ESTUDIO MONOGRAFICO: VULNERABILIDADES EN REDES DE INTERNET ALAMBRICAS E INALAMBRICAS

ARLEY GUILLERMO RESTREPO ZULUAGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROYECTO DE SEGURIDAD INFORMÁTICA II
CEAD DOSQUEBRADAS
2018

ARLEY GUILLERMO RESTREPO ZULUAGA

Monografía para optar al título de
Especialista en Seguridad Informática

Asesor
Martín Camilo Cancelado
Docente Escuela ciencias básicas, tecnología e ingeniería
Universidad nacional abierta y a distancia

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

PROYECTO DE SEGURIDAD INFORMÁTICA II

CEAD DOSQUEBRADAS

2018

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Dosquebradas, 26 Julio de 2019

DEDICATORIA

A Dios y a mis padres

Dedico este trabajo primero a Dios por permitir la finalización de un nuevo ciclo en mi carrera profesional y por brindarme cada uno de los recursos disponibles para dar cumplimiento a cada una de las actividades propuestas.

Y a mis padres por el pilar fundamental en todo lo que soy, en mi vida, en mi educación, por el apoyo incondicional y por ser ese motor por el que cada día de vida seguiré luchando.

AGRADECIMIENTOS

A Dios

Por darme los medios y recursos necesarios para finalizar un logro más en mi vida profesional la cual me permitirá crecer y seguir creciendo a lo largo de mi carrera

A mis padres

Por ser el motor que cada día me impulsa a seguir adelante y a luchar con el fin de poderles dar un mejor futuro y calidad de vida, de igual forma agradecerles por ese apoyo incondicional en cada uno de los momentos y las etapas de frustración donde fueron pilares fundamentales para levantar la cabeza y continuar con este proceso.

A mis tutores

Por orientarnos y compartir sus conocimientos a través de cada una de las actividades realizando una retroalimentación asertiva con el fin de comprender y mejorar en cada uno de los procesos que se desarrollaron a lo largo de este proceso de formación.

A mis compañeros

Por el apoyo brindado en cada una de las etapas de este proceso de formación

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

El uso del internet ha impulsado el avance tecnológico a nivel mundial presentando su crecimiento mayor en los últimos años y llevando a un era de digitalización donde se es posible acceder a cualquier tipo de información sin importar el lugar físico o geográfico donde esta se encuentre, lo único que debe existir es una conexión a internet ya sea alámbrica o inalámbrica entre los dispositivos que contengan la información con el fin de poder consultar, modificar o incluso eliminar los datos que se deseen consultar.

El nacimiento del Internet se remonta a los años 1969[1] gracias a la búsqueda de un sistema que permitiera la comunicación rápida y efectiva entre los diferentes ordenadores que se encontraban conectados y que no necesariamente estén ubicados en el mismo lugar geográfico, con esto inicio la evolución de las conexiones a internet iniciando con tener conexiones cableadas con grandes estructuras y finalmente llegando a las conexiones inalámbricas que hoy día nos brindan movilidad y funcionalidad a la hora de buscar una alternativa para realizar una conexión a internet.

De acuerdo a lo anterior el Internet se ha convertido en una herramienta fundamental para las organizaciones actuales permitiendo el procesamiento de los datos y la consolidación de la información de una forma mucho más sencilla ágil ayudando a la toma de decisiones en tiempo real y contando con un canal de comunicación que va permitir el intercambio de información entre cada una de sedes o entre cada una de sus áreas facilitando y ganando tiempo y recursos que pueden llegar a ser invertidos en otro tipo de proyectos; actualmente el uso de las

[1]Internet nació de un proyecto militar y hoy es parte esencial de la vida diaria. El Espectador. [En Línea]: Colombia. Disponible en: https://www.elespectador.com/noticias/actualidad/articulo-internet-nacio-de-un-proyecto-militar-y-hoy-parte-esencial-de-vida-diar

conexiones a internet no solamente es usado en empresas pues esta evolución también ha tomado fuerza en hogares gracias a la gran cantidad de aplicaciones que ha traído la evolución y facilidad de acceso al internet y es así como actualmente la mayoría de los dispositivos que se adquieren en el mercado cuentan con una conexiona a internet haciendo mucho más fácil el acceso a las aplicaciones que a su vez han venido evolucionando gracias a la facilidad que brinda el internet para que el usuario final tenga acceso a ellas.

Precisamente es el crecimiento en el uso de internet a nivel mundial y la gran variedad de contenidos que este permite compartir a través de él lo que también permite que la seguridad en este tipo de conexiones se vea vulnerada dejando expuesta la información personal de miles de usuarios a nivel mundial y lo que ha hecho posible que la información de un gran número de organizaciones se vea vulnerada por causa de una conexión a internet no segura.

Teniendo en cuenta lo anterior y que gracias a los sistemas de información y a la evolución de las tecnologías los datos se han convertido en un activo de mucho valor para las organizaciones actuales y que debe permanecer de forma segura en el tiempo se hace necesario establecer parámetros de seguridad en cada una de las conexiones a la red que se construyan en las organizaciones ya sea que se hable de una red alámbrica o de una red inalámbrica y así mismo establecer una políticas de uso interno de los recursos informativos otorgados en las empresa para realizar las labores cotidianas de cada área, teniendo presente a qué tipo de información se puede tener acceso y que tipo de información es la que realmente debo proteger; este tipo de recomendaciones también es de suma importancia tenerlo en cuanto al uso de dispositivos móviles persónales pues hoy en día se comparte información en redes sociales que pueden llegar a comprometer nuestros nombres o activos de información.

INTRODUCCION

Este estudio monográfico tiene plasmada la evolución de las redes como canal principal para la comunicación y transmisión de datos a nivel mundial siendo hoy el más utilizado y permitiendo a las organización minimizar tiempo y costos a la hora de consultar, compartir, editar y consolidar su información en la cual se encuentra representada gran parte de las actividades y resultados de los servicios que cada una de ellas presta; es así como se mencionan los diferente tipos de conexiones y redes que han existido a lo largo de la evolución de este canal principal de comunicación y nos situamos en cuales los que actualmente tiene mayor uso a nivel de organizaciones y empresas que usan esto como una herramienta fundamental para su Core de negocio o funcionamiento.

Este estudio monográfico cuenta con un objetivo general y cuatro objetivos específicos que se desarrollaron en los tiempos establecidos en el cronograma de trabajo; el objetivo principal se centró en investigar cuáles son las vulnerabilidades más comunes en las redes de internet ya sean alámbricas o inalámbricas con el fin de poder ofrecer una guía de referencia que sirva para establecer medidas y conocer cuáles son esas puertas de seguridad trasera a las que le debemos poner atención en nuestras redes de datos ya sean domésticas o empresariales con el fin de mantener de forma la información a nivel de organización o a nivel de personas.

Los objetivos específicos abarcan los conceptos de red y tipologías de red más utilizada en la actualidad, así mismo se hace un análisis de aquellos ataquen que se han presentado a lo largo de la historia y de que formas pueden llegar a ocurrir estos; así mismo se centra en profundizar posibles soluciones y medidas de seguridad todo con el fin de servir como referencia de prevención y poder mantener la información de forma segura, integra y disponible.

OBJETIVO GENERAL

Realizar un estudio monográfico sobre las vulnerabilidades en redes de telecomunicaciones alámbricas e inalámbricas

OBJETIVOS ESPECIFICOS

1. Realizar un estudio e identificar aspectos generales sobre redes y sus protocolos de acuerdo los tipos de conexión alámbricos e inalámbricos

2. Analizar e identificar sobre las vulnerabilidades más aprovechadas por los ciberdelincuentes para generar ciberataques en organizaciones y usuarios finales

3. Elaborar una guía de referencia donde se establezcan parámetros generales de seguridad en la implementación de una conexión de red segura

4. Realizar un estudio sobres las tendencias en seguridad para la implementación de redes de telecomunicaciones seguras e inalámbricas

PLANTEAMIENTO DEL PROBLEMA

Actualmente el internet tiene un número de usuarios que supera las tres terceras partes de la población mundial[2] , de acuerdo a esta información es importante aclarar que la cantidad de datos que se transmite por segundo desde cada uno de los dispositivos que se encuentran conectados a una red de internet sea alámbrica o inalámbrica es muy alta, y si aparte de eso se va un poco más allá y se analiza que tipo de información es la que están procesando los usuarios o las terminales que están conectadas a la red nos encontraríamos una gran variedad de contenidos o de actividades que cada uno de ellos procesa y muy seguramente irán desde escuchar música o ver videos online, realizar consultas sencillas en alguno de los buscadores web existentes o quizás realizar búsquedas en redes sociales o publicar algún tipo de información de interés en alguno de los miles de portales que están abiertos solo con tener disponible una conexión a internet en nuestros dispositivos; pero que pasa con aquellos usuarios que van un poco más allá y aprovechan o utilizan sus conexiones a internet para realizar transacciones bancarias, acceso a cuentas de correo corporativas de organizaciones a nivel mundial, realizar transacciones de mercadeo electrónica entre o sin fin de actividades en los cuales nuestra información confidencial puede llegar a verse vulnerada por alguno de los intrusos o hackers que están en la red esperando que los usuarios caigan en las trampas.

De acuerdo a lo anterior y gracias a la facilidad que el internet cada día va ofreciendo a los usuarios para realizar cualquier tipo de transacción se deben pensar en implementar sistemas de red que sean seguros y que sean capaz de soportar los ataques que son enviados por los hackers a través de la red valiéndose de la misma evolución y alcance otorgado por las redes llegando a encontrar técnicas y así

[2]Susana Galeano. El número de usuarios de internet en el mundo supera el 50% de la población. Disponible en : https://marketing4ecommerce.net/usuarios-internet-mundo-2017/

enviar trampas a los usuarios incautos que posiblemente van a caer en unas de los tantos intentos que se envían al día logrando así capturar información personal como claves bancarias, acceso a aplicaciones corporativas, claves de correo electrónico incluso usuarios con altos privilegios para moverse en la red interna de la organización y así lograr consultar, modificar o incluso eliminar información de vital importancia para cada empresa según sea su caso.

Es así como el internet hace que muchos de los servicios que anteriormente eran costoso y demorados para generarse hoy en día se automaticen a través de aplicaciones o de herramientas web que realizan este tipo de trabajos de una forma ágil brindando facilidad y ahorrando tiempo al usuarios final pero es importante tener en cuenta un tema que actualmente pasamos por alto y es la seguridad e integridad de los datos con el fin de determinar o de evaluar si realmente nuestra conexión redes a nivel organizacional realmente si están protegidas o si cuento con las políticas internas tanto a nivel físico como a nivel estructural para crear un ambiente de navegación seguro en nuestros o si realmente se ha invertido el tiempo y recursos necesarios para llegar analizar que vulnerabilidades pueden llegar a presentarse en una máquina con el fin de poder dar soluciones a esos agujeros de seguridad y así estar tranquilo porque la información que estoy compartiendo está realmente protegida y no está quedando expuesta a ser modificada a borrada por terceros.

Y es que la seguridad en las conexiones a internet no era un tema al cual se le prestara mucha importancia hasta que los hackers más o menos entre los años 2005 a 2012 realizaron robos masivos de datos de cuenta bancarias por lo menos a 160 millones de clientes, así mismo Adobe admitió ser víctima de un robo de cuentas bancarias a gran escala[3] ; una vez conocidos este tipo de ataques y

3 Los seis mayores ciberataques de la historia. History. [En Línea]: Disponible en: https://mx.tuhistory.com/noticias/los-seis-mayores-ciberataques-de-la-historia

teniendo en cuenta que los hackers eran capaces de realizar ataques significativos en los cuales se viera afectada la información de las organizaciones o incluso llegar a secuestrar los datos de cierta organización con el fin de impedir su funcionamiento y viéndose obligada a pagar una cantidad de dinero con el fin de recuperar estos, en pocas palabras un ciber secuestro de la información que ha tenido su mayor auge en los últimos tres años donde se ha visto vulnerada la seguridad de las conexiones a internet de organizaciones a nivel mundial dejándolas sin información para continuar con su actividad.

Teniendo en cuenta los sucesos mencionados en el párrafo anterior y la evolución que presentan los medios de comunicación y las redes a nivel mundial y el provecho que los ciberdelincuentes están sacando de ellos por el gran volumen de información que se procesa por estos canales, vale la pena preguntarnos ¿Cuáles son las principales vulnerabilidades que se deben analizar para tener una conexión segura en redes alámbricas e inalámbricas?

Si bien es cierto que una conexión de red 100% segura no existe, en la actualidad hay herramientas y métodos que se pueden aplicar con el fin de que nuestras conexiones sean mucho más seguras; así mismo se cuenta con variedad de dispositivos que con una parametrización adecuada se puede ayudar a crear un escudo en nuestra infraestructura y de esta forma poder asegurar la información que a diario procesamos a través de las conexiones a Internet.

JUSTIFICACIÓN

La seguridad en una red es la confianza que se tiene para realizar un intercambio de información en el cual el riesgo a que la información que se está procesando sea vulnerada o robado debe ser el mínimo[4], esto con el fin de que los recursos de los usuarios y de las organizaciones estén protegidos y salvaguardados de los piratas informáticos que gracias a la evolución y al incremento del uso de internet se aprovechan para analizar y encontrar agujeros de seguridad en las aplicaciones o plataformas que comúnmente se utilizan para navegar en la web o para el procesar los datos correspondientes a la actividad desempeñada por las organizaciones y es así como fácilmente pueden llegar a capturar desde usuarios y contraseñas de redes sociales hasta los datos de cuentas bancarias mediante lo cual el usuario final se vería gravemente; es de ahí donde nace la importancia de tener una conexión a internet segura sin importar el tipo de red mediante el cual se realice la conexión es decir de forma alámbrica o inalámbrica.

En vista del crecimiento de los ataques de ciberseguridad que se han presentado en los últimos años[5], en los cuales organizaciones a nivel mundial se han visto afectadas de forma tal que han tenido que realizar un alto en transcurso normal de sus actividades debido al robo o perdida de la información y que así mismo ha incrementado el uso de técnicas por parte de los hackers con el fin de poder llegar a capturar información proveniente de usuarios del corriente a través de la creación de plataformas falsas y del uso de herramientas que lo que hacen es instalarse en nuestras máquinas con el fin de capturar cada uno de los movimientos y actividades realizadas por los usuarios finales o en ocasiones pueden llegar a obtener el control remoto de nuestras máquinas logrando así obtener datos de suma importancia a

[4]Certsuperior. Seguridad en Redes. [En Línea]. Disponible en: https://www.certsuperior.com/SeguridadenRedes.aspx

[5] El Tiempo. Aumentan los ciberataques para robar dinero a escala mundial. (2018, 05 de Marzo). [En Línea]. Disponible en: http://www.eltiempo.com/tecnosfera/videojuegos/entrevista-a-alejandro-gonzalez-y-a-jairo-nieto-creadores-de-estudio-de-videojuegos-colombiano-222336

través de los cuales pueden lograr a tener acceso a las plataformas informáticas de organizaciones o de usuarios finales que van a ser afectados por el plagio de dicha información.

A todo lo anterior se suma que actualmente la mayoría de las organizaciones cuenta con un sistema de información en el cual se procesa y almacena toda la información vital para su funcionamiento lo cual convierte este tipo de información en un activo de alto valor para la organización el cual se debe conservar de forma segura, así mismo debe permanecer integro en el tiempo y al mismo tiempo puede ser consultado en cualquier momento y desde cualquier lugar; pero así mismo este tipo de activos lo que hace es llevar a los hackers a que se inventen nuevas técnicas de ataques y posibles herramientas con el fin vulnerar la seguridad de las redes con el único objetivo de poder robar o dañar la información precisamente de ahí surge la necesidad e importancia de que hoy día se dedique tiempo a crear redes e infraestructuras que nos permitan tener una conexión a internet segura, realizar una a adecuada parametrización a las redes y así mismo establecer políticas y herramientas que nos ayuden a mantener nuestra información protegida o mitigar los impactos que puede llegar a causar un robo de información

MARCO TEORICO

MARCO CONCEPTUAL

El primer protocolo de comunicación entre ordenadores se remonta a los 1969[6] en plena guerra mundial donde por medio de un proyecto militar se busca establecer o encontrar un método o modelo de comunicación que fuera capaz de resistir ataques nucleares y que asegurara la información transmitida entre las tropas para esta época su nombre era ARPANET y que se encargaría de dar inicio a uno de los métodos de comunicación más utilizado a lo largo de todos los tiempos; pues actualmente es el más utilizado; luego en 1971 se envía el primer email y el 30 de Abril de 1993 nace lo que actualmente conocemos como internet o World Wide Web teniendo un crecimiento acelerado en los próximos años pero que se vio frenado en el año 2000 debido a que está conformado por miles de compañías que solo eran portales sin nada diferente que ofrecer y que no tenían ningún plan de sostenimiento y es así como se da el cierre de muchas de están compañías que ofrecían contenidos web; pero poco después llega el renacimiento de internet acompañado del término web 2.0 la cual da un mirada y perspectiva diferente a la web integrándola con comunidades de usuarios de todo el mundo y ofreciendo servicios enfocados a redes sociales, blogs, bibliotecas de consulta y otro tipo de contenidos suministrados y que eran de gran interés para el público; es después del renacimiento del internet donde se inicia la masificación de la revolución digital a nivel de organizaciones y empresas que empieza a evolucionar en las tecnologías utilizadas para el procesamiento de los datos haciendo que todos sus procesos se vayan optimizando y ganando tiempo en las comunicaciones que habitualmente manejaban logrando un mejor nivel de productividad.

