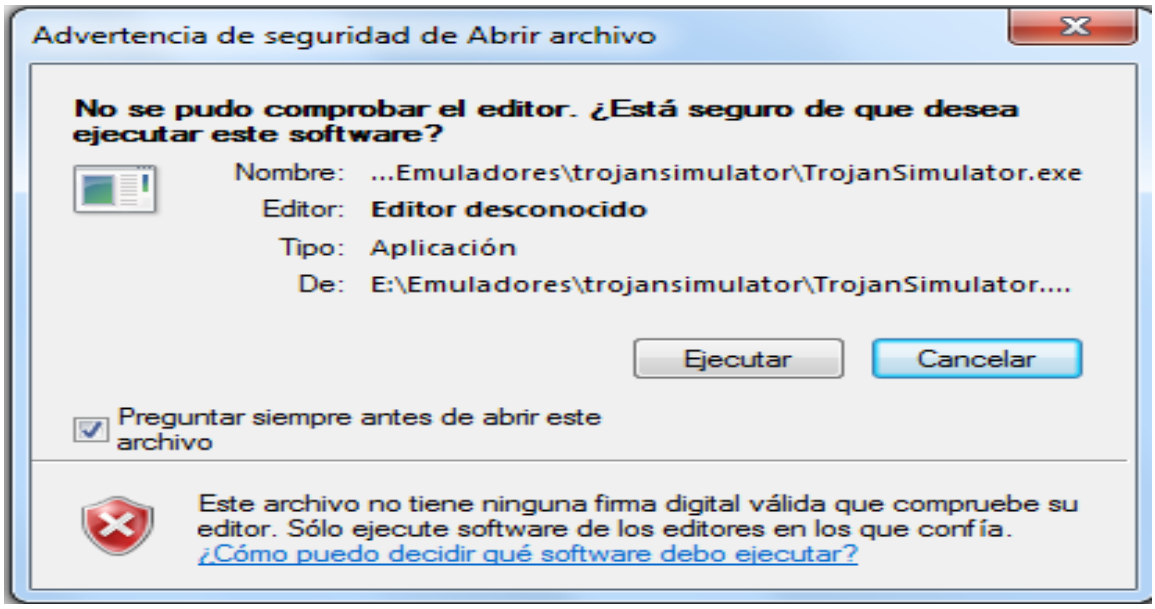


Figura 6.12.- Mensaje de advertencia de seguridad.

Si se desea hacer uso del firewall es necesario, que el administrador de la red informática no realice la instalación de antivirus que lo impidan su ejecución. Por otro lado el firewall puede ser personalizado con diferentes reglas que realicen el bloqueo de amenazas informáticas en el sistema informático.

Antivirus

Con el uso de antivirus, desde el inicio en el que se inserta el dispositivo USB, detecta que puede existir una amenaza e inicia a realizar un escaneo del dispositivo como se muestra en la Figura 6.13.

Figura 6.13.-Mensaje de escaneo de una amenaza informática.

Una vez que el antivirus termina de ejecutar el escaneo, despliega el mensaje que se muestra en la Figura 6.14, indicando que se ha eliminado la amenaza que se encontró antes de que esta se ejecutara.

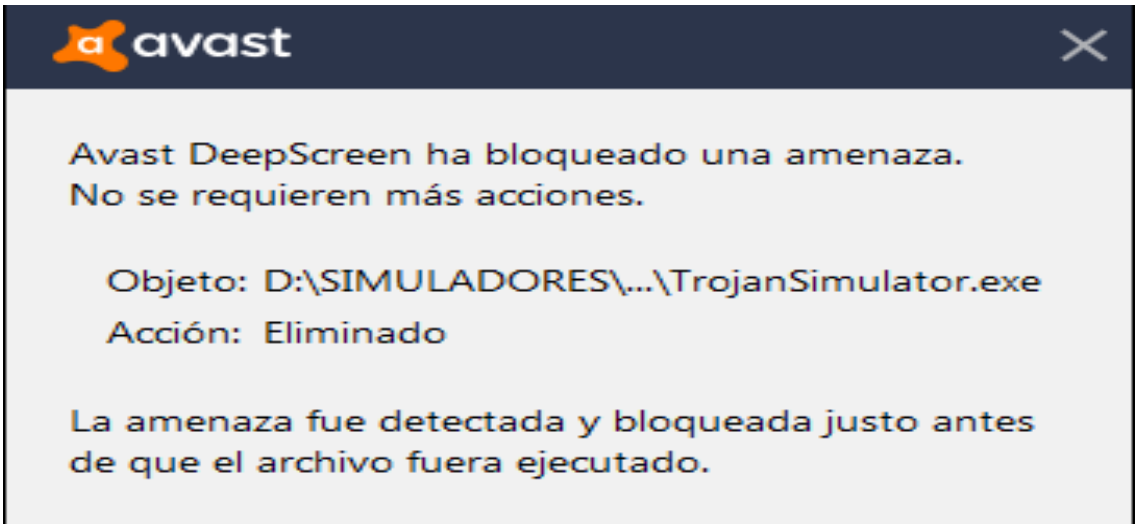


Figura 6.14.- Mensaje de eliminación del simulador.

Windows Defender y Sin ningún método de protección

Al dar clic en el Trojan Simulator para iniciar a instalarlo en las computadoras que contaban con Windows Defender y las otras que no contaban con ningún método de protección, se ejecutaba sin ningún problema como se muestra en la Figura 6.15.

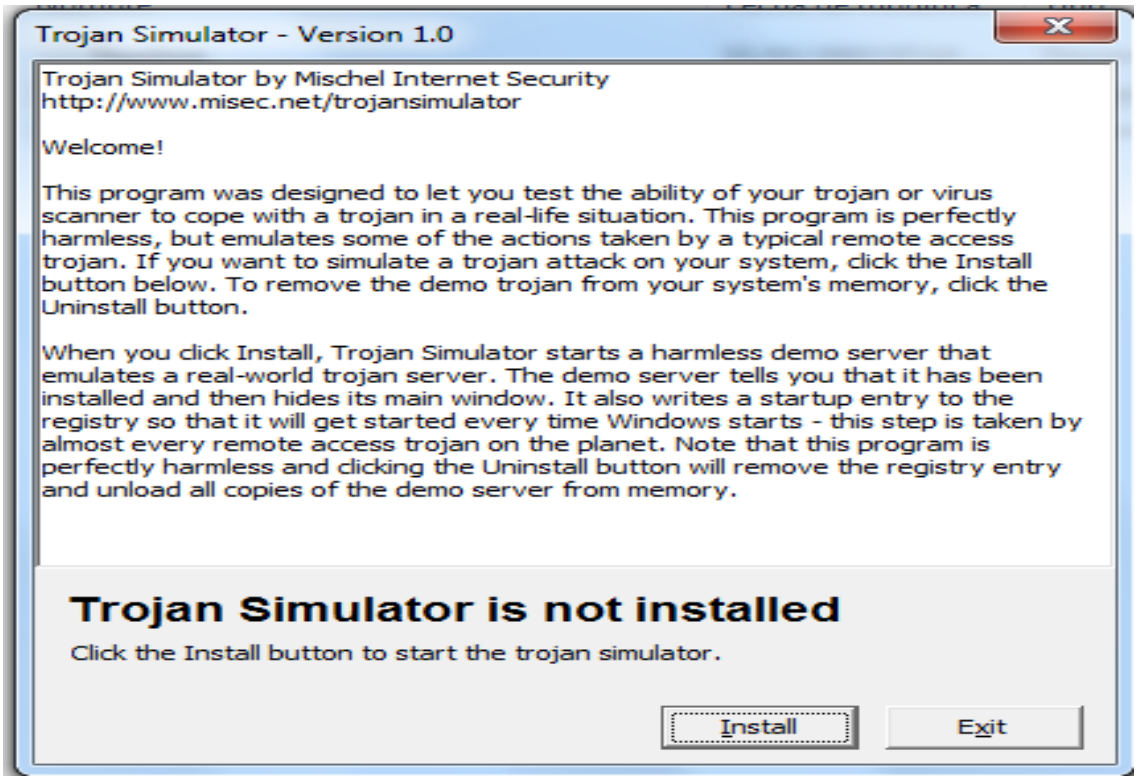


Figura 6.15.-Mensaje de instalación del Trojan Simulator.

Después de realizar una actualización de Windows defender el simulador se sigue ejecutando sin ningún problema en las computadoras, este no contiene en su base de datos un registro de que el simulador de troyano es una amenaza.

El objetivo de los tres simuladores es verificar si el método de protección con el que cuenta en ese momento la computadora es eficaz, y visualizar el comportamiento de respuesta que tendrían en caso de estarse enfrentando a amenazas reales que pudieran probar algún daño en la red LAN.