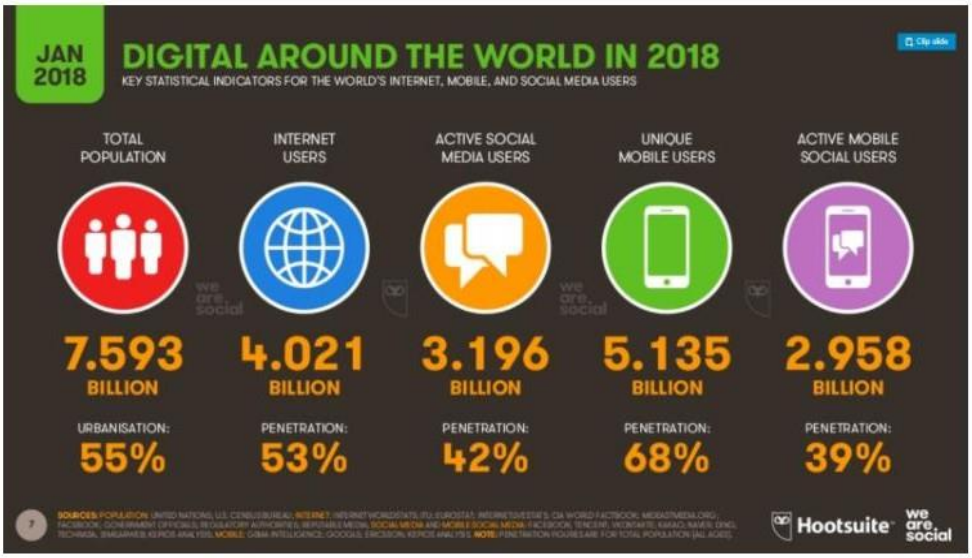
Según el informe presentado en el 2018 por la organización We Are Social y

[6]Internet nació de un proyecto militar y hoy es parte esencial de la vida diaria. El Espectador. [En Línea]: Colombia. Disponible en: https://www.elespectador.com/noticias/actualidad/articulo-internet-nacio-de-un-proyecto-militar-y-hoy-parte-esencial-de-vida-diar

[7]Susana Galeano. Febrero 2018. El número de usuarios de internet en el mundo supera el 50% de la población: 4000 millones (2018). [En Línea]. Disponible en: https://marketing4ecommerce.net/usuarios-internet-mundo-2017/

Hootsuite[7] a cerca de las tendencias y el número de usuarios que habitualmente se conectan a internet encontramos que actualmente en el mundo hay alrededor de 7.593 habitantes y que de este número el 53% de la población mundial ya son usuarios activos lo cual representa un crecimiento acelerado el uso de la red a nivel mundial.

Figura 1: Digital A round The World In 2018



Fuente: https://marketing4ecommerce.net/usuarios-internet-mundo-2017/

Precisamente es el uso del internet el que nos ha llevado a buscar formas y métodos de conectarnos a él en función de compartir y consultar todo el contenido existente en la red encontrándonos con las diferentes opciones que actualmente tenemos para lograr una conexión a internet; pero el problema que se tiene no es como me conecto a internet si no que tanta seguridad tengo en mi red con el fin de mantener la información segura y que los datos que yo transfiera entre ellos pueda mantenerse segura e integra.

Las formas de conectarse a una red han evolucionado con el paso de los años

gracias al creciente avance que proporcionó el uso de las tecnologías a nivel mundial creando la necesidad de generar formas de conectar varios ordenadores entre sí para que de esta forma puedan compartir y consultar contenido en la web; para realizar estas conexiones existen a lo largo del tiempo se han presentado diferentes tipos de conexión donde su mayor auge se ve reflejado con el nacimiento de las conexiones que se realizan a través de líneas telefónicas o ADSL, luego se dio una evolución y se pasó a las conexiones a través de redes cables mediante cableado coaxial, fibra óptica o incluso una combinación de las mismas proporcionando mayores niveles de velocidad para los usuarios, seguido surgen las conexiones inalámbricas que ayudan a la movilidad y portabilidad de la información, para luego dar un paso más y llegar a las conexiones a través de dispositivos móviles con las tecnológicas GMS,GPRS y 4G y finalmente llegar a las conexiones satelitales [8].

Figura 2: Tipos de Conexiones a Internet

https://www.econectia.com/blog/tipos-de-conexiones-a-internet-cual-te-conviene-mas

Con el fin de poder conectar uno más equipos se crea el concepto de red que en

[8]Econectia. Mayo 2017. Tipos de conexiones a Internet. ¿Cuál te conviene más? [En Línea]. Disponible en: https://www.econectia.com/blog/tipos-de-conexiones-a-internet-cual-te-conviene-mas.

términos de informática según el portal ecured.cu[9] hace referencia a un conjunto de equipos informáticos que se complementar mediante herramientas de software conectados en si mediante dispositivos físicos o inalámbricos con el fin de recibir y enviar impulsos eléctricos, ondas electromagnéticas o cualquier otro medio de transporte de datos para finalmente compartir información, recursos y ofrecer servicios a usuarios finales; las redes se clasifican teniendo en diferentes criterios o características relacionadas con el alcance, el tipo de conexión, relación funcional, topología o función entre otro tipos de generalidades pero este documento nos centraremos en las comunes y usadas de acuerdo al alcance y aplicabilidad en las organizaciones actuales.

Basándonos en el portal www.gadae.com[10] las redes que actualmente tiene mayor uso son:

RED DE ÀREA PERSONAL (PAN): Generalmente este tipo de red se utiliza para estructuras donde los dispositivos no superan una distancia mayor a los 100 metros pues están diseñadas para espacios reducidos y para conectar pocos equipos a ella.

RED DE ÀREA LOCAL (LAN): Este tipo de red es que más utilizados y generalmente el más instalado en las organizaciones incluso si se trata de un edificio completo ya que permite conectar ordenadores, impresoras, escáneres y muchos más dispositivos que requieran una conexión a internet para su funcionamiento con el fin de poder interactuar con los demás recursos o nodos conectados a ella, es capaz de abarcar desde 200 hasta 1 kilómetro.

RED DE ÀREA METROPOLITANA (MAN): Este tipo de red es capaz de abarcar espacios mucho más grandes a las anteriormente mencionadas su uso principal se

[9] Ecured.cu. Red de Computadores. [En Línea]. Disponible en: https://www.ecured.cu/Red_de_computadoras

[10] Samuel Juliá. Tipos de redes Informáticas según su alcance. [En Línea]. Disponible en: http://www.gadae.com/blog/tipos-de-redes-informaticas-segun-su-alcance/

da en las zonas wifi instaladas en grandes espacios mediante las administraciones públicas de las ciudades y así mismo abarca toda la infraestructura de cables de un operador de telecomuniciones.

RED DE ÀREA AMPLIA (WAN): Son las que suelen ser desplegadas por los proveedores de internet con el fin de poder cubrir las necesidades de red de un país o ciudad.

RED DE ÀREA LOCAL VIRTUAL (VLAN): Son redes interconectadas de forma lógica a través de protocolos o puertos con el fin de reducir el tráfico y mejorar la seguridad en la conexión y así mismo con el fin de generar redes segmentadas por áreas.

En el párrafo anterior se mencionan los tipos de conexiones de red que generalmente se utilizan pero para este trabajo monográfico nos enfocaremos en analizar las vulnerabilidades en las redes LAN ya que están son las que generalmente se utilizan en las organizaciones actuales con el fin de poder identificar cuáles cuales son los tipos de ataques más utilizados por los hackers para realizar ciber ataques y así mismo poder llegar a mitigar el impacto o disminuir el riesgo de que estos ocurran en una red LAN alámbrica o inalámbrico realizando una parametrización adecuada de los recursos y creando políticas que ayuden a mejorar la seguridad de los datos y de la red completa en general.

Si bien es cierto que el internet y las conexiones de red han facilitado el trabajo de las organizaciones actuales y del mundo general ya que se ha encargado de optimizar las comunicaciones y la transferencias de datos también es cierto que esta evolución también ha creado un problema en cual se debe pensar y dedicar tanto tiempo como recursos y es el de la seguridad de la información pues cuando se crea una red conectada a internet se está dejando la información de la compañía expuesta a todos a aquellos que tenga acceso a la web esto gracias a protocolos y servicios activos en los sistemas operativos que no son parametrizados de la forma

adecuada pueden llegar a convertirse en un dolor de cabeza y es ese punto al cual se desea llegar; poder identificar cuáles son aquellos puntos vulnerables de los sistemas operativos y del hardware utilizado para realizar conexiones de red los cuales tienen relación con puertos, servicios, protocolos de conexión entre otros y los cuales son ya muy bien conocidos por los piratas informáticos con el fin de poder vulnerar la seguridad de una red interna en una organización con el fin de robar, modificar o consultar información que es considerada como confidencial para una empresa.

¿Qué es una vulnerabilidad? [11]; enfocando el termino vulnerabilidad en la seguridad informática se hace referencia a una debilidad de un sistema informático o una conexión el cual puede ser utilizado y causar daño; la debilidad se puede llegar a presentar en cualquier parte de la red es decir puede presentarse en una computadora, en un servidor, en uno de los router o en el mismo firewall; es decir que las vulnerabilidades en las organizaciones se deben contemplar tanto en el hardware como el software utilizado; una vez se identifica la vulnerabilidad nace una amenaza que enfocada en seguridad informática es una circunstancia que tiene un potencial para causar daño o perdida materializando un ataque en uno de los dispositivos que componen la red y finalmente se tiene un riesgo de que esa amenaza se materialice teniendo una probabilidad alta o baja de acuerdo a las medidas que se tomen una vez se identifiquen las partes vulnerables en la red.

Una vulnerabilidad puede llegar a presentarse tanto a nivel de hardware como a nivel de software[12]:

[11] Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. [En Línea]. Disponible en: https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo
[12] Diego Mesia. Vulnerabilidad de Seguridad. [En Línea]. Disponible en: http://diegomesia.com/vulnerabilidad-de-seguridad/

VULNERABILIDADES EN EL SOFTWARE: Generalmente los fabricantes de software realizan grandes esfuerzos por cerrar puertas traseras o brechas de seguridad que puedan llegar a comprometer la seguridad de los usuarios sin embargo es difícil logran un 100% en la seguridad es así como las aplicaciones o sistemas operativos presentan errores que se pueden convertir en vulnerabilidades y ser aprovechas para obtener acceso no autorizados a las redes.

VULNERABILIDADES EN EL HARDWARE: Este tipo de vulnerabilidades se pueden clasificar en dos tipos, una en vulnerabilidades que viene desde la fabricación del hardware el otro es enfocado al tema de la parametrización que se da a dichos dispositivos, aunque en este caso iría muy ligado a los fallos del software.

Entre los ataques a los cuales se encuentran expuestas las redes alámbricas e inalámbricas en la actualizad se pueden clasificar de acuerdo al tipo de ataque y entre ellos se encuentra ataques a través de software maliciosos o malware mediante internet cuyo fin es crear códigos maliciosos e introducirlos en páginas comúnmente visitadas por los usuarios e infectarse en ocasiones sin darse cuenta, este tipo de ataques tiene tres divisiones y son los virusa, gusanos y troyanos; también están los ataques a servidores y a infraestructuras de red cuyo objetivo es enviar tanta información como se pueda a un servidor o servicio con el fin de colapsarlo dejándolo así sin la posibilidad de responder a las peticiones legitimas de los usuarios, este tipo de ataques no solo se presenta en servidores web sino también en servidores de correo y servidores DNS entre otros. Cuando se presenta un ataque de denegación de servicio puede darse porque se presente una inundación de conexiones, se colapse el ancho de banda o se proceda a realizar un ataque directo sobre alguna de las vulnerabilidades identificadas en el servidor.

Otro de los ataques que se puede llegar a presentar es el análisis de paquetes que recorren la red o SNIFFERS que hacen referencia a un analizador de paquetes de

red con el cual se puede realizar un escaneo de todos los datos que son transmitidos a través de la red y a través de ellos obtener información que puede ser utilizada para afectar la seguridad de la organización; este tipo de ataques puede llegar a presentarse tanto en redes alámbricas como inalámbricas.

La suplantación de identidad es otro de los ataques pueden presentarse esto hace referencia a la suplantación de las direcciones ip y así realizar inyección de paquetes falsos a la red; así mismo la modificación y borrado de datos enviados puede ser otro de los ataques generados aprovechándose de las vulnerabilidades de la red este consiste en escanear los datos que circulan por red y adicional a esto puede llegar a modificar, eliminar o crear contenido malicioso e inyectarlo en la red[13].

[13] Sergio De Luz. Noviembre 2010. Ataques a las redes: Listado de diferentes ataques a las redes de ordenadores. [En Línea]. Disponible en: https://www.redeszone.net/2010/11/03/ataques-a-las-redes-listado-de-diferentes-ataques-a-las-redes-de-ordenadores/

ACTIVIDADES A DESARROLLAR

Con el fin de dar cumplimiento a los objetivos específicos lo primero que se debe realizar es estudio utilizando referencias bibliográficas validas que estén enfocadas a las conexión de internet alámbricas e inalámbricas y que su tema principal sea el de la seguridad en redes y sus principales vulnerabilidades conocidas hasta hoy, este debe ser un análisis profundo donde se iniciara estudiando principalmente la seguridad en redes internas que habitualmente están configuradas en las organizaciones con el fin de proveer conexiones entre todos sus dispositivos y poder de esta generar una red organizacional mediante la cual se comparta información, así mismo se debe segmentar los riesgos encontrados de acuerdo al tipo de conexión ya que puede ser una conexión cableada o una conexión inalámbrica.

Una vez se identifiquen los riesgos en las redes se debe crear una segmentación a nivel del tipo de vulnerabilidades pues en este caso se tiene vulnerabilidades de tipo hardware y otros de tipo software en los cuales se realizará una referencia de las principales puertas de acceso que se dejan abiertas en los dispositivos físicos y en los dispositivos de software ya que en la mayoría de las ocasiones se dejan con la configuración con que vienen por defecto.

Con el fin de realizar un sondeo parcial sobre qué tanta importancia se le da al tema de seguridad de la información en las organizaciones se realizará una recopilación de conceptos en máximo 10 empresas de la ciudad de Pereira y Dos quebradas con el fin de realizar un esquema parcial sobre qué medidas se están tomando con el fin de crear y mantener una red realmente segura.

Se realizará un estudio sobre los diferentes tipos de ataques a los que puede estar expuesta una red identificando sus principales fuentes de acción de ¿Cómo pueden presentarse?, ¿Cuáles son los medios más comunes de generar estos ataques? Y ¿Qué acciones se deben tener en cuenta a fin de que el riesgo de sufrirlos sea el mínimo?; crear así un documento que sirva como referencia bibliográfica para

implementar controles de seguridad en las redes internas sean cableadas e inalámbricas y ayudar a mejorar la seguridad de la información.

Finalmente se esperar realizar un estudio sobre las tendencias en el tema de seguridad informática, aunque se entiende que es un tema que está en constante avance si puede llegar a establecer aquellos parámetros que van a ser fundamentales en un futuro teniendo en cuenta los nuevos desarrollos tecnológicos y los nuevos productos de seguridad ofrecidas por los proveedores en cuanto a este tema.

CRONOGRAMA DE ACTIVIDAES

Tabla 1 : Cronograma de actividades

1. PLAN DE TRABAJO													
ACTIVIDAD		MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10	MES 11	MES 12
No	ANTEPROYECTO												
1	Selección y delimitación del tema			X									
2	Formulación del tema de investigación			X	X								
3	Planificación de las actividades			X	X								
4	Identificación de fuentes			X	X								
5	Portada												
6	Resumen			X	X								
7	Introducción			X	X								
8	Marco Teórico			X	X		X	X					
9	Desarrollo			X	X		X	X					
10	Realizar el estudio				X		X	X	X				
11	Conclusiones							X	X				
12	Bibliografía			X	X		X	X	X				
13	PROYECTO												
14	Plan de trabajo						X						
15	Recopilación de Información						X	X					
16	Tabulación de Información							X					
17	Resultados Obtenidos							X					
18	Redacción de ajustes en el informe final							X					
19	Entrega de PROYECTO							X	X				

DESARROLLO OBJETIVO

Realizar un estudio e identificar aspectos generales sobre redes y sus protocolos de acuerdo los tipos de conexión alámbricos e inalámbricos

El termino red es utilizado desde hace muchos años atrás incluso antes del nacimiento de lo que hoy en día conocemos con como internet; es así como el concepto de red con el propósito de abarcar un área amplia que pudiera establecer comunicaciones de forma estable a lo largo de un territorio nacional, se produce en Suecia y Francia a principio del siglo XIX. Lo anterior se reconocía como un telégrafo óptico que consistía en una serie de torres que tenían una seria de brazos similares a las persianas los cuales se encargaban de codificar la información que transmitía la torre anterior usándose hasta mediados del siglo XIX cuando tiene su nacimiento el telégrafo.

Cada una de las torres que componían la red tenían que estar ubicadas a determinada distancia con el fin de ir transmitiendo la información de una en una hasta llegar a su lugar de destino; poco tiempo después se inicia la evolución de este tipo de redes y surgen así las redes telefónicas convirtiéndose en los medios principales de comunicación y transmisión de datos a nivel mundial; dando nacimiento al primer red telefónica en Boston, teniendo uno de sus mayores éxitos cuando se pudo lograr comunicación con algunos doctores de la zona para brindar ayudar tras el choque de dos trenes de la época y así conseguir que estos llegaran de forma inmediata[14].

Con el nacimiento y contextualización del nacimiento de las primeras de redes de datos como canales de comunicación podes mencionar las redes de INTERNET que es la directamente responsable de que hoy en día este concepto este tan evolucionado y tan ampliamente utilizado a nivel mundial permitiendo que el mundo este interconectado desde cualquier parte del mundo sin importar su ubicación geográfica ; es así como Internet es hoy día catalogado como un amplio concepto

de comunicación que tiene su origen en la combinación de dos palabras provenientes del inglés, la primera es INTER (national) y NET (work) [14]; y que gracias a esto se define como una red informática que se compone de por un sistema de redes de comunicación interconectadas por una familia de protocolos TPC/IP permitiendo la comunicación a nivel mundial.

Según el portal informaticamilenium otra definición de internet o algunas veces llamado LA RED seria; sistema mundial de redes de computadoras, integrado por diferentes redes de cada país del mundo por medio del cual un usuario desde cualquier computador conectado en caso de contar con los permisos apropiados, tener acceso a información de otra computadora, y poder tener inclusive comunicación directa con otros usuarios en otras computadoras[15].

Con el fin de conocer el origen y nacimiento del internet como red de comunicación a nivel mundial cabe mencionar que este es un servicio cuyo éxito ha sobrepasado los límites iniciales para los cuales fue creado y es muy importante conocer y entender la diferencia entre INTERNET y WWW, pues Internet es el servicio que permite la comunicación bilateral mientras que la www es la agrupación de herramientas y protocolos que hacen posible el acceso remoto a información desde cualquier parte del mundo y que utiliza el internet como medio de transporte de los datos.

[14] Informática redes de computadores. Introducción a las redes de datos. Orígenes y Evolución. [En Línea]. Disponible en: https://sites.google.com/site/informaticaredesdecomputadoras/unidad-1-Introduccin-a-las-redes-de-datos/1-1-origenes-y-evolucion

1.1 ORIGEN DEL INTERNET[16]

El internet inicio su desarrollo con la fabricación de las primeras computadoras electrónicas en el año 1950 por la agencia de Proyectos de Investigación Avanzada (ARPA) y que recibió el apoyo de países como Estados Unidos, Reino Unido y Francia ejecutando así la conexión entre dos computadores físicos; en este año ARPA era una compañía militar y su único objetivo fue crear una forma de comunicación con el fin de poder defenderse de los ataques rusos.

Más adelante en 1969 se crea ARPANE, que era una red que se encargaba de conectar universidades, agencias gubernamentales y contratistas de defensa a nivel de todos los Estados Unidos con el objetivo de mejorar las comunicaciones cuya evaluación inicio de forma acelerada pues para los 70 ya contaba con casi 60 nodos interconectados.

A pesar de que la ARPANET solucionó una parte del problema para comunicación entre diferente sedes remotas, no era aplicable para los campos de batalla que era donde estaban los soldados y que era por quien inicialmente se creó dicha red; fue así como nacen las conexiones inalámbricas con el fin de permitir la transmisión de datos mediante Radio o Satélite; una vez se logra esto se crean conexiones de las redes inalámbricas a las red ARPANET con el fin de que las computadores sirvieran de manera remota recibiendo el nombre de internetworking que se define como la conexión de una red de ordenadores con otras redes a través de la utilización de un

[15] Informática Milenium. Internet. [En Línea]. Disponible en: https://www.informaticamilenium.com.mx/es/temas/que-es-internet.html
[16] Gestión. ¿Cuál es la historia del Internet? [En Línea]. Disponible en: https://gestion.pe/tecnologia/historia-internet-240094?ref=gesr

método común de encaminamiento de información de paquetes entre las redes [17]Es en el intento por conectar los computadores con las demás redes donde surgen el conjunto de protocolos de internet TCP/IP desarrollados por Robert E. Kahn y Vint Cerft que según el portal monografías estos protocolos son el conjunto de reglas establecidas entre dos dispositivos para permitir la comunicación entre ambos; y que gracias a estos protocolos empieza a funcionar la comunicación entre las redes inalámbricas y las redes alámbricas, esto fue en el año 1976, y convirtiéndose en un protocolo estándar para ARPANET en el año 1983.

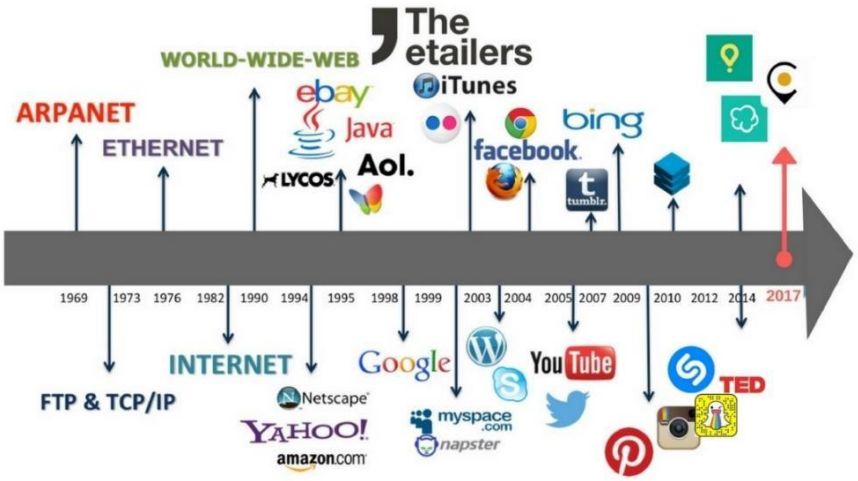
Para ese entonces la evolución ARPANET fue tan exitosa que inicio su expansión a nivel mundial y con ella se da el nacimiento de otras redes con fines específicos como es el caso de NSFNET cuya finalidad era promover la investigación avanzada, así mismo surgen redes dedicadas a las fuerzas armadas, a la educación entre otras y unas de carácter público y otras de carácter privado.

Para el año 1990 nace lo que hoy en día conocemos como la www que según el portal gestión es un sistema de distribución de documento de hipertexto o hipermedias interconectados y accesibles vía Internet, dando acceso a cualquier usuario de ver los archivos siempre y cuando cuente con los permisos requeridos para verlos.

Es así como Internet a lo largo de todos estos años ha venido en constante evolución con el fin de mejorar la comunicación y dar acceso de forma remota a contenidos que antes eran impensables; después del nacimiento de la www en los años 90 empiezan a nacer plataformas de gran importancia tales como Yahoo!, Amazon, google, MySpace, YouTube, Mozilla, twitter, y una gran variedad de redes de sociales que hoy día siguen en constante evolución gracias a la internet.

[17] Danny Kevin Reyes Quevedo. Internetworking. [En Línea]. Disponible en: https://www.monografias.com/docs110/internetworking/internetworking.shtml

Figura 3: Desarrollo Cronológico del Internet



Fuente: https://www.theetailers.com/internet-la-historia/

1.2 DEFINICIÓN DE RED INFORMATICA

La palabra red se define como la estructura que dispone de un patrón que la caracteriza, y por su parte el termino Informática hace referencia a los saberes de la ciencia que posibilitar el tratamiento de datos de manera automatizada a través de computadores u ordenadores; de acuerdo a lo anterior el termino de Red Informática según el portal definición. De es el conjunto de equipos entre ellos computadores, periféricos entre otros que están interconectados con el fin de permitir compartir diversos recursos; el hecho de compartir los recursos se hace posible a la interconexión de los equipos a través de dispositivos que permiten el envío y la recepción de ondas que se encargan de transportar los datos que se desean compartir[18]. Por su parte el portal asper.es define una Red Informática como dos o más ordenadores conectados entre sí con el fin de compartir recursos, ya se

[18] Definición. Definición de Red Informática. [En Línea]. Disponible en: https://definicion.de/red-informatica/

hardware o software; permitiendo así que varios usuarios puedan intercambiar información, pasar archivos, compartir periféricos y ejecutar programar instalados en ordenadores instalados en la red[19].

El nacimiento de las redes informáticos causó una revolución en las formas de comunicación y de transmisión de datos, brindando mayor facilidad en especial a las organizaciones que anteriormente debían realizar de forma manual la mayor parte de sus actividades diarias viéndose obligadas a invertir más tiempo y más recursos en procesos que con las redes y el interne se facilitaron en gran medida; si bien es cierto la evolución que tuvieron las compañías con el nacimiento de las redes no fue inmediato si se empezó a notar un notorio crecimiento en la eficiencia y en la recolección de información pues ya era mucho más fácil compartir y consolidad la información incluso acceder a ella desde sitios remotos lo cual ahorra recursos y tiempo para implementar en mejoras de procesos internos dentro la compañía; de acuerdo a lo anterior se pueden mencionar algunos de los beneficios que las redes informáticas trajeron al mundo :

- Poder conectarse a una red de Internet
- Poder compartir recursos entre los diferentes equipos conectados en la red; ya sean periféricos, software o documentos ofimáticos.
- Reducción de costos en transportes y envió de información de un lugar a otro.
- Crear una conexión que permite compartir y consultar archivos ubicados en cual lugar del mundo con tan solo un clic
- Permitir consolidar la información de organizaciones que cuentan con múltiples Sedes en diferentes lugares geográficos
- Optimización de procesos
- Disponibilidad de la información

[19] Apser.es. Las redes informáticas: qué son, tipos y topologías. [En Línea]. Disponible en: http://www.apser.es/blog/2015/06/20/las-redes-informaticas-que-son-tipos-topologias/

1.3 CLASIFICACIÓN DE REDES INFORMATICAS[20]

Una Red Informática puede llegar a clasificarse de acuerdo a su estructura o forma de transmisión; es por eso que en la actualidad existen las siguientes clasificaciones para los principales tipos de Redes de Informática:

- Redes por Alcance
- Redes por Tipo de Conexión
- Redes por Topología
- Redes por Direccionalidad
- Redes por Grado de Autenticación
- Redes por Grado de Difusión
- Redes por Servicio y Función

1.3.1 Redes Por Alcance

[21] Cuando hacemos referencia a redes por alcance nos estamos enfocando en aquellos tipos de redes que abarcan o comprenden un área determina en una posición geográfica y que son clasificadas de acuerdo al alcance o la capacidad de área que cada una de ellas pueda abarcar; de acuerdo a lo anterior las redes por alcance están clasificadas así:

- PAN: Personal Area Network
- LAN: Local Area Network
- CAM: Campus Area Network
- MAN: Metropolitan Área Network

[20] @Gobierno TI. TIPOS DE REDES INFORMATICA. [En Línea]. Disponible en: https://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/

[21] @Gobierno TI. TIPOS DE REDES INFORMATICA. [En Línea]. Disponible en: https://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/

- VLAN: Virtual LAN
- SAN: Storage Área Network

1.3.2 Personal Area Network

De acuerdo con el instituto de Ingenieros Eléctricos y Electrónicos (IEEE por sus siglas en ingles de Institute of Electrical and Electronics Engineers), una rede área personal es una red capaz de soportar los segmentes de 33 pies o más longitud. Una red PAN puede ser utilizada para conectar dispositivos personales como teléfonos celulares, auriculares y asistentes digitales personales entre sí a otros dispositivos autónomos y redes más grandes sin necesidad de cables[22].

1.3.3 Redes por Tipo de Conexión

Las redes por tipo de conexión varían de acuerdo a como se realice la transmisión de datos es decir si se realiza por medios guiados en el caso de que se use una conexión por cable ya sea cable coaxial, par trenzado o una fibra óptica; o si la conexión se realiza por un medio de transmisión inalámbrico ya sea onda de radio, infrarrojos, microondas u otro tipo de transmisiones de tipo inalámbrico.

Entre los tipos de PAN más utilizadas se encuentra

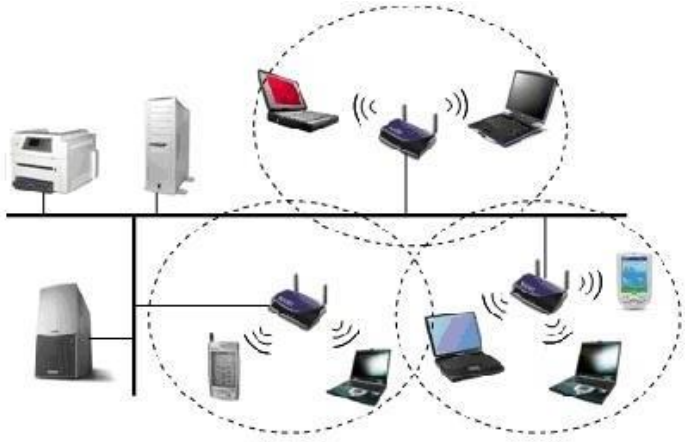
- Bluetooth: Muchas de las redes PAN se basan en conexiones a través de bluetooth, tecnología inalámbrica de corto alcance, inventada por la compañía Sueca Ericsson en el año 1994.La conexión a través de este tipo de dispositivos se hace posible gracias a un chip pequeño de computadora con una radio Bluetooth y el software que les permite conectarse a otros dispositivos mediante ondas de radio. Un dispositivo bluetooth puede conectar hasta otros siete dispositivos

[22] David Dunning. ¿Qué es una red PAN? [En Línea]. Disponible en: https://techlandia.com/red-pan-info_261597/

para formar una PAN, técnicamente conocida como Piconet. Una ventaja que tiene la conexión a través bluetooth es que consumo de energía es bajo y es óptimo para dispositivos portátiles.

- Infrarrojo: Esta es una tecnología que se conecta a través de radiación con longitudes de ondas comprendidas entre 1 y 100 micrones tiene un alcance corto, pero un bajo consumo y bajo costo. Una gran desventaja que tiene esta tecnología es que requiere un punto de visión directa entre los dispositivos de una PAN para poder realizar una conexión efectiva.
- Wifi: Las redes wifi también pueden llegar a ser consideradas redes PAN aunque están tienen su mayor usabilidad en redes LAN y WAN.

Figura 4: Redes por Tipo de Conexión



Fuente: https://gobiernoti.files.wordpress.com/2011/07/wlan1.jpg

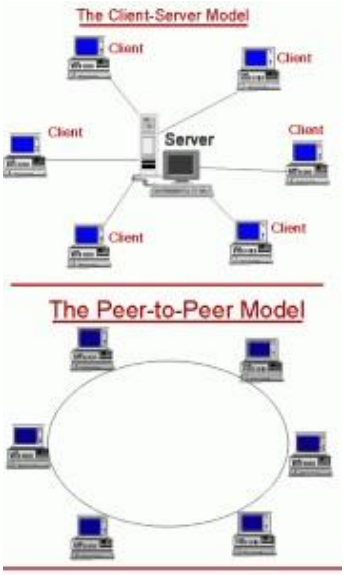
1.3.4 Redes por Relación Funcional

[23]Las redes por relación funcional abarcan aquellas redes donde hay una relación

[23] @Gobierno TI. TIPOS DE REDES INFORMATICA. [En Línea]. Disponible en: https://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/

dirección entre mi red y otras redes; inmerso en esta clasificación podemos encontrar las redes de tipo Cliente/Servidor donde un todos los clientes están interconectados en relación a un dispositivo considerado como el servidor principal el cual se encarga de centralizar los recursos y aplicaciones disponibles para el uso de los clientes conectados a la red; también están incluidas las redes de tipo P2P (igual a igual), este tipo de redes no cuentan con un servidor principal sino que cada nodos pone a su disposición los servicios recursos para que pueden accederse desde otros nodos similares a él.

Figura 5: Redes por Relación Funcional

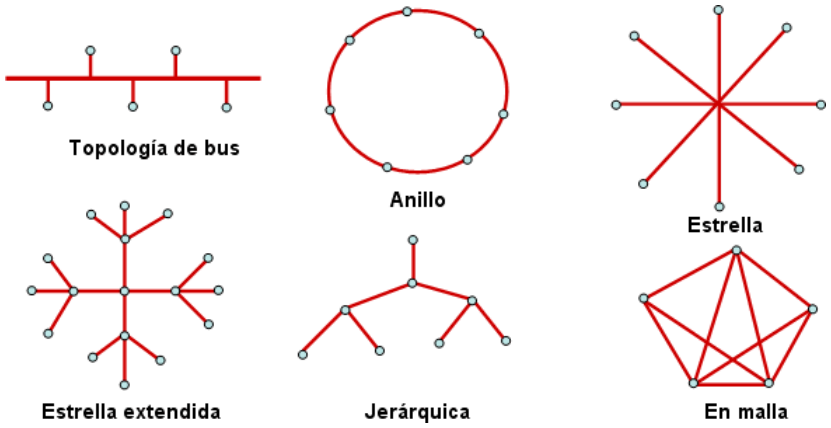


Fuente: https://gobiernoti.files.wordpress.com/2011/07/peer_to_peer111.gif

1.3.5 Redes por Topología

Este tipo de redes está establecido de acuerdo a la estructura mediante la cual se unen los diferentes nodos que la componen, estas a su vez se clasifican en topología en Bus, en Anillo, en Estrella, en Malla, en Árbol y Redes Mixtas.