Como se comprobó con el caso de estudio que si en la red no se cuenta con ningún método de protección, las amenazas informáticas se pueden ejecutar, instalar fácilmente en el sistema sin que el administrador de la red o usuario se percate de que está siendo víctima

de ataques informáticos que dañen, pongan en riesgo el sistema y la información confidencial que tenga almacena. Sin duda alguna es necesario tener métodos de protección que ayuden a minimizar las vulnerabilidades y eviten que la facilidad con las que intrusos entren a la red con el objetivo de dañar el software o robar información.

USO DE NESSUS

Después de realizar el caso de estudio se continuo a realizar la instalación de la herramienta de escaneo "Nessus" como se muestra en el Anexo A, después se accede al interfaz de la aplicación, se da clic en nuevo escaneo avanzado, el cual realiza una exploración de los puertos además de una serie de ataques, como obtener acceso de forma no autorizada para tomar el control del sistema, verificar si existe el almacenamiento de archivos maliciosos o si se siguen ocupando servicios no actualizados y que tengan deficiencias, o malas configuraciones de seguridad, que comprueben la seguridad de la red, como se muestra en la Figura 6.16.

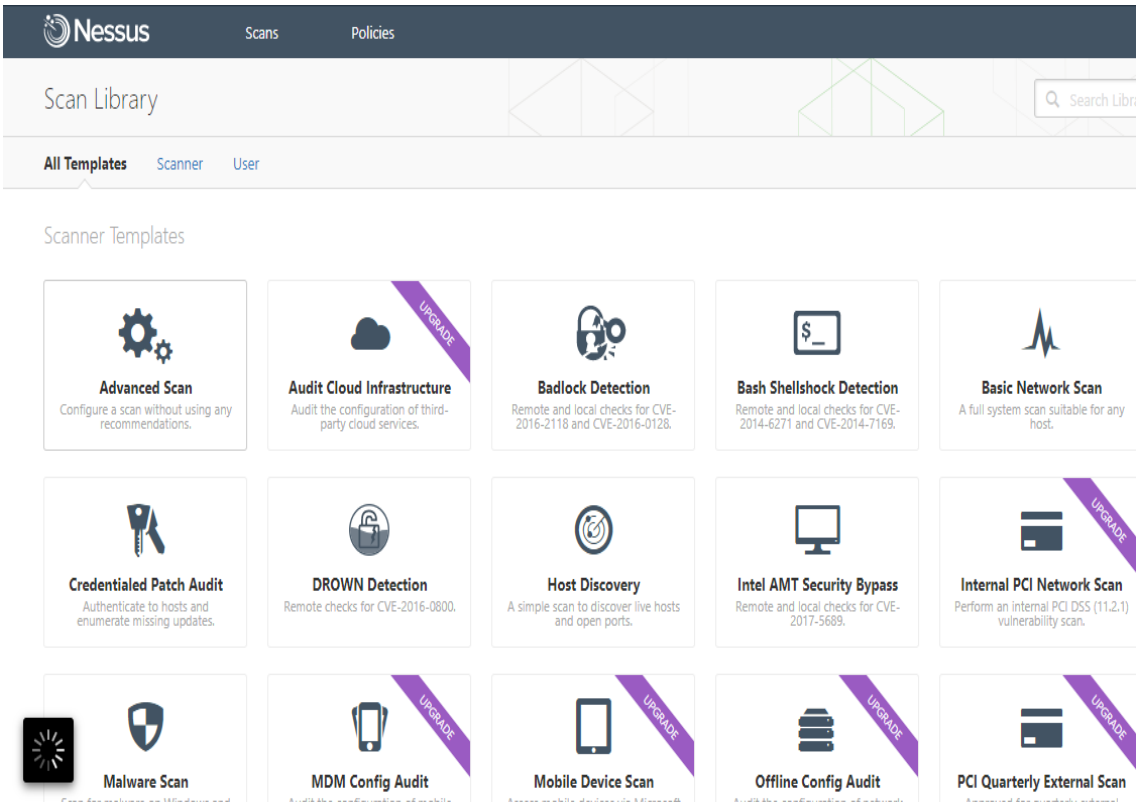


Figura 6.16.- Interfaz de la herramienta Nessus..

Después se configura el nombre y rango de direcciones IP ´s, a las cuales se les realizara el escaneo avanzado, como se muestra en la Figura 6.17.

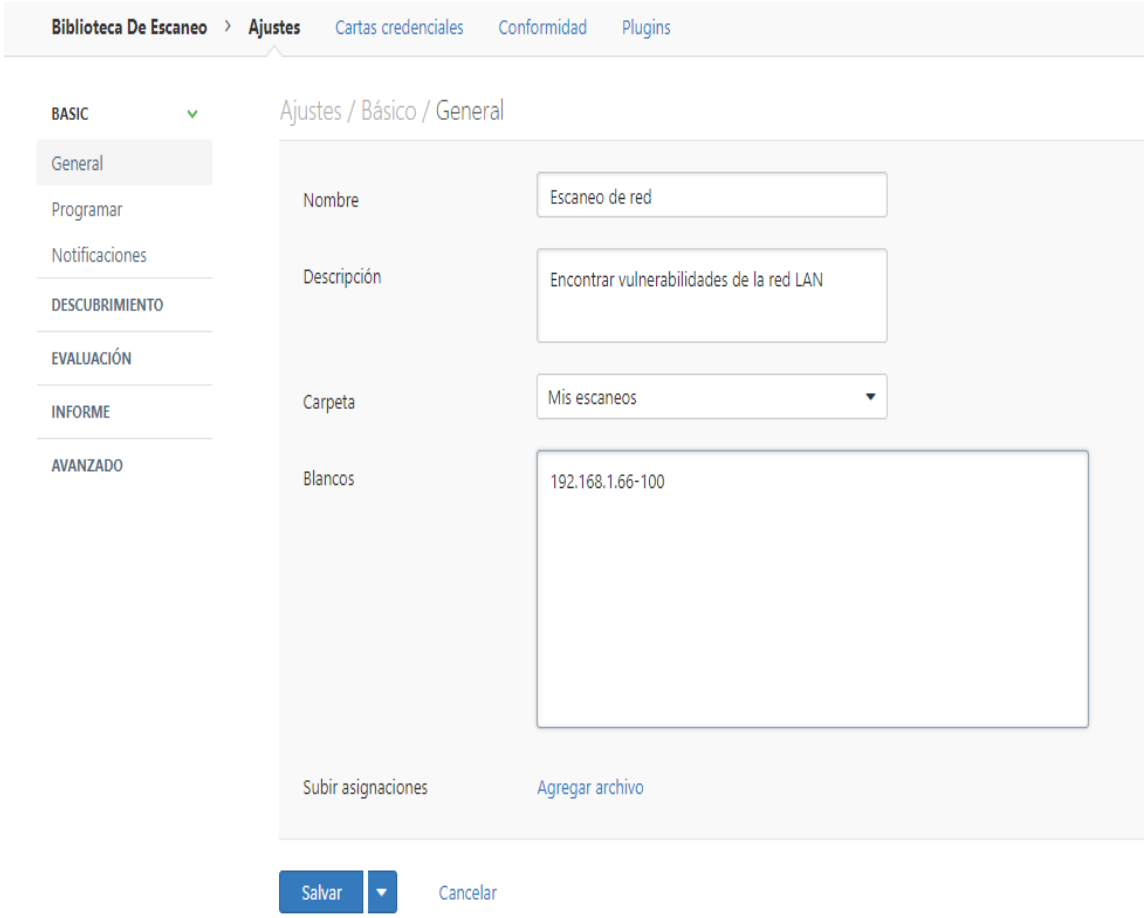


Figura 6.17.-Configuración del escaneo avanzado.

Se debe de dar clic en Salvar para guardar el nuevo escaneo que se ha configurado después dar clic en ejecutarlo para que inicie el escaneo de todas las direcciones IP´s y al terminar de realizar el escaneo de la red, se muestra las vulnerabilidades que se encuentran en la red, es necesario hacer uso de herramientas de escaneo de vulnerabilidades para comprobar el estado actual de la seguridad de la red.

6.3 Propuesta de prevención de ataques informáticos

De acuerdo al caso de estudio se demuestra que es necesario contar con algún método de protección, por este motivo en la red LAN se implementó la siguiente propuesta de prevención de ataques informáticos con la finalidad de desarrollar una estrategia para evitar y contrarrestar ataques mediante el uso de diferentes métodos de prevención.

- En primer lugar es necesario que el administrador de red utilice y recomiende a los usuarios contar con contraseñas seguras (que contenga más de ocho caracteres, que combinen letras, dígitos y caracteres especiales), realizar constantemente la copia de seguridad de los datos, evitando la duplicidad de documentos y archivos no utilizados, es necesario recordar que el activo más importante de la red informática es la información.
- Instalar el antivirus que cumpla con las características necesarias para la protección de la información de la red LAN, como lo demuestra el caso de estudio, el antivirus fue el método de prevención que detectó los simuladores de amenazas con mayor eficiencia. En caso de no contar o desear comprar un antivirus se recomienda activar el firewall de Windows o utilizar el antivirus que viene por defecto en los sistemas operativos de Windows "Windows defender" como último método de protección.
- Realizar la constante actualización del sistema operativo, software y el navegador utilizado en la red LAN, también es recomendable desinstalar software que no sea necesario u obsoleto con el objetivo de liberar espacio en el disco duro para el almacenamiento de información.
- Por otro lado, dependiendo del navegador que se esté utilizando, el administrador de la red puede instalar herramientas que proporcionan los mismos navegadores (extensiones) para evitar las diferentes amenazas de spyware, adware, phishing, la ventaja con la que cuenta es que son gratuitas y seguras.
- También es necesario que todas las computadoras utilicen algún tipo de software anti-ransomware, de acuerdo con el informe de seguridad 2016 de Cisco, este tipo de amenaza está cada vez más en aumento porque para los intrusos informáticos resulta una operación de bajo mantenimiento y proporciona una rápida

rentabilización, ya que los usuarios pagan a los atacantes directamente en criptodivisas [30]. La mayoría de los antivirus están incluyendo la detección de amenazas de tipo ransomware, pero es recomendable hacer uso de herramientas adicionales que protejan de este tipo de amenazas.

- El informar a los usuarios de la red LAN de los diferentes tipos de amenazas a las que se encuentran expuestos al estar inmensos en el mundo del Internet y proporcionarles información acerca de cómo disminuirlas, es un método de prevención que ayuda a crear una educación de prevención, que poco a poco debe de dar resultados. Sin duda alguna los usuarios que no cuentan con ninguna información acerca de los métodos de prevención informática son los más vulnerables a sufrir ataques informáticos constantemente en sus dispositivos electrónicos y estos pasan desapercibidos, y con eso aumentan las amenazas en la red, casi siempre estas se propagan por los demás dispositivos conectados.
- Por último, es necesario estar realizando escaneos en la red en busca de vulnerabilidades, para detectar los puntos que puedan estar vulnerables y por lo tanto solucionarlos.

En la Tabla 6.1, se muestran las diferentes herramientas de protección que se ocuparon en la propuesta de prevención de ataques informáticos, con el objetivo de mejorar la seguridad de la red LAN [39, 40].

Tabla 6.1.- Herramientas de protección.

Nombre	**Protección ante:**	**Descripción**
Bitdefender TrafficLight	Malware Phishing Gratuito	Analiza las páginas que visita el usuario en busca de malware e intentos de phishing. Realiza la búsqueda cada vez que se accede a diferentes páginas para evitar la amenaza de sitios Web ilegítimos.
Trustnav Adblock & Security Suite	Adware Gratuito	Mantiene la seguridad al consultar cada sitio web al que se accede o en la descarga que se esté realizando, evitando las amenazas de tipo adware. Si el sitio web

		o la descarga está calificado como inseguro, se le notificará para evitar que el usuario de información acerca de la tarjeta de crédito, credenciales, o cualquier tipo de información a intrusos
AdGuard	Spyware Gratuito	Bloquea dominios conocidos por extender malware, protegiendo el ordenador contra virus, caballos de troya, gusanos, software espía y programas de anuncios. Adguard realmente minimiza el riesgo de infección por virus y bloquea el acceso a sitios maliciosos para evitar ataques.
Bitdefender Anti Ransomware	Ransomware Gratuito	Es una herramienta de seguridad gratuita que ofrece protección ante el ransomware existente y emergentes. Manteniendo sus archivos seguros del cifrado de una manera simple y no intrusiva.

7 RESULTADOS Y DISCUSIÓN

Después de mejorar la seguridad informática en la red LAN, se realizó un escaneo en busca de vulnerabilidad para verificar si después de la implementación de la propuesta de prevención de ataques informáticos fue efectiva para disminuir las diferentes vulnerabilidades informáticas.

Como se muestra en Figura 7.1, el resultado del escaneo avanzado con la herramienta "Nessus" demuestra que no se encuentran vulnerabilidades de alto, mediano o bajo riesgo en la red LAN, solo hay vulnerabilidades de tipo informativas, que son aquellas que no proporcionan ningún riego al sistema, comprobando así la efectividad de la propuesta, además de demostrar que entre mayor sea el número de métodos de protección que se utilicen en la red informática aumenta la seguridad de la misma disminuyendo las vulnerabilidades.

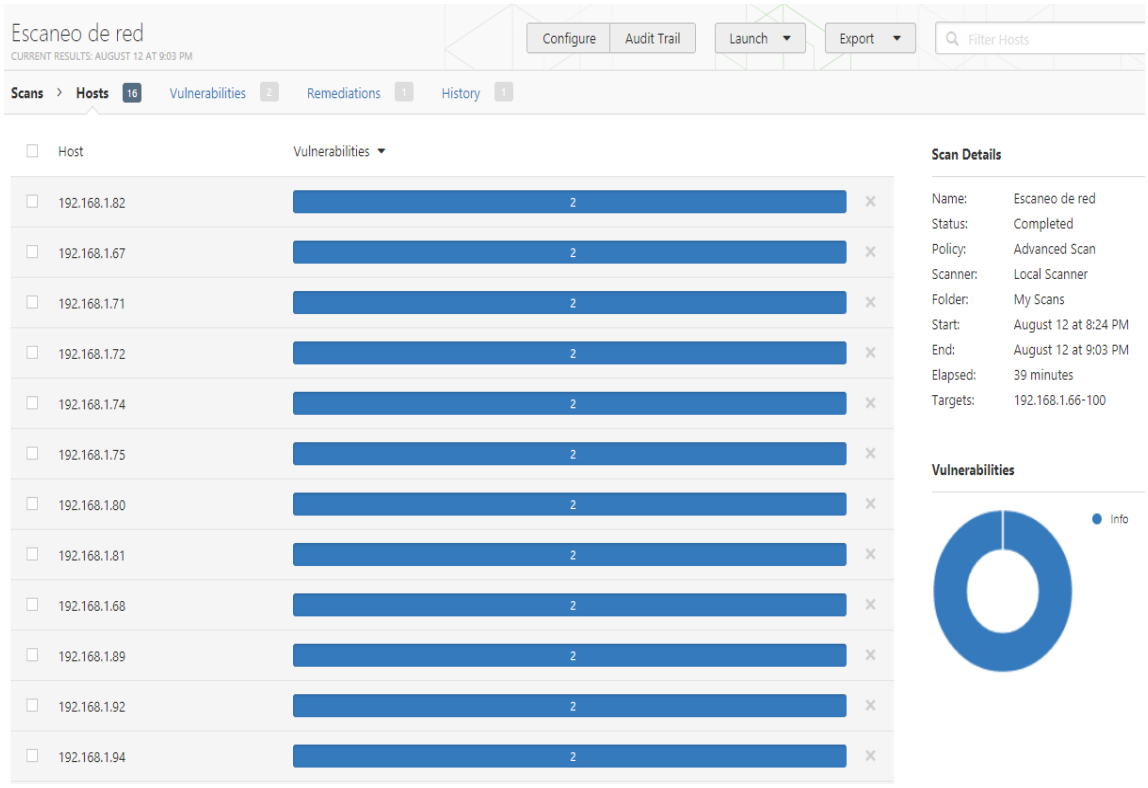


Figura 7.1.- Resultados del escaneo de la red LAN.

Se muestra en la Figura 7.2, el tipo de vulnerabilidad con el que cuenta cada una de las computadoras son informativas: la primera es que informa que Nessus realizo un escaneo y la otra es de tipo traceroute que hace referencia a que se realizó el seguimiento de la

pista de los paquetes que vienen desde el host que fue escaneado de la red LAN que fueron escaneadas.