Figura 6: Redes por Topología



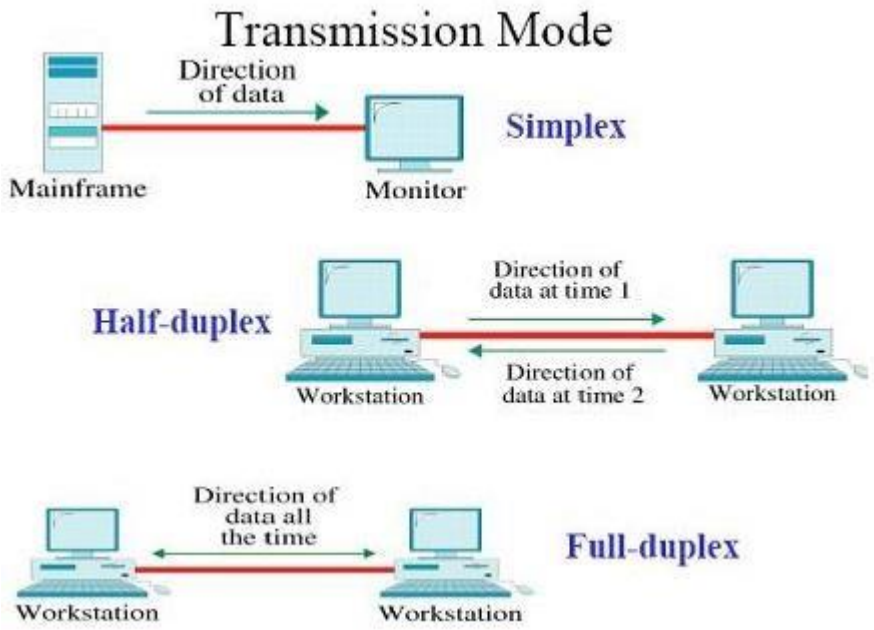
Fuente: https://gobiernoti.files.wordpress.com/2011/07/topologia-de-red1.gif

1.3.6 Redes por Direccionalidad de Datos

[24] Este tipo de redes es caracterizado por la dirección o ruta mediante la cual está dirigida o hacia donde esta apunta la información que se está emitiendo o decepcionando; es por eso que en ellas existe una clasificación que comprende los siguientes tipos; Simplex solo existe un emisor y emite información hacia una única dirección; Half-Duplex cuando la información es bidireccional pero solo un equipo está en la capacidad de transmitir a la vez y Full Dúplex cuando ambos equipos están en la capacidad de enviar y recibir información de forma simultánea.

Figura 7: Redes por Direccionalidad de Datos

[24] @Gobierno TI. TIPOS DE REDES INFORMATICA. [En Línea]. Disponible en: https://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/



Fuente: https://gobiernoti.files.wordpress.com/2011/07/simplexhalfduplexfullduplex.jpg

1.3.7 Redes Según Grado de Autenticación

[25] En esta clasificación se conocen las redes privadas y redes de acceso público; es así como una red privada requiere el ingreso de datos de autenticación u un medio de validación alterno para poder ingresar o conectarse a la red; mientras que una red de acceso público permite que los usuarios accedan a ella de forma libre.

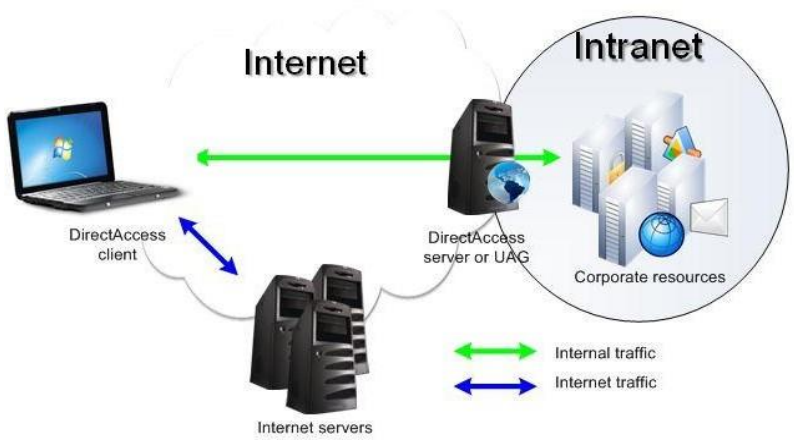
1.3.8 Según Grado de Difusión

Otra clasificación similar a la red por grado de autentificación, corresponde a la red por Grado de Difusión, pudiendo ser Intranet o Internet. Una intranet, es un conjunto de equipos que comparte información entre usuarios validados previamente, Internet en cambio, es una red de alcance mundial gracias a que la interconexión

[25] @Gobierno TI. TIPOS DE REDES INFORMATICA. [En Línea]. Disponible en: https://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/

de equipos funciona como una red lógica única, con lenguajes y protocolos de dominio abierto y heterogéneo

Figura 8: Redes Según Grado de Difusión



Fuente: https://gobiernoti.files.wordpress.com/2011/07/intranetvsinternet1.jpg

1.4 FORMAS DE CONEXIÓN A INTERNET

Como ya se mencionó a la largo de este documento internet es un canal de comunicación utilizado a nivel mundial y que de cierta se volvió parte de la vida de millones de persona ya sea para suplir necesidades a nivel laboral, a nivel de investigación o simplemente como plataforma de ocio ya que esta permite la interconexión desde diferentes lugares remotos a la información que comúnmente requerimos o necesitamos ayudando a que las organizaciones ejecuten sus tareas cotidianas de forma ágil y desde cualquier lugar que cuenta con una conexión a internet.

Hay dos formas de conectarse a internet, la primera y la que se ha utilizado durante mayor tiempo es una conexión de tipo alámbrico y la segunda conexión de tipo

inalámbrica ambas formas de conexión de cierta forma ofrecen una conexión adecuada a la red ya se debe definir muy bien cuales son las necesidades que se tiene a nivel de red pues es importante tener en cuenta el número de equipos que se van a conectar a la red, que tanto tráfico de información se va a manejar a nivel de esa red y ya temas se seguridad de acuerdo al nivel requerido.

1.4.1 Conexión Alámbrica a Internet

Una conexión a internet alámbrica es la transmisión de datos o señal de internet mediante el uso de cableado que funcionan como conductores y que permiten la conexión efectiva a internet siempre y cuando esta señal provenga de un ente emisor activo.

1.4.2 Tipos de Conexión Alámbrica

[26] A lo largo de la existencia de internet como red se ha diversificado las formas de lograr una conexión efectiva a través de cableado una con mayores beneficios en cuanto a velocidad de transmisión de datos y a calidad de servicio.

Entre los principales tipos de red cableada utilizadas a nivel mundial se encuentran:

- Conexión a través de red telefónica conmutada
- Conexión digital RDSI
- Conexión ADSL
- Conexión por fibra óptica

[26] Isidro Ros. (6 mayo 2018). Conexiones cableadas a Internet, ¿conoces los tipos que existen? [En Línea]. Disponible en: https://www.muycomputer.com/2018/05/06/tipos-conexiones-cableadas-internet/

1.4.3 Conexión a través de red telefónica

Este tipo de conexión actualmente ya no está en uso pero una herramienta clave cuando el internet tuvo sus primero inicios cuando se inició el despliegue de esta red; su función se daba mediante una llamada a una línea telefónica según el número que el proveedor del servicio le asignara la conexión desde que se marca hasta que se conecta tiene una duración aproximada de 20 segundos, el cobro por este tipo de servicio era de acuerdo a la tarifa de una llamada según la época, aunque existían planes preferenciales que tenían una tarifa mejor; era un servicio costoso que ofrecía navegación pero a una velocidad no superior a los 56Kbps

1.4.4 Conexión digital RDSI

Al igual que las conexiones por red telefónica conmutada este tipo de tecnologías también están en desuso, pero tuvo una participación muy grande cuando se dio a conocer ya que era una de las tecnologías que prometía mucho y se volvía demasiado popular, pero una de la razón para que fracasara fueron sus elevados costos de implementación.

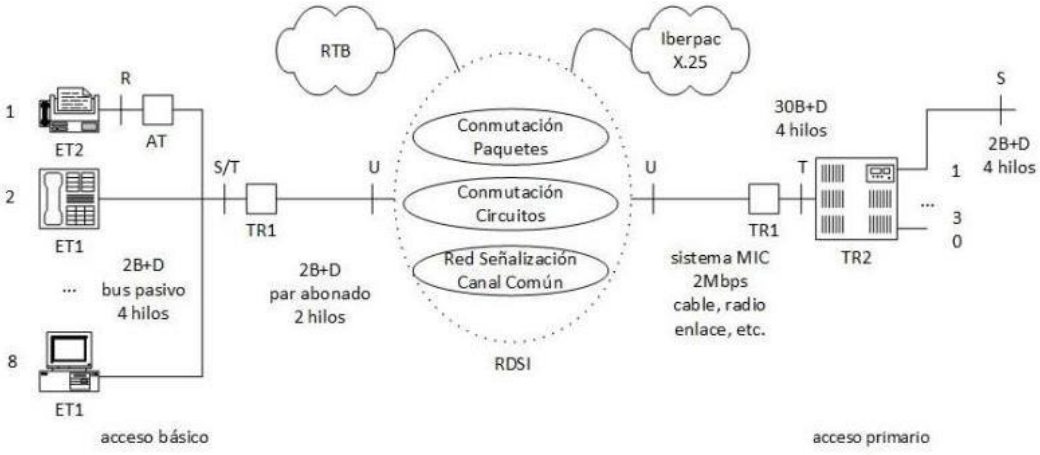
[27]La red RDSI es la evolución de la red telefónica conmutada convencional la cual facilitaba las conexiones de extremo a extremo, entre las principales características de las RDSI están:

- Acceso a través de interfaces normalizados
- Conectividad digital de extremo a extremo
- Conexiones por conmutación de circuitos a n x64 Kbps
- Incorporación de elementos de conmutación de paquetes.
- Utilización de vías diferentes para el envió de señalización y transferencia de información.

[27] Ramón Jesús Millán Tejedor. (2008). RDSI (Red Digital de Servicios Integrados). [En Línea]. Disponible en: https://www.ramonmillan.com/tutoriales/rdsi.php

- Señalización entre en el usuario y la red según el protocolo de canal D
- Amplia gama de servicios.

Figura 9: Estructura de Acceso de la RDSI



Fuente: https://www.ramonmillan.com/tutoriales/rdsi.php

1.4.5 Conexión por ADSL

[28] ADSL o Línea de Abonado Digital Asimétrica es una tecnología que permite la conexión a internet usando una línea telefónica la cual realiza la transmisión en modo digital de la información mediante cables de pares simétricos de cobre, en este caso la conexión también se realiza a través de una línea telefónica pero esta vez mediante conexiones de banda ancha e internet tipo dial-up usando modem para realizar la transmisión de datos.

[28] Julie Maugard. (7 marzo 2017). Todo lo que necesitas saber sobre tecnología ADSL. [En Línea]. Disponible en: https://www.killmybill.es/tecnologia-adsl/

En las conexiones ADSL el enrutador es el encargado de modular la señal de los datos en una banda de frecuencias que resulta más alta que las bandas que se emplea en las comunicaciones telefónicas y a su vez existe un filtro que se encarga proteger las señales para que están no sufran distorsiones y también separando las señales ya moduladas de la señal telefónica.

Es así como las conexiones por ADSL trabajan mediante tres canales que permiten la comunicación entre un mismo cable, un canal permite descargar los datos, otro permite el envío de los datos y el tercero permite la comunicación a través de líneas telefónicas convencionales.

Principales características de las conexiones ADSL

- Necesita una sola línea telefónica para la transmisión de datos y transmisión de voz
- Se requiere de un modem que permita el tráfico de datos entre la propia línea
- El cable ADSL se conecta a un puerto de Ethernet del ordenador
- La velocidad de los datos varía de acuerdo a la oferta de los proveedores
- La tecnología ADSL es una conexión a internet a través de banda ancha.
- Permite transmisión de datos y de voz sin afectar la calidad de los servicios
- Se puede escoger el ancho de banda de acuerdo a las necesidades
- Es sencilla de instalar
- Actualmente es una de las utilizadas y cuenta con una mayor cobertura

4.6 Conexión por fibra óptica

La conexión por fibra óptica es la evolución de las tecnologías anteriores pero que toma un concepto completamente diferente con el fin mejorar la calidad de las conexiones a internet, la fibra óptica es una hebra delgada de vidrio o silicio fundido

que conduce la luz que se utilizada en este caso para convertir esto una tecnología que proporcione transmisión de datos e información.

La fibra óptica son ligamentos de vidrio que están compuestos por núcleo, revestimiento y funda protectora permitiendo la transmisión de señales de luz y eléctricas en recorridos que generalmente son de distancias muy largas que fue utilizada para hacer posible la conexión a internet, este tipo de conexión es uno de los más rápidos en las tecnologías alámbricas.

La conexión a internet a través de fibra óptica es el sistema más moderno en cuanto a redes cableadas, este tipo de tecnologías respeta el ancho de banda contratada aun cuando estén muchos clientes conectado y adicional a esto es una de las tecnologías más estables ya que no sufre mayores interferencias, también es una tecnología que ofrece un nivel seguro en cuanto a conexión y uno de sus mayores atractivos son las velocidades que ofrece ya que son superiores a los otros tipos de conexión alámbricos[29].

4.7 Ventajas de las conexiones por fibra óptica

- Transmisión de datos a alta velocidad: Este tipo de tecnologías ofrece una mayor velocidad de conexión ya que se pueden llegar a una velocidad de 10Gb por segundo lo que asegura una velocidad de conexión mucho más rápida y una mejor experiencia para el cliente.
- Mejor ancho de banda: En cuanto al ancho de banda se hace referencia a la cantidad de información que se puede procesar o enviar al mismo tiempo sin ralentizar la conexión.

[29] Samuel Juliá. Ventajas de la fibra óptica sobre el cable de cobre. [En Línea]. Disponible en: http://www.gadae.com/blog/ventajas-de-la-fibra-optica-sobre-el-cable-de-cobre/

- Evita interferencias: Esta tecnología evitan las interferencias electromagnéticas lo cual da una mayor calidad de conexión y mayor disponibilidad.
- Mejor calidad de video y sonido: Mediante este tipo de tecnologías es mucho más fluido realizar conferencias de trabajo virtuales ya que la calidad de video y sonido se mantiene gracias al ancho de banda y velocidad de la conexión
- Mayor seguridad: Es mucho más fácil detectar intrusos en una red por fibra óptica ya que ofrece muchas más herramientas para su inspección.

1.4.8 Tipos de conexión Inalámbricas

El acelerado crecimiento y evolución que ha traído la tecnología a nivel del mundo genera cada día nuevas plataformas y nuevas formas de conectarse a internet, es así como las conexiones wifi llegan aportar su funcionalidad y comodidad en un mundo donde se requiere contar con información al instante y que este siempre disponible.

[30] Una red inalámbrica es la que permite conectar diversos dispositivos sin necesidad de una conexión física, sino estableciendo comunicación mediante ondas electromagnéticas que se conectan a través de puertos prestablecidos con el fin de conceder acceso a internet.

Ventajas de las conexiones inalámbricas

- Ofrece mayor movilidad y comodidad a la hora de realizar una conexión
- Permite realizar conexiones de red en edificaciones antiguas en las cuales sea muy costoso realizar instalaciones por cable
- Sistema que permite reubicación fácil y rápida de las estaciones

[30] Definición de red inalámbrica. [En Línea]. Disponible en: https://definicion.de/red-inalambrica/

1.4.9 Estándares y especificaciones de las redes WI-F

Con el avance de las tecnologías y la necesidad de lograr una mejor velocidad a la hora de realizar conexiones inalámbricas en dispositivos se creó la familia de estándares 802.11que consta de una serie de técnicas de modulación semidúplex por medio del aire que utilizan el mismo protocolo básico; esta familia de protocolos define el uso de los niveles inferiores de la arquitectura o modelo OSI mediante el cual se especifican las normas de funcionamiento de una red de área local inalámbrica, su primera versión se dio en 1197 y fue creado por el instituto de ingenieros eléctricos y electrónicos (IEEE) y que actualmente aún se encarga de realizar su mantenimiento y mejoras[31].

Tabla 2: Estándares y especificaciones de las redes wifi

FAMILIA	802.11	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ad	802.11ah
Velocidad (Teórica)	2 Mbit/s	54 Mbit/s	11 Mbit/s	54 Mbit/s	600 Mbit/s	6.96 Gbps	7,13 Gbit/s	-
Velocidad (práctica)	1 Mbit/s	22 Mbit/s	6 Mbit/s	22 Mbit/s	100 Mbit/s	100 Mbit/s	Hasta 6 Gbit/s	-
Frecuencia	2,4 Ghz	5,4 Ghz	2,4 Ghz	2,4 Ghz	2,4 y 5,4 Ghz	5,4 Ghz	60 Ghz	0,9 Ghz
Ancho de banda	22 MHz	20 MHz	22 MHz	20 Mhz	20/40 MHz	asta 160Mhz	2 MHz	2 MHz
Alcance	330 Metros	390 Metros	460 Metros	460 Metros	820 Metros	600 Metros	300 Metros	1000 Metros
Año de Implementación	1997	1999	1999	2003	2009	2013	2012	2016

Fuente: https://norfipc.com/redes/tipos-redes-estandares-wi-fi-diferencias.php

- VULNERABILIDADES EN REDES ALAMBRICAS E INALAMBRICAS

La seguridad de la información es un tema que actualmente está tomando mucha fuerza en las organizaciones–esto gracias al rápido crecimiento que ha tenido la industria tecnología en las organizaciones mundiales aportando formas diferentes y agiles de realizar los procesos que habitualmente retrasaban un poco su producción, pero fue este mismo crecimiento el que hizo que hoy en día muchas empresas dependan 100% de internet para poder prestar sus servicios de la forma correcta y así garantizar una disponibilidad de la información para sus clientes esto

[31] IEEE 802.11. [En Línea]. Disponible en: https://es.wikipedia.org/wiki/IEEE_802.11

por la gran variedad de plataformas que pueden integrarse a través de la red teniendo información en segundos estando ubicando desde cualquier lugar remoto.