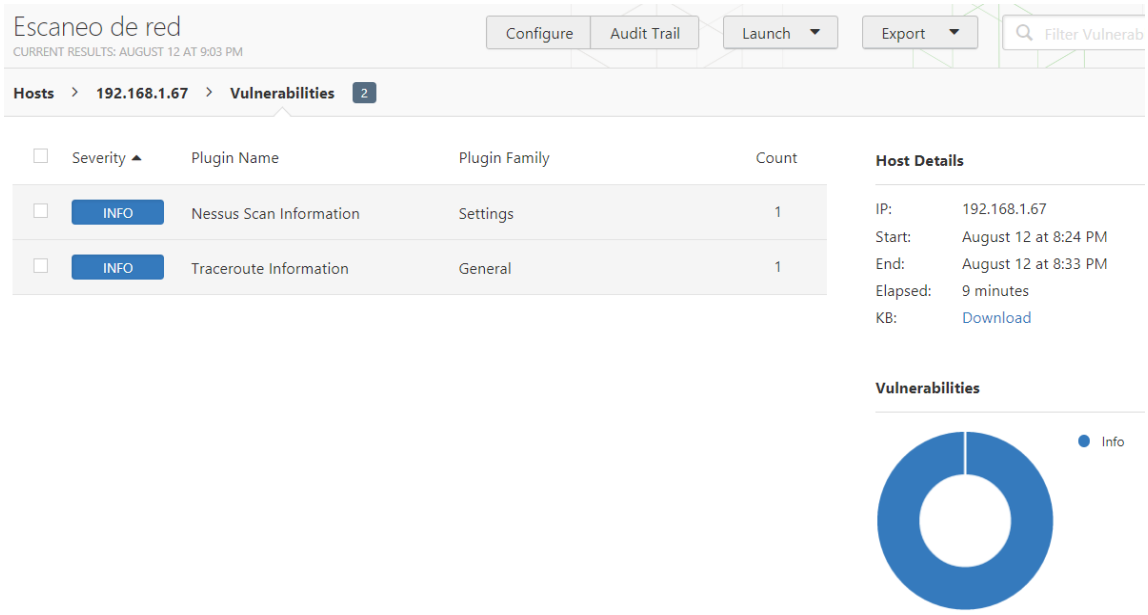


Figura 7.2.- Resultados de las vulnerabilidades encontradas en las computadoras de la red LAN.

En la actualidad no hacer uso de diferentes métodos de prevención y protección es un gran error, de acuerdo al informe semestral de Cisco de 2017 [38], la evolución del "Internet of Things" (IoT, Internet de las cosas) aumenta las posibilidades de los intrusos informáticos de realizar ataques en cuanto a su escalabilidad e impacto potencial, por lo que, seguirá en aumento, aprovechando las vulnerabilidades de seguridad para aprovecharlas y realizar daños en el sistema. Por esta razón es necesario mejorar la seguridad de la red para disminuir la probabilidad de ser víctima de algún tipo de ataque informático.

CONCLUSIONES

En el presente trabajo se ha podido evidenciar que el crecimiento de los ataques informáticos sigue avanzando constantemente, así como la gran cantidad de herramientas de detección de vulnerabilidades y de protección que existen, por lo tanto, no realizar la protección de un sistema informático permite el fácil acceso de intrusos al sistema poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información, además de aumentar los costos por realizar mantenimiento correctivo a los dispositivos dañados.

Por otro lado, a través del caso de estudio se observaron los diferentes resultados de los métodos de protección ante simuladores de amenazas que dio pauta a la elaboración de la propuesta de prevención de ataques informáticos.

Después de mejorar la seguridad informática de la red LAN, mediante el uso de los métodos de la propuesta de prevención de ataques como la actualización del sistema operativo, software y el navegador, además del uso de antivirus así como herramientas anti spyware, adware, phishing, y ransomware, además de realizar el mejoramiento de las contraseñas, se comprobó por medio del escaneo de vulnerabilidades de la red que no se contaba con ningún tipo de vulnerabilidad que pudiera ocasionar daños en los dispositivos.

Los administradores de las redes informáticas deben estar en una constante actualización en el área de seguridad informática, de este modo mejorarían sus acciones de respuesta ante las inminentes amenazas que se están generando, es necesario enfatizar que la seguridad de la información es la parte central de cualquier tipo de red, por lo que siempre se deben realizar búsqueda de las posibles vulnerabilidades que pudiera presentar la red.

Se concluye indicando que sin importar el tipo de red con el que se cuente es necesario utilizar diferentes métodos de prevención así como la realización constante de detección de vulnerabilidades con el uso de las diferentes herramientas de escaneo que existen y de este modo realizar un plan de acción para disminuir la posibilidad de sufrir ataques informáticos.

Trabajos Futuros

Se pueden realizar algunos de los siguientes trabajos de investigación:

- Realizar una comparación de las herramientas de detección de vulnerabilidades “Nessus” y “OpenVAS”, describiendo su facilidad de uso, las ventajas y desventajas que proporcionan después de haber realizado diferentes escaneos con dichas herramientas.
- Realizar un trabajo de investigación que proporcione las principales ventajas y desventajas del avance del Internet de las Cosas en cuanto a la seguridad informática.

REFERENCIAS

[1] Unidad de Innovación y Nuevas Tecnologías de la División de Desarrollo Productivo y Empresarial de la CEPAL, "La nueva revolucion digital: De la internet del consumo a la internet de la produccion", Informe, CEPAL,Santiago, Agosto 2016.

[2] Prensario TI Latín América, "Seguridad IT en Latinoamérica", Informe, Prensario TILA, Enterprise & Pymes,Argentina, Marzo 2017.

[3] Clasificación de la Información, (2017,12 Junio), Tipos de clasificación [Online] Available:http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Clasificacion_de_la_Informacion.pdf

[4] Jose Fabián Roa Buendía, *Seguridad Informática*, Aravaca, Madrid: McGraw-Hill, 2013.

[5] Paul Rascagneres, *Seguridad informática y Malwares*, Europa, ENI, Colección Epsilon, 2016.

[6] Álvaro Gómez Vieites, *Enciclopedia de la Seguridad Informática 2da Edición Actualizada*, Madrid, RA-MA, 2011

[7] Seguridad de la Información, (2017,12 Junio), ISO 27001: La norma ISO 27001 del Sistema de Gestión de Garantía de confidencialidad, integridad y disponibilidad [Online] Available: https://www.aec.es/c/document_library/get_file?uuid=a89e72de-d92b-47cf-ba5e-5ea421fcbeb4&groupId=10128

[8] Natali Jasso Guadiana , "Cómputo en la nube: Seguridad en el gestionamiento de la información", Tesis de Licenciatura, Universidad Nacional Autonóma de México, Estado de México, 2012.

[9] Comunicación y redes,(2017,12 Junio), Criterio de redes, [Online] Available: https://sites.google.com/site/rominaceballosredes/criterio-de-redes.

[10] Bruce A. Hallberg, *Fundamentos de Redes*, Cuarta Edición, Mexico,D.F: McGraw-Hil Interamericana, 2014.

[11]Medios de Transmisión,(2017,18 Junio), Guiados y No Guiados, [Online] Available http://www.dte.us.es/personal/sivianes/tcomu/MediosTransmision.pdf

[12] Nuria Oliva Alonso, *Redes de comunicaciones Industriales*, Aravaca, Madrid: UNED, 2013.

[13]Elastixtech,(2017,18 Junio), Fundamentos de redes y TCP/IP, [Online] Available: http://elastixtech.com/wp-content/uploads/2014/01/FUNDAMENTOS-DE-REDES-Y-TCP_IP.pdf

[14] Sistemas Abiertos,(2017,18 Junio), Protocolos de red, [Online] Available: http://redesbirdg.galeon.com/sistemasa.htm

[15] Informática, (2017,18 Junio), Caracteristicas de los protocolos de red, [Online] Available: https://books.google.com.mx/books?isbn=8466506098

[16] José Dordoigne, Redes Informaticas: Nociones fundamentales, 5ta Edicion, Barcelona, ENI, 2015

[17] Sistemas Industriales Distribuidos(2017,19 Junio), Redes de comunicaciones:Topologias y Enlaces [Online] Available: http://www.uv.es/rosado/courses/sid/Capitulo2_rev0.pdf

[18] Symantec, (2017, 19 Junio). Glosario de Seguridad 101 [Online]. Available: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

[19] Sistema de Gestión de Seguridad de la Información (2017,19 Junio), ISO 27001: Amenazas y vulnerabilidades [Online] Available: http://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

[20] Javier Ríos Yáguez,"Técnicas y herramientas de análisis de vulnerabilidades de una red", Proyecto de fin de grado, Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación, Madrid, 2014

[21] Henry Cristhian Mancheno, Ivette Lorena Robles, "Vulnerabilidades y Seguridad en Redes TCP/IP", Tesis de Licenciatura, Quayaquil, Ecuador, 2013

[22] José Manuel Agrelo, Informatica Forese: Auditoria de seguridad, España: Universidad Autónoma de Madrid, 2014.