Fue gracias a la evolución de las redes como plataformas tecnológicas de servicios que se empezó a hablar de seguridad de la información pues a medida que se presentaban nuevas tecnologías estos permitían ir compartiendo más información valiosa y sensible de los clientes, de igual forma se empezaron a integrar plataformas bancarias, tiendas online, pasarelas de transacciones monetarias, bolsa entre otro número grande opciones que la red puede llegar ofrecer; esta acogida a nivel mundial de plataformas hizo ver para los hackers un mundo lleno oportunidades de obtener ganancia si explotaban, vulneraban o robaban la información que circulaba por las redes pues y al fin y al cabo esos se convirtieron en un activo más para las compañías las actuales las cuales deben velar y comprometerse a mantener segura y sin verse afectada por nadie más, es decir firmar cláusulas de privacidad.

¿Pero de qué forma puede llegar un hacker o un pirata informático la información que circula por la red y de qué forma puede llegar a tener acceso a ella si se supone es información confidencial?; es sencillo pues se dieron cuenta que en la parametrización de una se pueden presentar errores ya sea por parte humana que van ligadas a la configuración y parametrización que se le asigne a los dispositivos o son vulnerabilidades que vienen ocultas ya sea en sistemas operativos, equipos de hardware u otro tipo de aplicaciones que comúnmente utilizamos para gestionar o administrar las redes o que también pueden ir directamente ligadas a las aplicaciones que se utilizan en el día a día y se dieron a la tarea de buscar formas de aprovechar esos agujeros de seguridad para apropiarse de dicha información y así mismo causar daño a la red a la cual se conectan.

El tema de vulnerar redes se ha vuelto un negocio lucrativo a nivel mundial ya sea porque roben tu información, porque la modifiquen, la borren o porque infecten tú red enterar con ransomware que se propaga y toma el control total de todos los

dispositivos conectados dejando de esta forma la red sin ninguna opción de funcionamiento.

2.1 DEFINICIÓN DE VULNERABILIDAD

[32] Una vulnerabilidad en seguridad informática se refiere a una falla o debilidad en un sistema dando la posibilidad de que un atacante pueda violar la confidencialidad, integridad, disponibilidad, controles de acceso y consistencia del sistema o de los datos y aplicaciones que están dentro de él.

[33] Las vulnerabilidades en seguridad informática son errores que da la opción que desde afuera se realicen actos sin permiso similares a los que ejecuta el administrador del equipo, incluso de puede llegar a suplantar al usuario.

[34] Una vulnerabilidad en términos de informática hace referencia a un fallo o debilidad en un sistema de información que pone en riesgo la seguridad de la información permitiendo que el atacante pueda llegar a comprometer la integridad, disponibilidad de la información, siendo condiciones y características propias de los sistemas de una organización la cual las hace susceptibles a las amenazas.

[32] Definición de vulnerabilidad. [En Línea]. Disponible en: http://www.alegsa.com.ar/Dic/vulnerabilidad.php
[33]Seguridad informática/Vulnerabilidad. [En Línea]. Disponible en: https://es.wikibooks.org/wiki/Seguridad_informática/Vulnerabilidad
[34]Amenaza vs vulnerabilidad, ¿sabes en qué se diferencia? [En Línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

2.2 TIPOS DE VULNERABILIDADES INFORMATICAS[35].

2.2.1 Vulnerabilidad Física

La vulnerabilidad física está catalogada como la opción de obtener un acceso físico al dispositivo y de esta forma poder tomar el control realizando las acciones que finalmente terminaran en una amenaza o un ataque.

Este tipo de vulnerabilidades generalmente son aprovechadas por empleados que pueden llegar a tener un acceso fácil a los centros de redes y equipos de una organización pues de cierta forma ya tienen una idea de cómo está conformada y estructura la red de dicha organización, adicionalmente también conocen la ubicación de los activos informáticos y saben que tan importantes son o no para la organización lo cual facilita de cierta forma que pueda llegar a presentarse un ataque. [36] Según el portal economía digital el enemigo más temible de las empresas es un empleado antiguo ya que el 47% de los ataques se generan directamente dentro de las compañías datos según la encuesta mundial de seguridad de la información del año 2018 uno de los países más afectados es España.

En el grupo de vulnerabilidades de tipo físico existen algunas que son de cierta forma las más utilizadas y por las que generalmente se presentan ciberataques en organizaciones; entre ellas están relacionadas directamente:

- Accesos no autorizados: este tipo de vulnerabilidades está directamente relacionado con que el atacante puede obtener el ingreso físico al hardware, a través de mecanismos o maniobra que logren vulnerar o alterar la seguridad física que se tiene en las instalaciones de la organización; va directamente ligado a lograr acceder de forma física a las centrales de datos

[35]Vulnerabilidades informáticas. [En Línea]. Disponible en: https://capacitateparaelempleo.org/assets/4aq4l6q.pdf
[36]Los ciberenemigos más temidos de las empresas son empleados y despedidos. [En Línea]. Disponible en: https://www.economiadigital.es/tecnologia-y-tendencias/la-mitad-de-los-ciberataques-dentro-de-empresas-son-de-empleados_520085_102.html

y de esta forma poder alterar o alterar alguna de la partes allí instaladas con el fin de dañar el funcionamiento de la red o generar alteraciones a nivel organizaciones en cuanto a su correcto funcionamiento; este tipo de ataques generalmente es difícil que se presente ya que la mayoría de directores de tecnología tiene especial cuidado con sus centrales de datos pero no se está libre de que pueda suceder.

- Robo de cuentas de usuarios: en este tipo de vulnerabilidades el robo de usuarios no están tecnificado como en otras, pues en este nivel se trata básicamente de lograr encontrar archivos en la red de la organización o simplemente en agendas de usuarios con altos privilegios en la red con el fin de poder lograr un acceso físico a los equipos y dispositivos que controlan la red en la organización generalmente este tipo de ataques se presenta cuando los usuarios no prestan cuidado a tener bien protegidos los datos y contraseñas que les son asignados.

- Infección por medios extraíbles: esta es quizás unas de las principales vulnerabilidades o formas de infección que son aprovechadas, ya que es muy sencillo poder insertar un archivo o código malicioso en la red a través de una USB, SE o un CD/DVD pues en muchas de las organizaciones este tipo de restricciones no se tiene estipulada como política de seguridad y los usuarios tienen la libertad de utilizar este tipo de dispositivos lo cual genera un riesgo elevado ya que es una puerta que se deja abierta a los ciberdelincuentes para insertar códigos malware que se propagan por la red y pueden llegar a bloquear por completo el funcionamiento de una red entera.

- Robos de sesión: en este caso se hace referencia a los usuarios que usualmente deben pararse o dejar sus puestos solo durante largo tiempo o que deben estarse parando de su puesto repetitivamente y no tienen por

política dejar bloqueadas las sesiones de sus máquinas cada vez que se levanten del puesto dejando expuestos sus archivos e información ante otros usuarios que fácilmente pueden utilizar sus sesiones para realizar modificaciones o alteraciones de la información o de la red.

- Robo, modificación o eliminación de datos: este tipo de vulnerabilidad se presenta cuando ya ha pasado una de las que se mencionaron anteriormente pues para poder robar o modificar información vulnerable para la organización es necesario que logre ser efectivo cualquiera de los casos mencionados anteriormente

Si bien las vulnerabilidades de tipo físico se prestan para realizar ataques que generalmente no son ataques tecnificados en un principio pues generalmente son acciones manuales que se ejecutan directamente en los dispositivos o máquinas de la red que ya después de lograr el acceso físico si es posible aplicar técnicas de hackeo o ciberataques de mayor rango que pueden causar muchos más daño; las vulnerabilidades físicas puede decirse que son la puerta a las demás vulnerabilidades.

Adicionalmente en este tipo de vulnerabilidad también están catalogadas aquellas vulnerabilidades que son relacionadas con eventos naturales, riesgo eléctrico u otro tipo de catástrofe que de una u otra forma es muy difícil controlar pues no se puede llegar a tener control de ellas, y también aquellas que tiene que ver con la capacidad de carga que puedan llegar a soportar los dispositivos utilizados en la red sobre los cuales ya se tendría que tomar correctivos internos para mejorarlos.

2.2.2 Vulnerabilidad de tipo Humano

Las vulnerabilidades de tipo humano están directamente relacionadas con error de configuración o parametrización por parte de los administradores de red y que de cierta forma pueden llegar a ser aprovechados por ciberdelincuentes, estos errores

consisten en dejar parametrizaciones por defecto en las cuentas de usuarios, no establecer permisos a usuarios de la forma correcta nivelando privilegios de acuerdo a su nivel en la organización, dejar arriba servicios que no van a ser utilizados por la organización y ejecutar rutinas que son peligrosas o que pueden afectar el funcionamiento de la red; adicional a esto los errores no siempre van en cabeza de los administradores de, también se presentan error por parte de los usuarios comunes que habitualmente ejecutan rutinas o comando indebidos en las máquinas.

En este tipo de vulnerabilidades también puede estar relacionado los ataques ocasionados por empleados de la organización que como se mencionada en el apunte anterior es una de las principales causas de ataques ciberataques a nivel mundial.

Entre los tipos de vulnerabilidades más representativos de este grupo están:

- Configuraciones por defecto: en la actualidad la mayor parte de dispositivos de red o aplicaciones del mercado viene diseñados con una configuración por defecto que es la que generalmente los proveedores emplean para una fácil parametrización de los mismo, pero este tipo de configuración generalmente son aprovechadas por hackers con el fin de lograr accesos no autorizados ya sea a dispositivos de red o aplicaciones que pueden llegar abrir puertas de seguridad mucho mayores.

  Si bien las parametrizaciones por defecto son de ayuda a la hora de implementar cierta tecnología es muy importante que los administradores de red tengan en cuenta que nunca se debe dejar esta configuración, pues las contraseñas por defecto generalmente se encuentran publicadas en los dispositivos físicos o incluso una simple búsqueda en internet puede arrojar los datos necesarios para lograr acceso.

Las configuraciones por defecto generalmente aplican para hardware, software, motores de bases de datos y una de las grandes puertas de entrada a la red son los router.

- Habilitar servicios no usados: otro factor importante que se debe tener en cuenta en una red informática son los servicios que realmente voy a utilizar y que son vitales para la organización, pues generalmente los administradores de red realizan configuraciones donde dejan abiertos puertos o protocolos que no son utilizados por ninguna aplicación o servicio ofrecido por la organización ya que estos servicios no utilizados se convierten en puertas trasera o agujeros de seguridad que fácilmente pueden ser aprovechados por un ciberdelincuentes para enviar ataques o para lograr conectarse y tomar el control remoto del equipo; el hecho de deshabilitar los puertos y servicios no necesarios ayuda a mejorar y proteger la red y la información que por ella circula.

- Perfiles de usuario errados: un tema de suma importancia a nivel de usuarios son los perfiles que se les debe asignar según sean sus actividades y su rango en la organización, es decir definir hasta que nivel de privilegios puede llegar un usuario pues deben existir usuarios que tengan acceso a toda la información y otros usuarios que simplemente la van a poder consultar y así se debe ir armando un árbol de privilegios que se debe asignar.

  El error estaría si por error se generar perfiles con privilegios elevados a usuarios que no tiene por qué acceder a información sensible dándole acceso a herramientas o a procesos que son de su responsabilidad lo cual pueden llegar a causar fugas de información y alteración o modificación de la información de forma no autorizada.

- Actualizaciones hardware y software: en un área de tecnología es común que se cuente con cronogramas establecidos para realizar mantenimientos de hardware o de software según se presente la necesidad, pero puede llegarse a dar el caso de que se ejecute un mantenimiento de forma incorrecta afectando algún parte del hardware o que se presenten errores en el desarmado y armado de partes; en cuando a software es probable que alguna de las actualizaciones no se ejecute con éxito o por alguna situación los dispositivos se reinicien en medio de un proceso de mantenimiento o actualización de software, aplicaciones o sistemas operativos.

- Implementación errónea: la falta de conocimiento o inexperiencia también juega un papel importante es las vulnerabilidades de tipo humano, ya que de este tipo de problemas se puedan dejar abiertas una serie de puertas de seguridad que son comúnmente muy utilizadas por hackers para apoderarse de la información o para lograr acceder a un red; en este tipo como ejemplo podemos mencionar dejar habilitadas configuraciones por defectos en hardware y software, habilitar de forma errada servicios que no se van a utilizar en la organización, dejar parámetros innecesarios en bases de datos u aplicaciones o incluso en el mismos sistema operativo.

2.2.3 Vulnerabilidad de las comunicaciones y del software

La red o más bien el internet cada día se sigue convirtiendo en una herramienta que cada vez más personas y organizaciones utilizan a nivel del mundo teniendo en cuenta que muchos de los servicios que se prestan por estas se hacen a través de la red un ejemplo claro de ellos es el sector bancario, el sector de la educación y las entidades gubernamentales que actualmente ofrecen un gran número de trámites con tan solo un clic o un ingreso a una plataforma lo cual ha facilitado y revolucionado los medios de transmisión y comunicaciones de datos, pero por ese

sin número de transacciones importantes que cada segundo se realizan en la red es que usuarios con intenciones diferentes a las del común iniciaron a realizar análisis sobres las aplicaciones y sobre las vulnerabilidades que se pueden llegar a presentar tanto en el software como en el hardware que hacen posible que corran y se realicen transacciones a nivel mundial.

Una vez empezaron a detectar puertas de seguridad abiertas que de una u otra forma se podían aprovechar detectaron que para ellos era posible ejecutar ataques relacionados con denegaciones de servicios, podían llegar a penetrar en una red y apoderarse de la información de los usuarios, lograr un control remoto de las maquinas atacadas, realizar escaneos sobre los servicios o aplicaciones que se ejecutan en la red, analizar el tráfico que circula por la red entre otro número de formas utilizada para tacar y robar información sensible de las organizaciones.

De acuerdo a investigaciones realizadas en diferentes portales de internet se realizar una recopilación de los principales ataques realizados en redes a nivel mundial aprovechándose de las vulnerabilidades que tienen las redes y los sistemas operativos utilizados en las organizaciones; en esta relación encontramos:

2.2.3.1 Ataques de Denegación de servicio

[37] Según el portal Genbeta en seguridad informática, un ataque de denegación de servicios es la unión de varios ordenadores que centran sus ataques a un solo servidor y es considerado como un ataque que tiene como objetivo dejar inaccesible un sistema o una red de computadores que unidos entre si hacen posible el correcto funcionamiento de un servicio o un recurso y que de ser efectivo el ataque dejara a los usuarios conectados sin acceso a las plataformas requeridas.

[37] Ataque de denegación de servicio. [En Línea]. Disponible en: https://es.wikipedia.org/wiki/Ataque_de_denegación_de_servicio

[38] Otra definición para este tipo de ataques la encontramos en el portal Genbeta, este lo define como un ataque distribuido denegación de servicio por sus siglas en inglés y que se asocia directamente cuando muchos ordenadores atacan un objetivo en específico con el fin de que este deje de funcionar.

De acuerdo a las definiciones encontradas los ataques de denegación de servicio tiene como único objetivo perturbar el correcto funcionamiento de una red o bloquear el acceso a un servicio determinado que es prestado por una plataforma web y que generalmente provocan la perdida de conectividad entre el usuario final y el servidor sobre el cual está alojado el servicio, adicional a esto la red sobre la cual esté conectada el servidor se va ver afectada por su rendimiento ya que las solicitudes enviadas al servidor van a consumir el mayor porcentaje de ancho de banda dando como resultado final una sobrecarga de recursos y finalmente una perdida en los servicios ofrecidos por la compañía.

Este tipo de ataques generalmente se dan mediante una saturación de puertos por el envío masivo de información o solicitudes poniendo al límite la capacidad del servidor o maquina prestadora del servicio y por ende haciendo que este ya no esté disponible a terceros; este tipo de ataques son utilizados por hackers con el fin de sabotear actividades gubernamentales, o elecciones democráticas entre otro tipo de servicios ofrecidos por paginas a nivel mundial, aunque también son de gran uso por administradores de red o plataformas tecnológicas con el fin de poner a prueba sus servidores e identificar que tanta carga pueden llegar a soportar.

Los ataques de denegación de servicio pueden presentarse de varias formas, a continuación, relacionamos algunos de los ataques DoS más utilizados:

- ICMP FLood Attack: la inundación de ping es uno de los ataques de denegación de servicio donde el atacante envía una cantidad altísima de paquetes de solicitud de eco o ping de ICMP (Protocolo de Mensajería de

[38] Guillermo Julián. (2 febrero 2012). ¿Qué es un ataque de DDoS y cómo pararlo? [En Línea]. Disponible en: https://www.genbeta.com/web/son-los-ataques-ddos-efectivos-como-medio-de-protesta

Control) que aprovechando la opción de saturación de ping que envía este tipo de paquetes lo más rápido posible sin esperar una respuesta.

El objetivo de esta técnica es agotar el ancho de banda de la víctima o de la red objetivo a través del envío en forma continua de los paquetes ICMP de forma que cuando la víctima trate de responder sobre cargue tanto el ancho de subida como el ancho de bajada; este tipo de ataques son mucho más efectivos cuando el atacante posee un mayor ancho de banda que el equipo atacado pues de esta forma será efectivo mucho más rápido y así la víctima no podrá procesar la cantidad de paquetes recibidos.

Otro uso que se le puede dar a este tipo de ataques es para realizar diagnósticos por perdidas de paquetes de red y problemas de rendimiento en la red o servidores que prestan el servicio.

- Fraggle DoS Attack: este tipo de ataques el atacante se encarga de enviar una gran cantidad de tráfico mediante solicitudes de eco UDP a una ip objetivo, mientras que los paquetes enviados camuflan la ip saliente con la del equipo objetivo lo cual hace posible que los dispositivos de red o de enrutamiento entreguen mensajes a todos los hosts que conforman dicha red haciendo que estos respondan las peticiones al mismo tiempo a través de repuestas ECHO lo cual va hacer que la red se sature y sea incapaz de trabajar con normalidad creando ralentización en los servicios prestados y en los recursos utilizados.