[23] CSRIT-CV,(2017, 20 Junio) Herramientas para el escaneo y detección de vulnerabilidades, [Online], Available: https://www.csirtcv.gva.es/es/paginas/herramientas-escaneadoras-y-detectoras-de-vulnerabilidades.html

[24] Revista Electronica de Computacion, Informatica, Biometria y Electronica, (2017, 20 Junio), Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web, [Online], Available: http://recibe.cucei.udg.mx/revista/es/vol4-no1/computacion05.html

[25] Henry David Quishpe, "Análisis de Vulnerabilidades en la Red LAN", Tesis de Licenciatura, Universidad Nacional de Loja, Ecuador, 2016

[26] Scribd, (2017, 24 Junio) Tipos de ataques informaticos, [Online], Available: https://es.scribd.com/doc/19397003/Tipos-de-Ataques-informaticos

[27] Scribd, (2017, 24 Junio) Tipos de ataques e Intrusos en las redes informaticos, [Online], Available: https://es.scribd.com/doc/36013250/Tipos-de-Ataques-e-Intrusos-en-Las

[28] Kasperky, (2017, 24 Junio), Tipos de Amenzas Informaticas, [Online], Available: https://latam.kaspersky.com/resource-center/threats/adware

[29] Seguridad de la Informacion, (2017, 24 Junio), Tipos de Amenzas, [Online], Available: http://www.segu-info.com.ar/ataques/ataques.htm

[30] CISCO, "Informe anual de seguridad", Informe, Cisco y/o sus filiales, América, Enero 2016.

[31] Victor Manuel Prieto Alvares, Ramon Adrian Pan Choncheiro , "Virus Informaticos", Universiadad de Coruña, Tesis de Licenciatura, 2014

[32] Securelist, (2017, 24 Junio), Panorama de las ciberamenazas en el primer trimestre de 2017, [Online], Available: https://securelist.lat/it-threat-evolution-q1-2017/85002/

[33] Tenable (2017,25 Junio), Escaner de vulnerabilidades Nessus, [Online], Available: https://www.tenable.com/products/nessus-vulnerability-scanner

[34] Kasperky Lab, (2017, 25 Julio) Simulador de virus EICAR, [Online], Available: https://support.kaspersky.com/mx/general/products/7399

[35] Knowbe4, (2017, 28 Julio) Simulador RanSim, [Online], Available: https://www.knowbe4.com/ransomware-simulator

[36] Raymondm computers, made easy, (2017, 28 Julio) Trojan Simulator, [Online], Available: https://www.raymond.cc/blog/test-the-effectiveness-of-your-antivirus-firewall-and-hips-software/

[37] Websetnet, (2017, 28 Julio) RanSim Ransomware simulador, [Online], Available: https://websetnet.com/es/ransim-ransomware-simulator-will-tell-computer-protected

[38] CISCO, "Informe semestral de ciberseguridad", Informe, Cisco y/o sus filiales, América, Julio 2017.

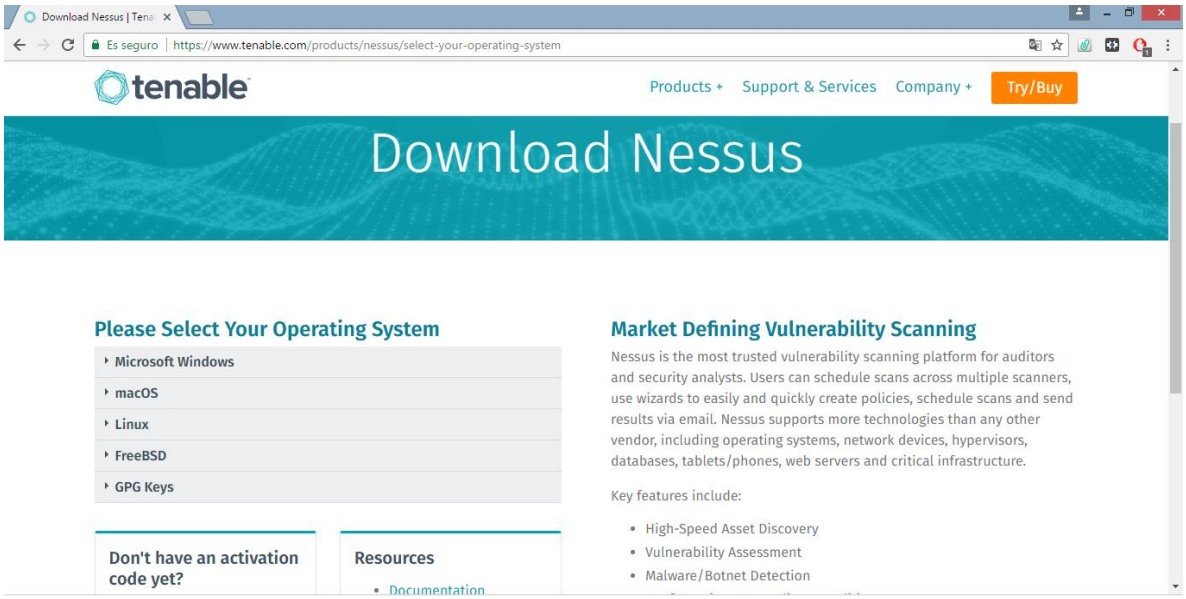
[39] Chrome Web Store (2017, 31 Julio) Extensiones, [Online], Available: https://chrome.google.com/webstore/category/extensions?hl=es

[40] BitDefender, (2017, 31 Julio) Anti-Ransomware Tools, [Online], Available: Https://www.bitdefender.com/solutions/anti-ransomware-tool.html

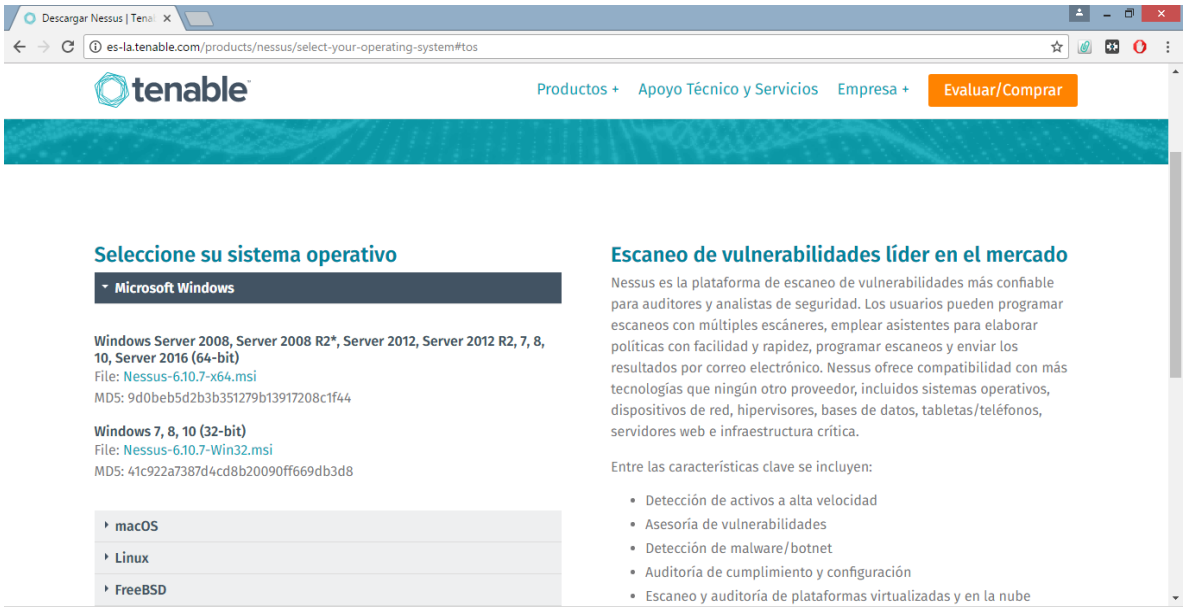
ANEXO A

Instalación de Nessus

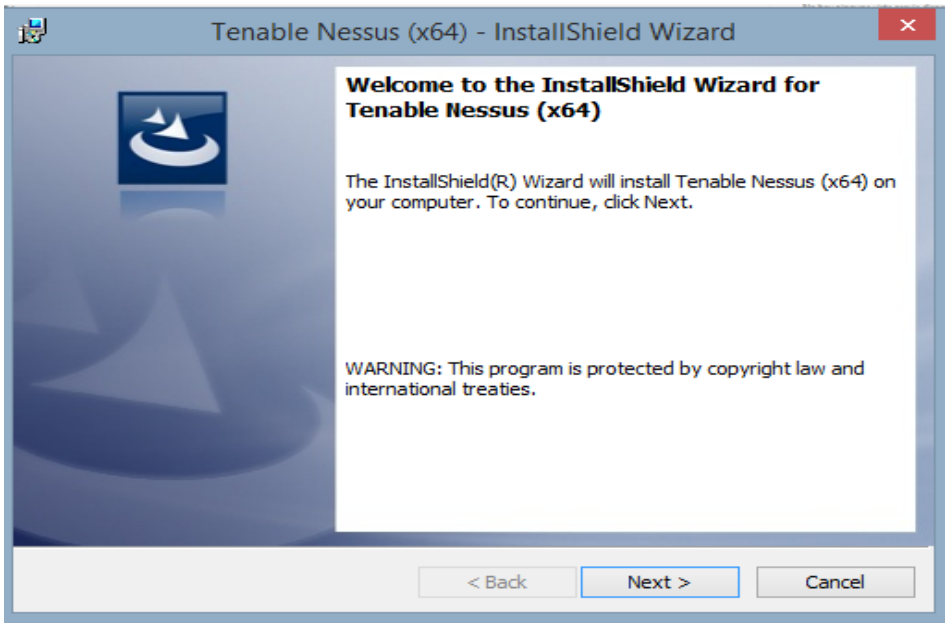
Acceder a la página principal de Nessus, para iniciar con la descarga y seleccionar la versión del sistema operativo de su preferencia.



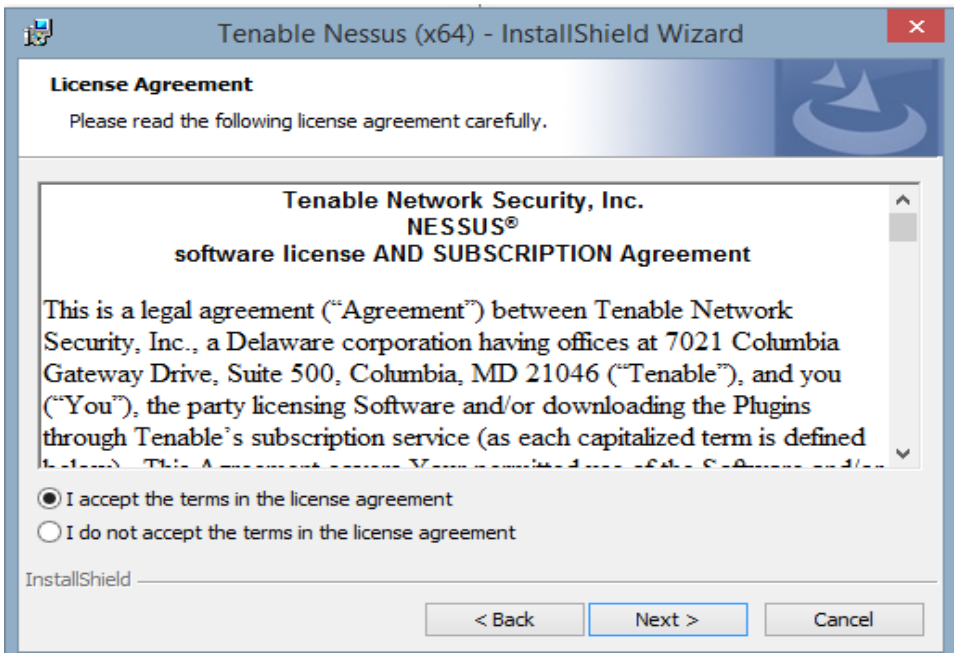
En este caso se hará la instalación en un sistema operativo Windows 8 de 64 bits.



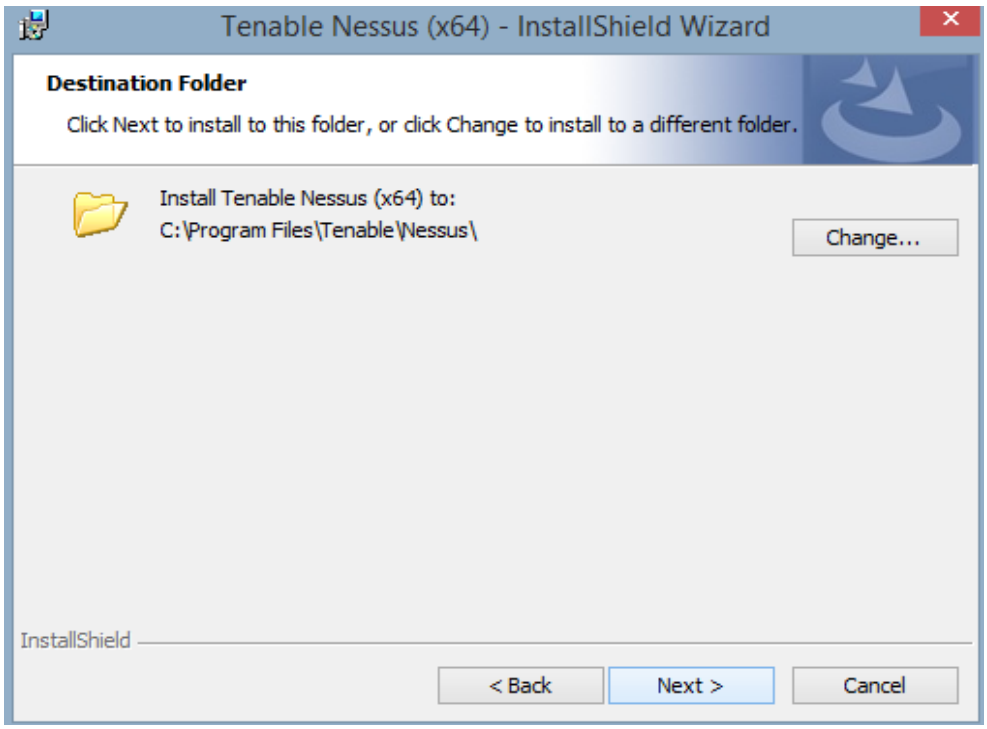
Después de que la descarga termine, ejecutar el instalador, aparece el siguiente asistente para la instalación, y dar clic en next para continuar.



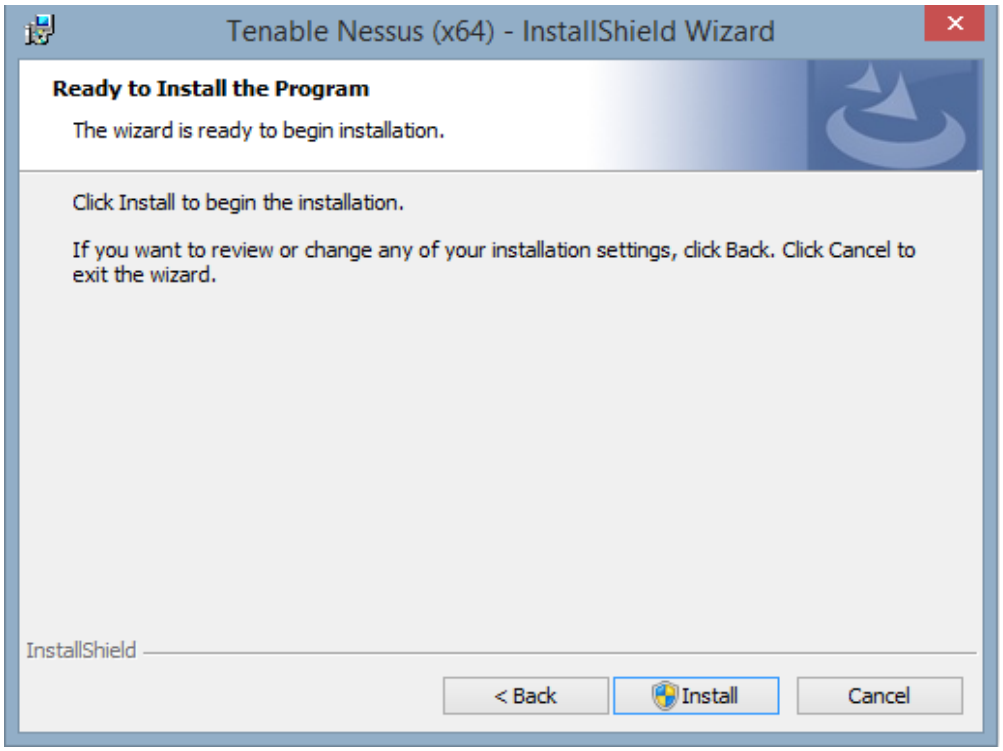
Leer y aceptar los términos y condiciones, dar clic en next para continuar.