- Jolt Dos Attack: este es otro tipo de ataque de denegación de servicio; en este caso lo que se hace es enviar un paquete ICMP de gran tamaño pero desfragmentado con el fin de que el equipo objetivo utilice todos sus recursos disponibles con el fin de poderle reconstruir nuevamente , como resultado se obtiene que la maquina atacada se congela o queda paralizada debido a que utiliza toda su capacidad para armar nuevamente el paquete y de esta forma

crea cuellos de botella en la red o en los servicios que son prestados a través del equipo objetivo.

- Land Attack: este tipo de ataque consiste en confundir a la maquina objetivo de modo tal que al recibir el ataque se bloque; el ataque consiste en enviar paquetes TCP SYN falsificados en los cuales la dirección ip de la maquina objetivo se completa en los campos de origen y destino de forma tal que al ser recibido por el objetivo provoca el conflicto y hace que la maquina se bloquee.

- SYN Flood: este tipo de ataque consiste en enviar una gran cantidad de paquetes TCP SYN pero que generalmente van aparentemente desde un hosts diferente para lo cual se falsifica las dirección ip que envían la solicitud, cada paquete recibido es tomado como una solicitud de conexión al servidor lo cual hace que este inicie a responder a hosts que nunca recibirán la respuesta ya que son ip falsificadas y evitando de esta forma que se respondan a peticiones que realmente si son legítimas.

2.2.3.2 Escaneo de Puertos

Una de las puertas de entrada de los atacantes a la red son los servicios o puertos que habitualmente acostumbramos a dejar activos sin necesidad o protocolos que dejamos habilitados aun cuando ninguna de nuestras aplicaciones las está utilizando o no son necesarias para el correcto funcionamiento del proceso informático dentro de la organización. Este es uno de los ataques mas populares y mano sencillos de realizar pues básicamente se debe contar con una herramienta que permita analizar una red o un host de destino en específico.

El escaneo de puertos es una técnica mediante la cual se puede realizar el reconocimiento de los servicios que una maquina objetivo tiene expuestos y de esta forma realizar un análisis de los posibles ataques que se pueden enviar a esta.

Adicionalmente por este tipo de ataques es posible que el atacante descubra cuales son los puertos por los que tiene habilitados los diferentes servicios ya que de acuerdo a la parametrización se pueden llegar a utilizar puertos pocos conocidos para despistar o proteger la información.

Realizar un escaneo de puerto puede considerarse como uno de los primeros pasos que debe realizar un atacante sobre su máquina objetivo ya que por medio de este puedo obtener información valiosa sobre su objetivo todo depende de nivel y sus conocimientos; es así como se puede obtener información como puertos habilitados, que aplicaciones tiene instaladas y porque puertos están configuradas, detalles del sistema operativo, versiones de aplicaciones, características de la arquitectura de la red entre otros; y con esta información se pueden buscar o identificar agujeros de seguridad de acuerdo a la información obtenida mediante este ataque.

Un escaneo de puerto puede llegarse a realizar de dos formas, un ataque se trata de obtener información de forma pasiva y otra de forma activa:

- Escaneo de puertos Activo: consiste en enviar cantidades grandes de paquetes con información o encabezados que no satisfacen los estándares generales con el único fin de recibir una respuesta y así llegar a identificar las versiones de aplicaciones y otros datos que se mencionaron en el párrafo anterior; este método en ocasiones deja de ser efectivo ya que puede ser detectado fácilmente por sistemas de detección de intrusos.

- Escaneo de puerto Pasivo: este método no es tan agresivo como el escaneo de puertos activo y por lo general es difícil ser detectado en la red por los IDS, en este caso se realiza un análisis de los datagramas ip que circulan por la red a través de un rastreador de puertos; al momento de dividirse los valores del datagrama se van tomando datos de los diferentes fragmentos obtenidos. A diferencia del método anterior es mucho mas demorado.

2.2.3.3 OS Finger Printing

Uno de los puntos más importante en las infraestructuras de red de una organización es el sistema operativo que utilizan para realizar las diferentes actividades es de ahí donde salen los esfuerzos por proteger la identidad de este pues cuando un atacante lo conoce fácilmente puede saber qué tipos de ataques o que tipo vulnerabilidades tiene disponibles.

Un ataque de OS Finger Printing se trata de realizar una serie de validaciones con el fin de recopilar información mediante la cual sea posible identificar qué tipo de y arquitectura de sistema operativo se están utilizando en las maquinas objetivo; [39] el OS Finger Printing activo se base que cada tipo de sistema operativo responde una forma diferente a los diferentes paquetes se le envían lo cual hace posible que a través de herramientas se puedan comparar las respuestas recibidas con datos referenciales conocidos y de esta forma poder llegar a identificar el sistema operativo de la maquina atacante. Este tipo de ataques generalmente puede ser combinado con un ataque de escaneo de puertos.

En este tipo de ataques también existe un OS Finger Printing pasivo que se basa en el análisis de los paquetes enviados por la maquina objetivo utilizando técnicas de sniffing, y así mismo se realiza la comparación de los paquetes con las bases de datos para identificar qué sistema operativo está utilizando la máquina.

Cabe resaltar en este tipo de ataques que el modo activo es más directo y confiable a la hora de querer saber el sistema operativo de la maquina objetivo, pero puede ser fácilmente detectado; mientras que el pasivo se realiza de modo más silencioso y genera poco tráfico en la red lo cual sería difícil de identificar en una red.

2.2.3.4 KeyLoggers

[39] Fernando Catoira. (18 octubre 2012). Pentesting: Fingerprinting para detectar sistema operativo. [En Línea]. Disponible en: https://www.welivesecurity.com/la-es/2012/10/18/pentesting-fingerprinting-para-detectar-sistema-operativo/

Esta puede ser considerada una amenaza bastante peligrosa ya que mediante este tipo de herramientas es posible realizar un seguimiento a cada una de las pulsaciones que se realizan en una maquina en la mayoría de casos sin el consentimiento del usuario atacado.

Un keylogger es un programa que puede ser de software o hardware utilizado por los atacantes con el fin obtener las pulsaciones del teclado de un usuario determinado lo cual ayudaría al atacante a obtener contraseña, número de tarjetas de crédito y débito con sus respectivas claves, realizar lectura de mensajes secretos, correos electrónicos y en general todo lo que el usuario atacado escriba va quedar registrado por los KeyLoggers.

Generalmente este tipo de malware están residentes en el sistema operativo de la maquina atacada ya sea a nivel de API en el teclado, en la memoria o incluso hasta en el mismo kernel; este tipo de software son de difícil detección ya que en ningún momento se ve afectado el funcionamiento de la maquina y así mismo para los antivirus es complejo realizar la detección ya que se almacén como archivos o tráfico normal dentro del ordenador.

2.2.3.5 ICMP Tunneling

Este tipo de amenaza lo que hace es aprovechar algunos tipos de firewall que no bloquean los paquetes ICMP o con el fin de poder establecer una comunicación directa entre dos computadoras sin necesidad de que estas interactúen con el resto de la red; de esta forma este tipo de ataques pueden llegar a colgar una maquina objetivo inundándola de paquetes de tipo ICMP.

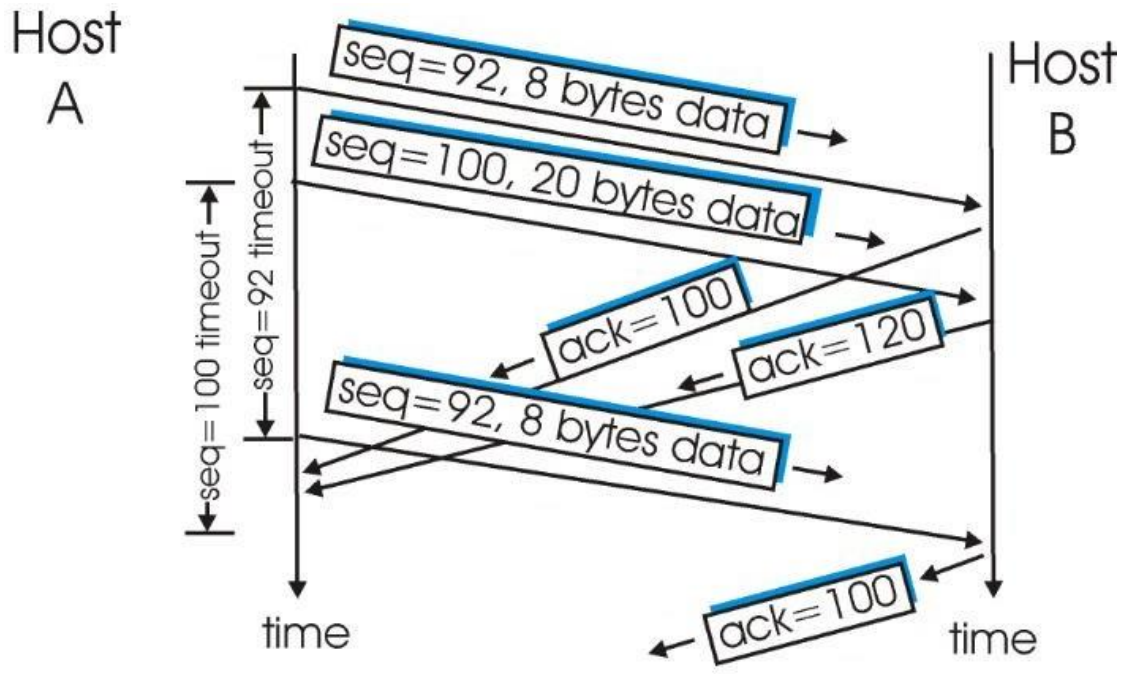
2.2.3.6 Ataque de Secuencia TCP

Un ataque de sentencias TCP consiste en realizar intentos con el fin de predecir o identificar el numero secuencial usado mediante el cual se identifican los paquetes en una conexión TCP con el fin de falsificar paquetes o realizar robos de sesión.

Este tipo de ataques puede considerarse como que el atacante inicialmente debe realizar un proceso de monitorización del flujo o tráfico de los datos de los hosts de la red teniendo en cuenta el origen y el destino; una vez identifique la secuencia el atacante lo que puede realizar es suplantar el destino y tomar el lugar de esa máquina con el fin de recibir todos los paquetes enviados por la maquina origen.

Una robe la sesión del equipo destino falsificara su ip haciéndose pasar por la maquina destino y enviara paquetes al dispositivo de origen teniendo acceso a la información que dicho hosts maneja o simplemente romper la comunicación entre ambas maquinas.

FIGURA10: Ataque de Secuencia TCP



Fuente: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

2.2.3.7 Ataque LOKI

[40] Los ataques LOKI se realizar a través una aplicación cliente/servidor que recibe este nombre y que fue desarrollado por Daniel Mende, uno de los hackers que más repercusión ha tenido a nivel mundial en los últimos años; esta aplicación cuenta con un entorno grafico que permite realizar ataques a múltiples protocolos y que permite manipular los protocolos de red para realizar ataques del tipo Man In The Middlen entre otro tipo de actividades maliciosos.

Entre los protocolos soportados se encuentran ARP, HSRP,HSRPVW, RIP, BGP, OSPF, EIGRP, WLCCP, VRRP, VRRPV3, BFD, LDP Y MPLS; a través de loki es posible demostrar que los datos pueden ser transmitidos de una forma secreta escondiéndolos en el tráfico que generalmente circula por la red. Este tipo de ataques se utiliza como una puerta trasera del sistema operativo Linux.

2.2.3.8 Software Malicioso

Uno de los ataques más antiguos a nivel de informática puede decirse que son los virus o también llamados softwares maliciosos que se encargar de realizar acciones dañinas en las maquinas donde se alojan con el fin de robar, modificar o alterar el correcto funcionamiento de las maquinas afectadas, entre los ataques por software malicioso o malware se encuentran las siguientes clasificaciones:

- Virus: este tipo de software está diseñado para propagarse en un host o maquina sobre la cual se instala y pasar de una a otra según los equipos conectados a la red, este tipo de programas está escrito principalmente para realizar modificaciones en el funcionamiento de los equipos sobre los cuales se instala.
- Gusanos: este al igual que el virus es un software malicioso con la diferencia que este posee la capacidad de autorreplicarse a través de las redes

[40] Loki en la plantilla. [En Línea]. Disponible en: https://underc0de.org/foro/hacking/loki/

informáticas sobre las cuales están conectados los hosts infectados; este tipo de amenazas o vulnerabilidades generalmente se presentan a deficiencias de seguridad en las máquinas de destino y su objetivo está enfocado en consumir recursos como ancho de banda en la red.

- Adware: este tipo de software generalmente viene respaldado por publicidad y se insertan en las maquinas atacadas a través de la instalación algún software o aplicación ya que tiene la capacidad de camuflarse fácilmente sin que el usuario se dé cuenta y su función es realizar un análisis del tráfico y de las páginas visitadas por el usuario con el fin de poder ofrecer publicidad referente a los gustos o preferencias analizadas.
- Spyware: este tipo de software malicioso se aloja en las maquinas atacadas con el fin de recopilar información sobre los usuarios o sobre la información que dicho usuario maneja; en términos generales funcionan como un software de monitorización.
- Troyanos: un troyano o caballo de Troya es un software malicioso que se aloja en la maquina objetivo con el fin de que el atacante puedo obtener acceso remoto a dicha máquina.
- Root Kit: este tipo de software maliciosos es un poco más agresivo y lo que busca es lograr acceso a los hosts infectados, pero con un nivel de administrador sin ser identificado con el fin de poder realizar acciones maliciosas en un host.
- Ransomware: este tipo de ataques es uno de los agresivos en los últimos días y su uso es mayor cada día a nivel mundial; consiste en un código malicioso que tiene como objetivo secuestrar la información de la maquina o de la red infectada según sea el caso y para poder obtener la contraseña de desbloqueo es necesario cancelar altas sumas de dinero de acuerdo a las exigencias puestas por el atacante.

2.2.3.9 Cracking de Contraseñas Wifi

Uno de los avances más representativos a nivel mundial y sobre medios de comunicación basado en internet ha sido la evolución de las conexiones wifi las cuales de cierto han aportado una gran variedad de mejoras y evolución en las formas de conectarse a internet desde cualquier lugar geográficamente hablando ya que da facilidad de disfrutar cualquier tipo de contenido sin la necesidad de utilizar cables sin embargo hay aspecto al que se le debe prestar un especial cuidado ya que este tipo de ataques puede presentar en las redes o conexiones inalámbricas existentes en la organización.

Este tipo de ataques consiste básicamente en lograr romper la seguridad de tu red wifi con el fin de poderse conectar a ella; pero realmente el peligro no radica en que se logre la conexión o no la red wifi, lo realmente importante está en que una vez un atacante logre conectarse a nuestra red wifi fácilmente va poder iniciar una serie de ataques y así mismo va poder analizar nuestro tráfico de red, visualización de hosts conectados a red entre otro tipo de información que puede verdaderamente importante si se desea robar o modificar información de alguno de los hosts relacionados en la red.

[41] Generalmente este tipo de ataques debe realizar en un rango mediante el cual se tenga alcance o se logre detectar señal de la red wifi a la cual se quiere atacar o penetrar y esto se hace posible a las fallas de seguridad que sean descubierto incluso en el protocolo WPA2 que es considerado el más seguro y estable hasta el momento; y que gracias a este tipo de ataques ha sido posible logar obtener datos sensibles como número de tarjetas crédito, contraseñas, mensajes, chat, email entre otro contenido transaccional usado por los hosts conectados a la red atacada.

2.2.3.10 Hotspots Falsos

Este tipo de ataques generalmente este dado en redes inalámbricas donde los atacantes se valen de la necesidad de tener conexión a internet encargándose de

[41] Lo que necesita saber acerca d WiFi Hotspot. [En Línea]. Disponible en: https://www.netspotapp.com/es/wifi-hotspot.html

crear conexiones o puntos de conexión falsos con el fin de los usuarios puedan llegar a conectar a estos.

En informática un Hotspot Wifi es un lugar físico que se proporciona para dar a los usuarios la posibilidad de utilizar sus dispositivos fuera de la casa y lograr así una conexión a internet gratuita. Estos puntos de acceso se hicieron populares hace más de una década en los establecimientos de comidas.

Son ataques fáciles de realizar ya que los usuarios que se conectan a redes wifi generalmente o están pensando en seguridad básicamente están pensando encontrar con disponibilidad de red en sus dispositivos para poder realizar sus transacciones o acceder al contenido que se requiera, es ahí donde los atacantes tiene habilidad de crear sitios de acceso a internet inalámbrico con el fin de acceder o robar información de los usuarios que se conecten a dicha red; y pueden llegar a existir hots spots pagos o gratuitos; una buena forma es crear un hots falso y solicitar datos o información confidencial de los clientes ejemplo que realicen el pago del servicio con sus tarjetas de crédito y de ahí capturar esos datos para posterior realizar estafas.

2.2.3.11 DNS Spoofing

Usualmente en red los servidores DNS pueden llegar a no tener mucha importancia para los usuarios o administradores de red; un [42] DNS (Sistema de Nombres de Dominio) es el que nos permite resolver el nombre de una página web por su dirección, de esta forma los usuarios no debemos acordarnos de la secuencia de números que conformar un IP y así poder acceder a dichos sitios.