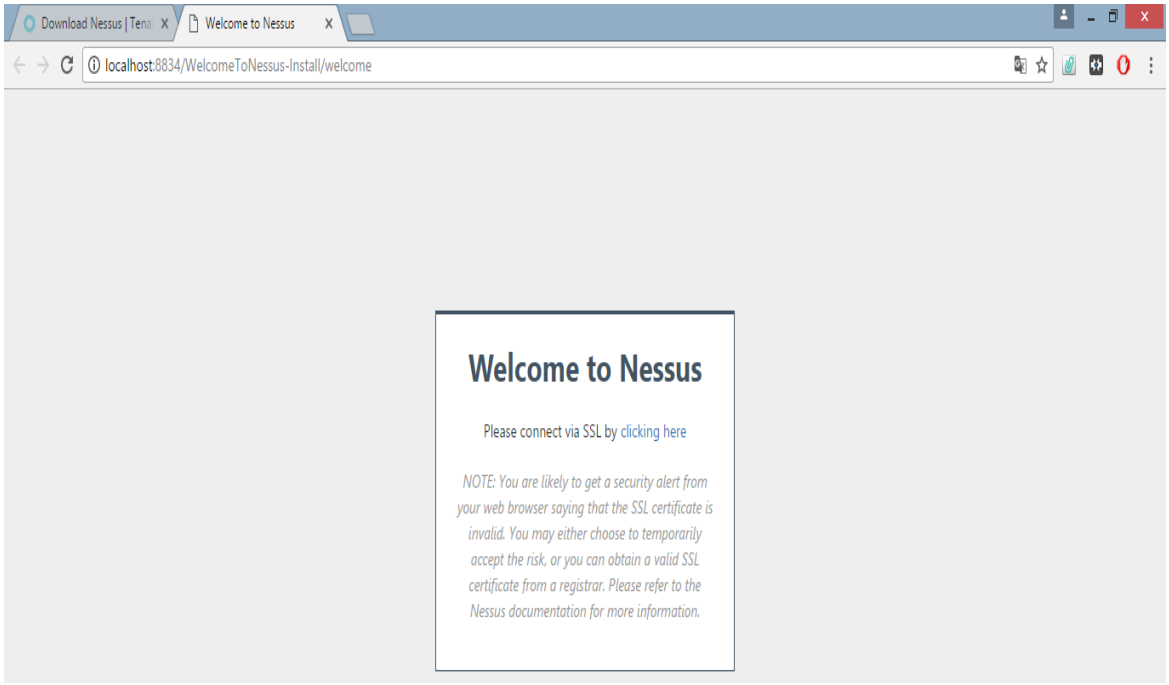
Se debe seleccionar la ubicación en el cual se instalara el software y dar clic en next.



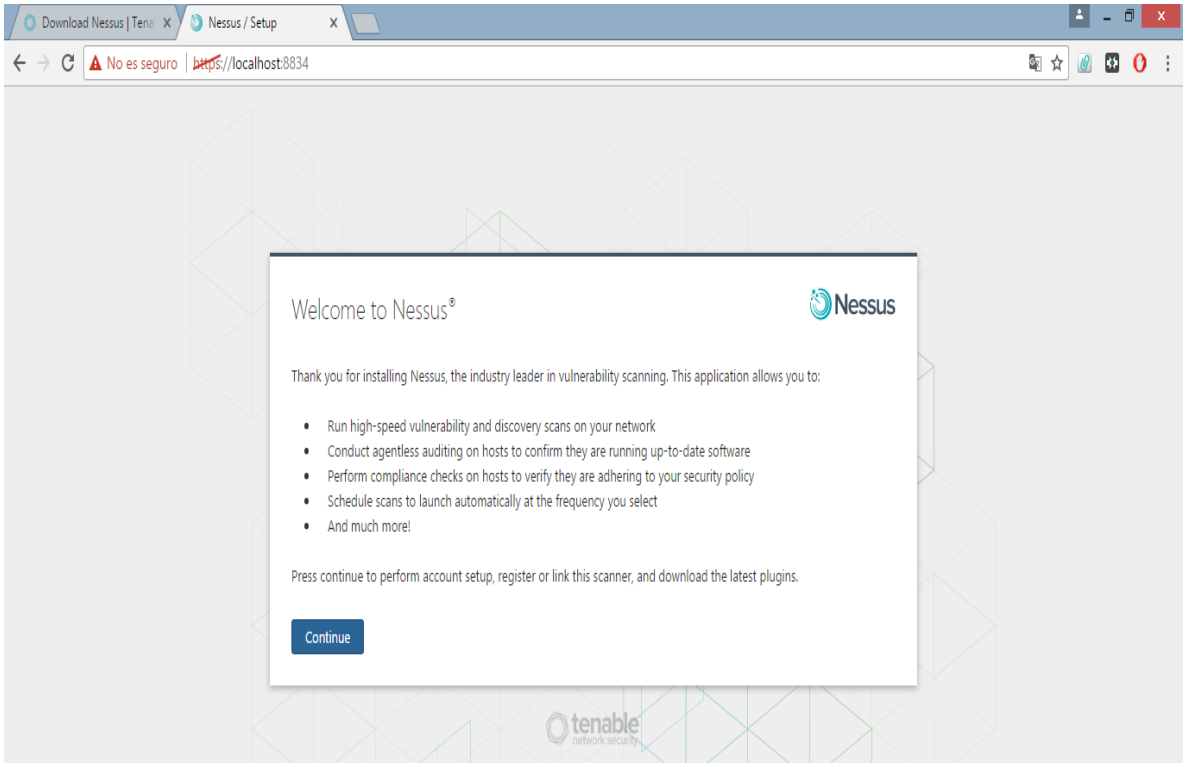
Dar clic en Install para iniciar la instalación.



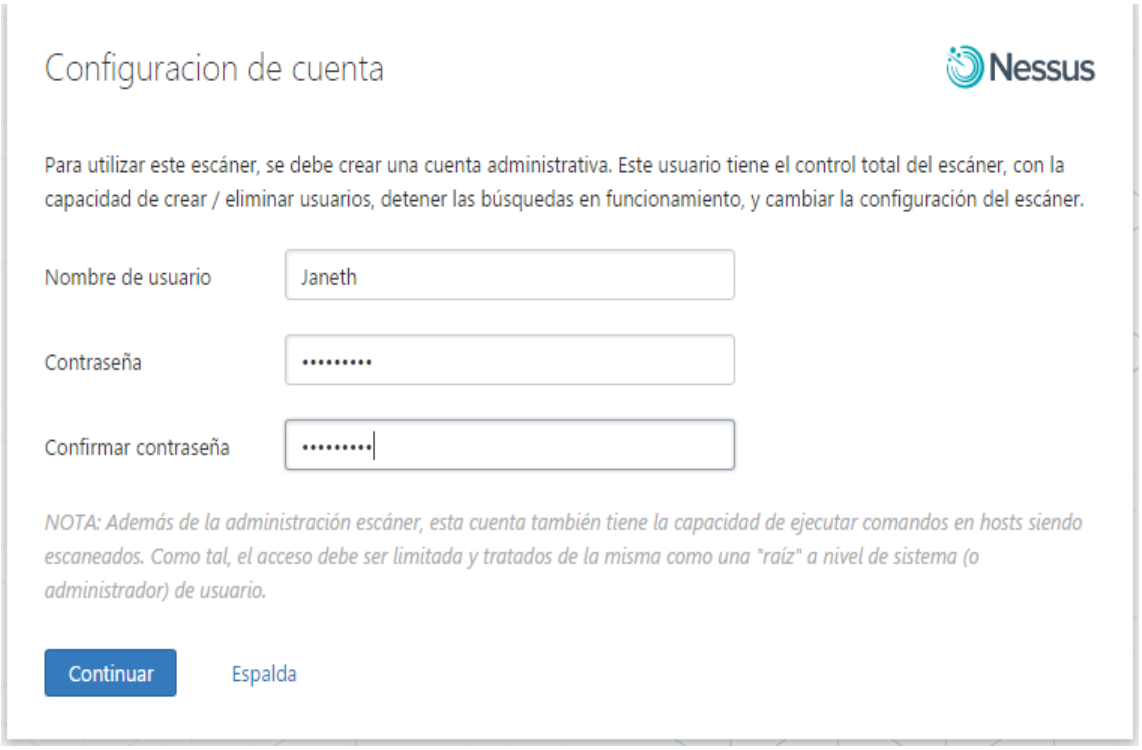
Finalizada la instalación se abrirá automáticamente una página en el navegador, dar clic en el apartado clicking here.



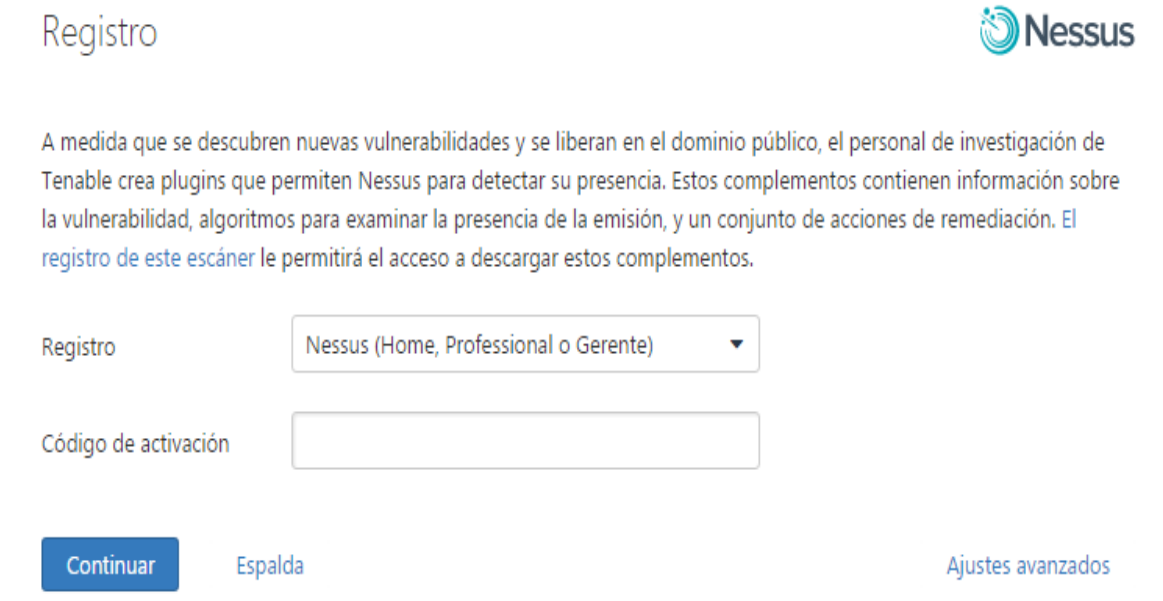
Despues dar clic en Continue.



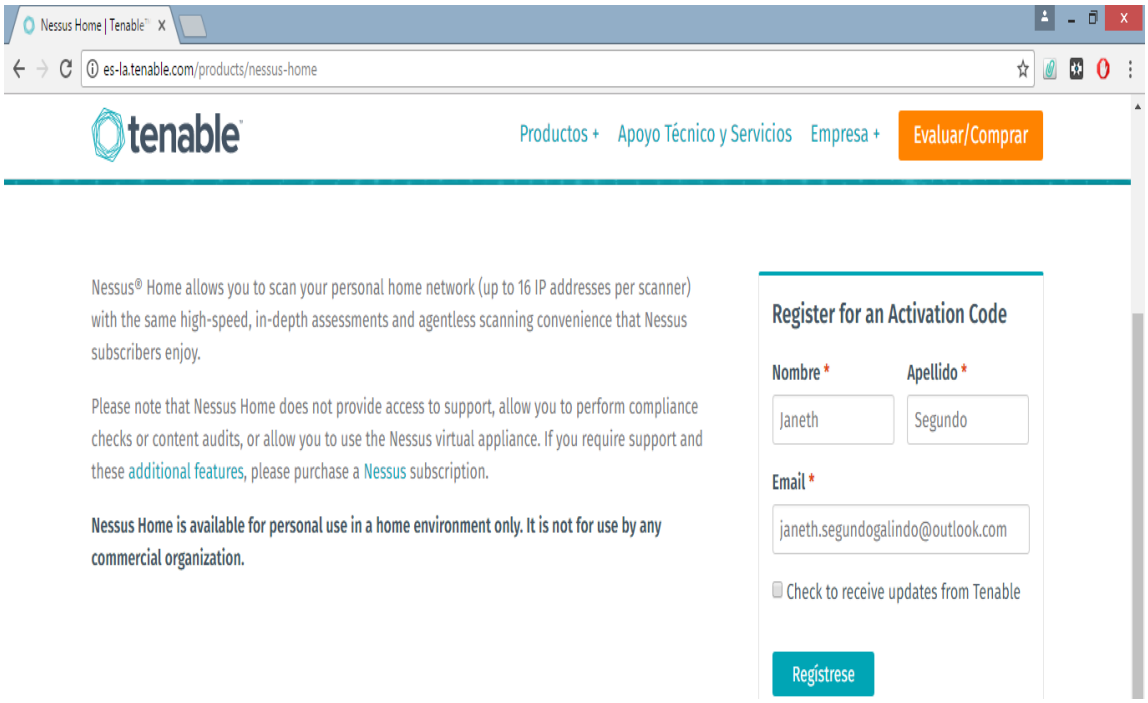
Se realiza la configuración de una cuenta de usuario. Se llena los datos que se solicitan que son el nombre, contraseña y confirmar contraseña y dar clic en continuar.



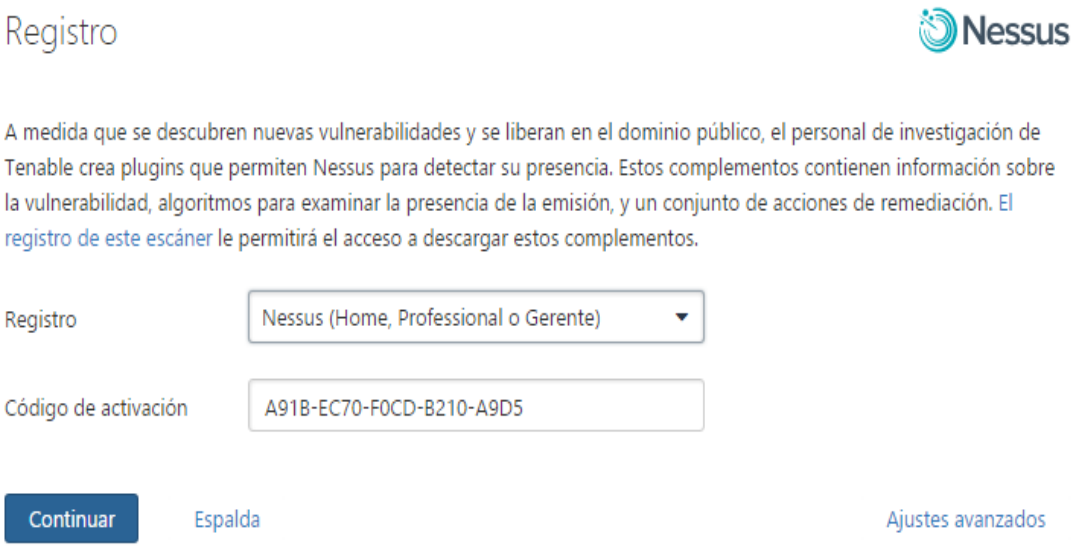
En este apartado se pide un código de activación para poder acceder a Nessus



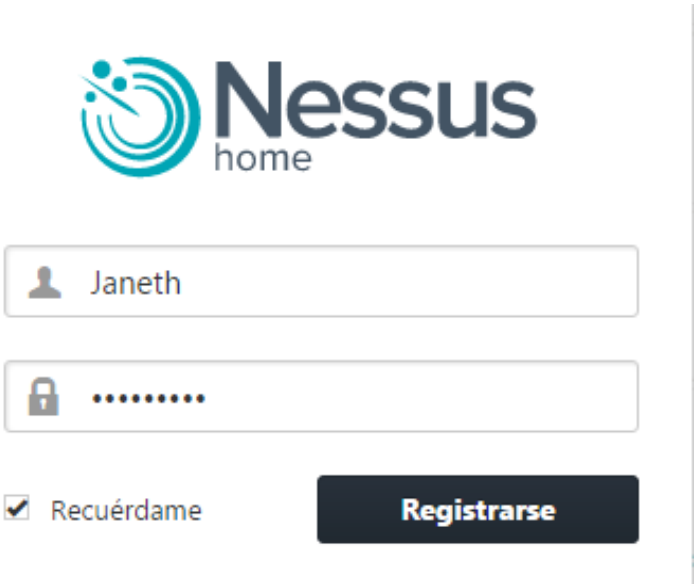
Para obtener el código de activación se debe acceder de nuevo a la página oficial de Nessus y seleccionar el apartado de obtener un código de activación, el cual despliega la siguiente ventana en el cual se debe de llenar los datos correspondientes para obtener un código y dar clic en registrese.



Despues del paso antriror automaticamente se debe de recibir el cogido de activacion, el cual se ingresa para realizar el registro correctamente y dar clic en continuar.



Luego se empezaran a descargar los plugins, al terminar el proceso, se pide que para ingresar a Nessus se debe de escribir el usuario, la contraseña y dar clic en Registrarse.



Y ahora ya se puede hacer uso de la herramienta Nessus para el escaneo de vulnerabilidades.