Es así como el DNS Spoofing es un método que se encarga de alterar las direcciones de los servidores DNS que utiliza la víctima y de esta forma establecer un control sobre las consultas y peticiones que realiza, y es así como la finalidad de

[42] Josep Albors. (9 febrero 2017). Ataques al DNS: cómo intentan dirigirte a páginas falsas. [En Línea]. Disponible en: https://www.welivesecurity.com/la-es/2017/02/09/ataques-al-dns/

este ataque es lograr modificar los registros que se almacenan en el servidor DNS por los cuales se decida el atacante.

En ocasiones para que un ataque de estos sea efectivo debe emplear algunos mecanismos como DNS cache poisoning, Man In The Middle, uso de estaciones falsas entre otros.

2.2.3.12 ARP Spoofing

Los ataques ARP Spoofing se presentan tanto en redes cableadas como inalámbricas y consiste en él envió de una serie de mensajes falsificados ARP (Protocolo de Resolución de Direcciones) a una red LAN, el objetivo a lograr es que el atacante logre vincular la dirección MAC de su máquina a una dirección MAC legitima y a su dirección ip de alguno de los equipos que se encuentran unidos a la red atacada, una vez se logre este vínculo la maquina atacante va poder recibir la información que pueda ser accesible a través de la IP atacada.

Entre los ataques de ARP Spoofing se pueden catalogar tres tipos:

- Ataque de Inundación MAC: este tipo de ataques da la posibilidad al atacante de obtener información de la red que esté relacionada con contraseñas que no estén encriptadas, correos electrónicos y conversaciones de mensajería instantánea; el objetivo de este tipo de ataque ARP es inundar al swicth con paquetes provenientes de dirección MAC diferentes y así consumir la memoria disponible de este y hacer que entre en un modo de apertura fallida que permite enviar todos los paquetes entrantes se envíen a todos los puertos disponibles y de esta forma ser capturados por el atacante.

- Envenenamiento de Caché DNS: este ataque consiste en emitir datos que no se originan de fuentes confiables a un servidor obligando a este a que los almacene en cache y una vez almacenes los distribuya a los hosts

conectados a la red. Generalmente estos ataques se presentan cuando se aprovechan vulnerabilidades del diseño de software.

- Ip Spoofing: este tipo de ataque ARP se basa es suplantar una dirección IP de un host legitimo con el fin de camuflar su verdadera dirección IP esto para hacerse pasar por una fuente confiable, con el único fin de lograr tener acceso a la información que está en las demás maquinas que se encuentran conectadas en la red. Esto se realiza a través del envío de un paquete con dirección ip falsificada con el fin de que el destinatario confié en el origen y conceder el acceso

2.2.3.13 ACK Flood

[43] Este tipo de ataques se encargan de aprovechar al máximo las propiedad ofrecidas por el protocolo de red ACK que permite la conexión entre un servidor invitado y un cliente mientras dure la sesión, el objetivo de este tipo de ataques es enviar una cantidad de paquetes ACK y borrar en el servidos aquellos donde las sesiones no existen, como el número de sesiones que no existen va ser muy alto el servidor va consumir sus recursos tratando de depurar los hosts cuyas sesiones son invalidas y así reducir su rendimiento o la caída por completo del servicio o servidor.

2.2.3.14 Ataque FTP Bounce

Los ataques relacionados con FTP Bounce se aprovechan del comando PORT para conectarse los servidores FTP y de este modo simular que enviar paquetes a usuarios conectados a la red, lo que hace es enviar archivos a los diferentes hosts probando puertos a ver cuáles están activos. Este tipo de ataques actualmente son

[43] ACK Flood Attack. [En Línea]. Disponible en: https://www.flowguard.io/about-ddos/types-of-ddos/ack-flood-attack

poco probables ya que la mayoría de servidores FTP traen inactivo el dicho comando.

2.2.3.15 TCP Session Hijacking

Los ataques de robo de sesión son ataques en los cuales atacante debe estar pendiente de la comunicación entre dos hosts ya que solo es posible realizar el robo de dicha sesión al momento de iniciar la autenticación que es donde se debe validar la autenticación de ambos hosts, este ataque consiste en que una maquina atacante robe la sesión TCP de una maquina objetivo y se haga pasar por ella durante todo lo que dure la comunicación teniendo así acceso a toda la información que le envié o transfiera el otros host.

2.2.3.16 Ataque Man-In-The-Middle

Este tipo de ataques es importante prevenirlo ya que se sitúa en el intermedio de la comunicación de dos hosts, es decir mediante este ataque se obtiene la posibilidad de recibir la información enviada por el host 1, abrirla, leerla y si es posible modificarla a su gusto antes de ser entregada al host número 2.

Es un ataque bastante peligroso ya que el atacante obtiene la capacidad y el privilegio de observar todo lo que se tramitando entre los dos hosts y de esta forma alterar a su antojo la información que va enviar al host de destino y así mismo fácilmente puede llegar a interceptar contraseñas, mensajes de correo electrónico, cuentas bancarias, autorizaciones para pagos, transacciones online entre otro tipo de servicios que circulan por la red.

[44] Es un ataque que puede llegar a presentase en redes alámbricas e inalámbricas, incluso uno de los ataques más comunes se presente a través de un router wifi que

[44] ¿Qué es un ataque MAN-IN-THE-MIDDLE? [En Línea]. Disponible en: https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/

actúa como intermediario entre los dos hosts con el fin de interceptar los datos y las comunicaciones.

2.2.3.17 Ataques de Aplicaciones web

Con las evolución de las plataformas tecnológicas y con el fin de mejorar cada vez sus servicios ofreciéndole a sus clientes mayores facilidades a la hora de realizar las transacciones sea cual sea el servicio, las compañías a nivel mundial han enfocado sus esfuerzos en realizar la mayor parte de sus procesos de forma digital y esto mismo se ha venido desarrollando para que los usuarios puedan realizar sus transacciones desde cualquier lugar del mundo solo con contar con una conexión a internet lo hace mucho fácil la vida y ahorra tiempo que es uno de los principales recursos que buscan cuidar los usuarios con el fin de agilizar y obtener lo todo ya; producto del consumismo y de la vida tan acelerada que se está llevando actualmente.

Pero fue esta evolución y la acogida que el uso de plataformas web para realizar transacciones de tipo bancarios, pasarelas de pagos, compras en internet, entre otro sin número de tramites que actualmente podemos realizar a través de la web lo que despertó el interés de los hackers con el único fin de robar información o de lograr provecho sobre los datos de los usuarios que son usuarios de este tipo de aplicaciones web.

Por lo anterior es de suma importancia tener en cuenta los tipos de ataques más representativos en aplicaciones web en este proyecto como forma de conocimiento sobre las vulnerabilidades que se puedan llegar a presente en las plataformas web si no se realiza un desarrollo responsable y no se ponen a prueba este tipo de servicios web; algunas de las vulnerabilidades en aplicaciones web son:

- Inyección SQL: Este tipo de vulnerabilidad es una de los más utilizados en las aplicaciones web, consiste en realizar una inserción de secuencias que generalmente son peticiones para que se realice alguna acción sobre la base de datos logrando así obtener acceso a información valiosa o incluso se puede llegar a obtener privilegios para crear, leer, actualizar, modificar o incluso eliminar información almacenada en la bases de datos y esto aprovechándose de los defectos de programación en la capa de la base de datos de la aplicación.

- Cross-Site Request: Esta técnica que traducida al español significa falsificación de petición en sitios cruzados lo que hace es forzar al navegador web de la víctima a realizar una petición a una aplicación vulnerable; y la aplicación se encarga de realizar la acción elegida a través de la víctima, pero cuya acción se realizará en nombre del usuario que se encuentre logueado en el momento

- Envenenamiento de Cookies: este tipo de vulnerabilidad se enfoca en realizar modificaciones en los contenidos de las cookies o de la información personal que almacenas los sitios web de cada uno de sus usuarios con el fin de saltarse los mecanismos de seguridad de las aplicaciones web y posiblemente llegar a robar la identidad de otros usuarios con mayores privilegios.

- Robo de Cookies: esta técnica se encarga de buscar todas las cookies activas en la memoria del computador del cliente a través de in script java y las enviara al atacante.

- Phishing: esta es una técnica que busca apoderarse de la información sensible de los clientes a través de hacerse pasar por entidades legitimas creando una réplica exacta del sitio web original pero que al momento de que

el cliente inserte sus datos personales inmediatamente van a ser ovados por el atacante.

- Web Defacement: este ataque consiste en dañar o cambiar la apariencia de un sitio web y lo realizan reemplazando el sitio web original por un sitio puesto por el atacante con el fin de dejar sin funcionar o de causar daños al sitio atacado.

- Buffer Overflow: esta vulnerabilidad se considera como un error del programador ya que se presenta cuando alguno de los procesos que conforma la aplicación almacena datos fuera de la memoria que fuer reservada para ellos haciendo que estos datos adicionales se escriban sobre la memoria adyacente que a su puede generar error en los accesos y entregar resultados incorrectos.

2.3 DATOS ESTADISTICOS DE CIBERSEGURIDAD AÑO 2018

[45] Según el reporte de seguridad emitido por la multinacional en seguridad ESET para Latinoamérica emitido en el 2018 donde se refleja un panorama general de la situación y evolución de la ciberseguridad y el cual está dividido en preocupaciones de las organizaciones, incidentes, implementación de controles por parte de las organizaciones y panoramas de seguridad en cuanto a las situaciones detectadas.

El incremento de los ataques de ciberseguridad a nivel mundial ha despertado una serie de preocupaciones en las organizaciones actuales y según el reporte de ESET las principales preocupaciones de las organizaciones a nivel de Latinoamérica son

[45] ESET Security Report 2018: el estado de la seguridad de la información en las empresas de la región. [En Línea]. Disponible en: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/

en primer lugar Ransomware con un 57%, seguido de las Vulnerabilidades con un 55% y en tercer lugar el Malware con un 53%.

Los altos porcentajes que se muestran en las preocupaciones de las organizaciones se deben al incremento en el número de códigos maliciosos que se detectaron en menos de un año lo cual es un incremento bastante alto lo cual deja claro que este tipo de infecciones y ataques sigue aumentando su tendencia todo esto encaminado a que este ha venido evolucionando en sus formas de actuar y que se convierte en una opción bastante rentable a los atacantes, según el reporte emitido por Eset el crecimiento en la detección de códigos maliciosos fue del 60%.

A nivel de la explotación de vulnerabilidades en las organizaciones el panorama no es para nada alentador pues en el año 2017 se reportaron 14700 contra 6447 del año 2016 lo cual tiene una representación del 120% siendo un aumento bastante alto por lo cual las organizaciones deben estar atentas a sus configuraciones y a sus estructuras de red con el fin de no ser víctimas de este tipo de ataques ya que es un problema que se está magnificando y que según la tendencia puede mantenerse.

De acuerdo a lo anterior la mayor cantidad de detecciones de código malicioso los porcentajes se encuentran así:

- Perú 25%
- Argentina 15%
- Colombia 10%
- Ecuador 5%
- Bolivia 2%
- México 20%
- Brasil 14%
- Chile 6%
- Venezuela 3%

También se encontró que las familias de códigos más propagadas durante el año 2017 fueron: TeslaCrypt, CryptoWall, Cerber, Crysis y Locky; adicional a estos también fueron registrados otros tipos de códigos como Win32/HoudRat.

Así mismo una de las preocupaciones de las organizaciones encuestadas en el informe de Eset es el robo de información el cual alcanzó un 51% esto por la gran variedad de amenazas que circulan en la red y mediante las cuales puede llegar a ser posible robar información valiosa y sensible de las organizaciones.

Índice de Infecciones por Ransomware

De acuerdo a los indicadores de obtenidos en la encuesta los países que tiene mayor índice de infecciones de tipo Ransomware son Ecuador y Venezuela ambos con un 22%

FIGURA 11: Infecciones de Malware por País

Fuente: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/

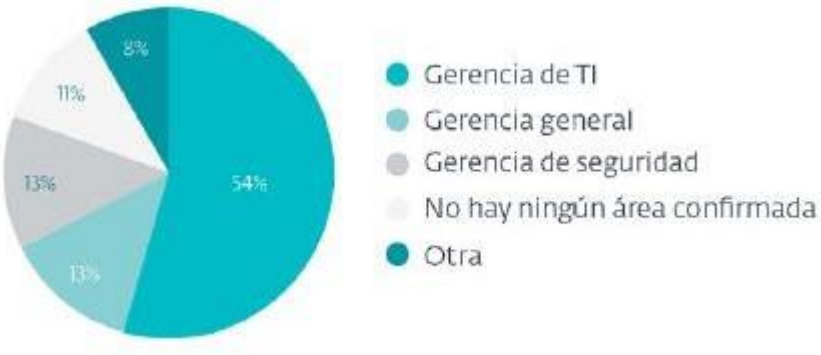
En este análisis también se hizo un estudio sobre los incidentes de códigos maliciosos de acuerdo al tamaño de las empresas lo cual deja reflejado en que las empresas de mayor tamaño van a contar con un sistemas y mecanismos mucho

más avanzados para la detección de este tipo de amenazas por lo cual la cantidad de detectada va ser mayor dando un margen para realizar las correcciones pertinentes; es así como en las organizaciones de tamaño pequeño se tiene un porcentaje del 40%, seguido de las medianas empresas con 45%, las grandes con 48% y las Enterprise con un 47%.

En este caso también se incluyó el tema de controles de seguridad o planes que gestionen de forma correcta la seguridad de la información, en este caso el resultado es el siguiente, 1% de las empresas encuestadas no cuentan con tecnologías que aseguren su información y por lo menos un 25% no posee o no cuenta con políticas de seguridad que gestionen y garanticen la protección de los datos y la información.

De acuerdo a las organizaciones estudiadas el mayor porcentaje de organizaciones centra la gestión de la seguridad de la información en el área de TI sin decir que esta sea una práctica errada lo que se recomienda por las buenas prácticas es que exista un área de seguridad dedicada a este pero solo un 13% cuenta con personal únicamente dedicado a la seguridad de la información, obviamente este factor influye en el tamaño de la organización y el presupuesto que destina para este tipo de gestiones.

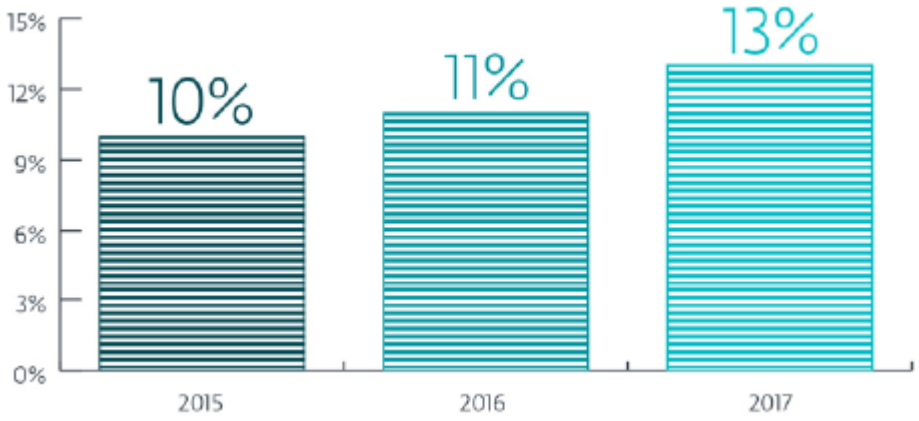
Figura 12: Área Encargada de la Gestión de la Seguridad



Fuente: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/

Otro de los puntos que se analizó en el reporte emitido por Eset es el presupuesto que es destinado por las compañías para atender el área de seguridad siendo este una las mayores quejas pues en muchas de las organizaciones no se cuenta o no se dispone de un presupuesto adecuado para la mantención de un departamento de dedicado esta actividad situación que actualmente no ha cambiado y las cifras se han mantenido durante el tiempo.

Figura 13: Empresas que Cuentan con Área Dedicada de Seguridad.



Fuente: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/

En otro tipo de estadísticas podemos remitirnos al informe otorgado por el gigante en tecnología y redes Cisco denominado [46]Últimas tendencias de seguridad e inteligencia ante amenazas podemos encontrar que el malware está siendo cada vez mucho más dañino y a su vez se está convirtiendo en un problema mucho más difícil de combatir debido a la experiencia que están desarrollando las atacantes.

A pesar que durante el año 2017 se logró encriptar el tráfico web global permitiendo mejorar la seguridad también abre una puerta eficaz para permitir ocultar actividades de comando y control por parte de los administradores de red.

[46] Últimas tendencias de seguridad e inteligencia ante amenazas. [En Línea]. Disponible en: https://www.cisco.com/c/es_co/products/security/security-reports.html

- PROTECCIÓN SOBRE VULNERABILIDAD EN REDES

3.1 RECOMENDACIONES GENERALES

El crecimiento de los ciberataques a nivel mundial ha generado que así mismo la seguridad en las infraestructuras de red se preparen con el fin de poder mitigar y protegerse de esta serie de vulnerabilidades que de una u otra forma dejan expuesta su información ante los hackers y a nivel mundial, ya que de la misma forma en que evoluciona la tecnología y sus formas de comunicarse y conectase así mismo los hackers están buscando nuevas estrategias para violar la seguridad de las redes en las compañías pues hoy en día explotar este tipo de vulnerabilidades se ha convertido en un negocio bastante lucrativo y que deja buenas ganancias a quien sean capaz de hacer efectivos dichos ataques.

En vista del creciente número de ataques a las diferentes compañías a nivel mundial y ver que las organizaciones y usuarios de cierta forma estaban desprotegidos frente a este tipo de ataques se presenta como una solución o una forma de prevenir la seguridad informática que está enfocada exclusivamente en proteger las infraestructuras tecnológicas de las organizaciones a nivel mundial que incluya una serie de estándares, protocolos, métodos, reglas de seguridad y un sin número de herramientas que de ser aplicadas de forma correcta van a generar un nivel mayor de protección frente a los tipos de ciberataques que hoy en día circulan por la red.

Es importante aclarar que nunca se va a estar 100% seguro o protegido de un ataque sin embargo lo que se puede lograr a través de estos mecanismos es que los niveles de riesgos y de vulnerabilidad sean menores y de esta forma hacer un poco más difícil el trabajo a los ciberdelincuentes que van a tener que buscar otras alternativas de penetrar la seguridad de una red.

[47] La seguridad informática es de suma importancia en las organizaciones actuales ya que se enfoca en cumplir con los pilares que son fundamentales para la comunicación y el funcionamiento de las infraestructuras de red; estos pilares son:

- Confidencialidad: debe velar porque únicamente los usuarios autorizados puedan tener acceso a la información.
- Integridad: únicamente aquellos usuarios que tengan permisos y privilegios pueden realizar modificaciones de la información
- Disponibilidad: los datos deben permanecer disponibles en cada momento y durante el tiempo cuando el usuario requiera acceder a ellos
- Autenticación: asegurarse de que los usuarios realmente si se estén comunicando y conectado realmente donde piensan y creen.

La protección hoy día es un tema fundamental en las organizaciones, ya que segundo a segundo se realizan millones de transacciones a nivel mundial cualquiera que sea el tipo pueden ser transacciones bancarias, archivos de herramientas ofimáticas, documentos legales, contraseñas usuarios entre otros y que deben mantener protegidos y no ser conocidos por terceros es por eso que este tema cada día toma más fuerza ya que como usuarios requerimos que nuestros datos realmente estén protegidos así mismo es importante garantizar que los servicios ofrecidos por las organizaciones realmente sean prestados de la forma correcta, que son funcionamiento no se vea alterado arrojando datos erróneos o perdiendo su funcionalidad.

[47] ¿Qué es la seguridad informática y cómo puede ayudarme? [En Línea]. Disponible en: https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/

Figura 14: Ciclo de desarrollo mantenimiento y mejora

Fuente: http://siempresa.blogspot.com/2012/07/sgsi-sistemas-de-gestion-de-la.html

3.2 RECOMENDACIONES PARA TENER UNA CONEXIÓN DE RED SEGURA

Actualmente todavía se presenta un interés poco en el tema de la seguridad informática a pesar de que el creciente número de ciberataques aumenta cada año causando perdida de datos, de integridad y de dinero a compañías multinacionales que se ven afectadas por este tipo problemas; pero es que sería algo inusual decir que una compañía va estar protegida en su totalidad sobre algún ataque o ciberataque pues el avance acelerado de los sistemas hace que cada día surja una nueva vulnerabilidad o una nueva forma de penetrar la seguridad de alguna red a nivel mundial lo cual hace el trabajo para los hackers un poco más fácil.

Pero es que a pesar de las recomendaciones de las compañías dedicadas a la seguridad informática muchas organizaciones aún no se atreven a aumentar su

presupuesto para mitigar estos impactos sino hasta que se ven afectados o son víctima de alguno de ellos; y es que [48] según Panda Security empresa española dedicada a la seguridad informática, existes tres motivos principales por los cuales las organizaciones no dedican suficientes recursos a este tema:

- Porque es muy costoso => 33%
- Porque no lo consideran un tema importante => 8%
- Porque un sistema de seguridad consume muchos recursos => 8%

El alto costo de las soluciones en seguridad es quizás uno de los primeros inconvenientes que las gerencias de las compañías tienen en cuenta para no incurrir en dichos gastos que de otra forma para ellos nos van a representar un intereses o incremento en sus utilidades.

Sin embargo, es importante seguir una serie de recomendaciones con el fin de poder establecer mecanismos de control que permitan proteger nuestra información de forma tal que se mitigue el impacto que un ciberataque pueda causar a una organización; algunas de las recomendaciones generales para que se implemente una conexión segura son:

- Política de Seguridad: el principio de seguridad a nivel de infraestructuras tecnológicas en las organizaciones a nivel mundial debe ser una política de seguridad que sea efectiva , que abarca todos y cada uno de los factores involucrados en el proceso informático de la compañía en el cual se delimiten responsabilidades por cada uno de los activos de la organización, funciones en cuanto a los procesos, validación de procedimientos, maneras de actuar frente a situaciones de riesgos, control y mecanismos de reacción durante el proceso informático, se establecer los procedimientos correctos de acuerdo a cada una de la áreas y para cada uno de los usuarios, y otro punto que

[48] Diego Lorenzana. (27 septiembre 2012). Consejos para implementar una segura red informática en nuestra empresa. [En Línea]. Disponible en: https://www.pymesyautonomos.com/consejos-practicos/consejos-para-implementar-una-segura-red-informatica-en-nuestra-empresa

debe ser muy importante en una política de seguridad en el ámbito de la seguridad informática es que se audite su cumplimiento y efectividad.

En la política de seguridad es importante que se implemente un política para el manejo de contraseñas y cuentas de usuario y donde se delimite la responsabilidad para cada usuario donde quede claro que dichas cuentas son solo de uso personal, así mismo como debe ser el uso adecuado de los recursos entregados por la organización para que se realicen los procesos según el cargo y el rango de cada usuario entre otros puntos que deben ir enfocados a la protección y seguridad de los datos y la red de la organización.

Figura 15: Pilares de las Seguridad informática

Fuente: http://esquemanacionaldeseguridad.com/iso-27001-gestion-de-la-seguridad-de-la-informacion/

- Implementar mecanismos de seguridad: otra acción importante que se debe realizar es contar con herramientas que brinden un nivel de seguridad a los equipos que se conectan a la red, por eso se considera importante contar

una herramienta antivirus que sea licenciada y que siempre este actualizada con las ultimas bases de datos de firmas para que se puedan detectar ataques y bloquear intentos de robo o intrusión de aplicaciones maliciosas en la red.

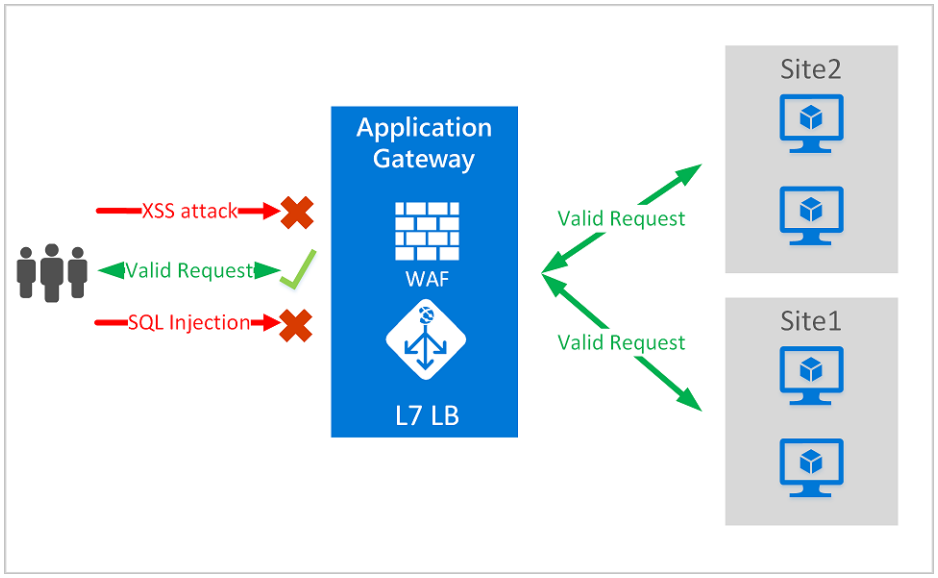
También es importante implementar herramientas Firewall ya sea a nivel de hardware o software el cual pueda establecer un filtro de toda la información circula por la red a través de una serie de reglas que implementa el administrador de la red según sus necesidades y su nivel de conocimiento.

También es importante que se establezcan herramientas que identifiquen intrusos en la red (IDS) las cuales ayudan y alertar sobre situaciones anómalas en una red de acuerdo a unos parámetros definidos y que son conocidos como normales por el administrador de red. Esto es posible gracias al análisis que se realiza al tráfico de datos que circula por la red.

Entre los tipos de firewall que se pueden llegar a implementar en una organización están:

WAF - Firewall de Aplicaciones Web: Este tipo de Firewall son dispositivos de hardware o software mediante los cuales es posible proteger los servidores de aplicaciones web sobre los ataques emitidos por ciberdelincuentes a través de internet permitiendo realizar un control avanzado sobre las transacciones que se realicen a través de él.

Figura 15: Firewall de Aplicaciones Web



Fuente: https://docs.microsoft.com/es-es/azure/application-gateway/waf-overview

Entre las opciones comerciales de Firewall de Aplicaciones Web encontramos los siguientes:

Basados en Dispositivos:

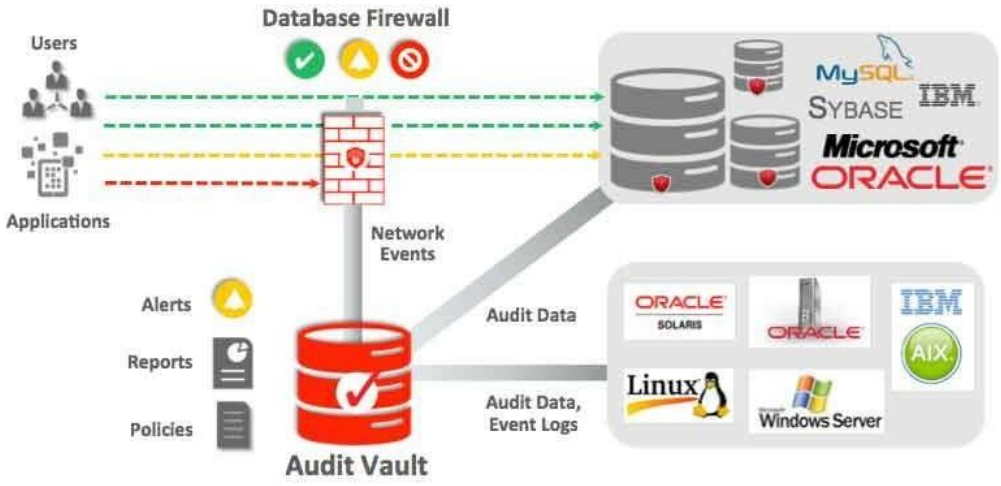
- Barracuda Network WAF
- Citrix Netscaler Aplication Firewall
- F5 Big-IP ASM
- Fortinet FortiWeb
- Imperva SecureSphere
- Monitorapp AIWAF
- Penta Security WAPPLES
- Radware APPWall

Basados en la Nube:

- AIONCLOUD
- Akamai Technologies Kona
- Cloudbric
- Cloudflare
- F5 Silverline
- Radware
- Sucuri Firewall
- WebScale Cloud Secure

Firewall de Base de Datos: Son aplicaciones de software que permiten filtrar mediante un conjunto de reglas preestablecidas todas aquellas peticiones que llegan al manejador de las bases de datos ayudando a bloquear peticiones maliciosas y permitiendo realizar un monitoreo de las actividades que se realizan en el motor de base de datos.

Figura 16: Firewall de base de datos



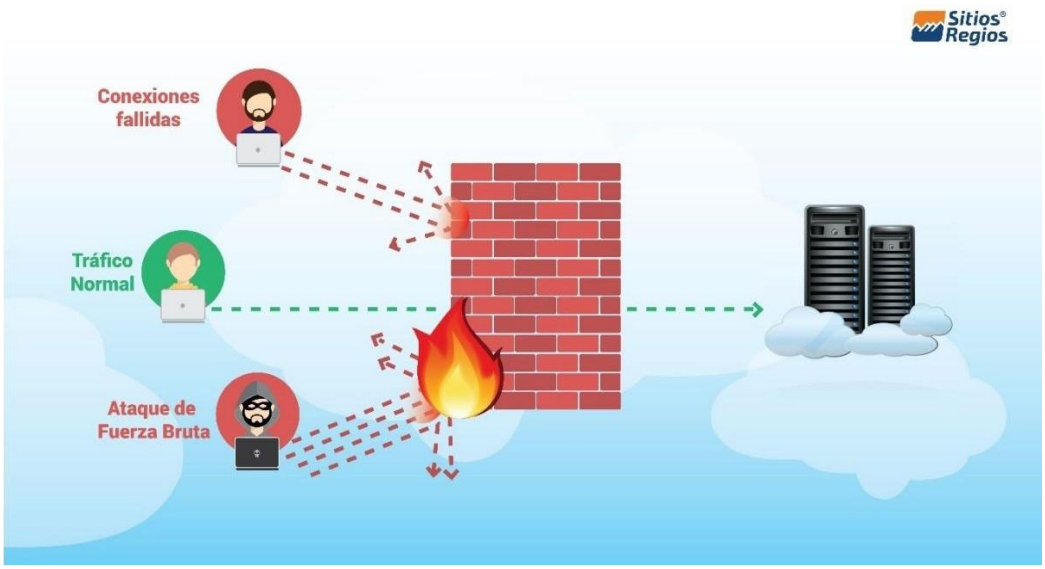
Fuente: https://noticiasseguridad.com/tecnologia/como-asesgurar-bases-de-datos/

Entre las opciones comerciales de Firewall de base de datos encontramos:

- GREENSQL
- Oracle Database Firewall
- ModSecurity
- Microsoft SQL server

Los firewalls que se mencionaron anteriormente son especializados o se centran su mayor fortaleza en bases de datos o aplicaciones web, sin embargo, existe otro tipo de firewall que se centran como tal en la seguridad de una red privada con el fin de bloquear aquellos intentos de acceso por personas no autorizadas al contenido de una red en específico, estos reciben el nombre de cortafuegos o firewall y están diseñados precisamente para bloquear el acceso a una red privada a aquellos usuarios que no cuentan con los privilegios para hacerlo centrándose en examinar los mensajes que entran y salen de la red para obstruir la llegada de aquellos que no cumplen con criterios de seguridad.

Figura 17: Firewall Cortafuegos



Fuente: https://portal.sitiosregios.com/knowledgebase/175/Como-evitar-ser-bloqueado-por-el-firewall-del-servidor.html

En la actualidad existen tanto firewall por hardware que vienen incorporados en los enrutadores y que deben configurar sus propias reglas de navegación entre ellos podemos encontrar productor ofrecidos por marcar como:

- Sonic Wall
- Fortinet
- Cisco
- TPLink

Y también se encuentran herramientas software pagas y libres que actúan como firewall o cortafuegos entre cual sea o no mejor depende de la parametrización que se realice en ellas, entre los firewalls por software encontramos

- ZoneAlarm Free Firewall 2017
- TinyWall
- Anti NetCut3
- Comodo Free Firewall
- PCTools Firewall Plus 7
- AVS Firewall
- HandyCafe Firewall

Adicional a los firewalls otro tipo de herramientas funcionales que ayudan a prevenir y proteger una red, estos son los IDS o IPS diseñados para aumentar la seguridad vigilando y examinando el tráfico en los paquetes que circulan en la red en busca de datos sospechosos.

IDS – Sistema de Detección de Intrusos: Este tipo de sistema aporta un grado de seguridad preventivo ante cualquier actividad sospechosa valiéndose de alertas que son enviadas a los administradores para que ejecuten acciones sobre los incidentes detectados.

IPS – Sistema de Prevención de Intrusos: Este es un dispositivo que ejerce control de acceso a una red de información con el fin de proteger los sistemas de ataques y abusos, y está diseñado para analizar los datos del ataque y actuar con el fin de detener dicho ataque al instante.

Entre las herramientas de detección y prevención de intrusos mencionamos las más utilizadas, entre ellas están:

- Snort
- Security Onion
- OpenWIPS.NG
- Suricata
- BroIDS
- OSSEC
- Open Source Tripwire
- AIDE

- Contar con un dominio: la implementación de un dominio en la red de una organización es importante ya que esta facilidad la administración de permisos y la configuración de la red en sí; ayudando al administrador de la red a ejecutar reglas de acuerdo a los usuarios y a los grupos de usuarios, así mismo podrá segmentar áreas que tengan mayores o menos privilegios que otros y ayudara a que cada equipo que se conecte a la red de cierta forma tenga que estar autenticado lo cual ayuda a mejorar la seguridad en la red.

- Software Licenciado: aunque parezca una recomendación poco útil el tema del software licenciado es muy importante en una organización primero porque detrás de este hay un tema legal respectos al uso de software legal y segundo porque al utilizar este tipo de software estamos contando con las

actualizaciones de seguridad entregadas por los proveedores del software con el fin de poder cubrir baches de seguridad en versiones anteriores y de esta forma proteger la información que está contenida en las máquinas de la organización.

- Política de copias de seguridad: si bien las copias de seguridad no ayudan a protegernos de ataques cibernéticos si nos ayuda a reponernos de uno pues es importante que dentro de la organización se estable una política de copias de seguridad en la cual se tenga en cuenta periodicidad y lugar donde se va guardar dicho respaldo y preferiblemente que sea almacenada en varias partes diferentes a la red interna de la organización.

  Pues una vez se sufre un ataque cibernético los respaldos de seguridad son los únicos que nos pueden asegurar la recuperación de información confiable e integra siempre y cuando se cuenta con una buena política de respaldos de seguridad.

- Mantenimientos: importante que la organización establezca mantenimientos tanto preventivos como correctivos dentro de la organización con el fin de validar que todas las aplicaciones estén actualizadas en sus últimas versiones, validar que tipo de software está instalada y hacer validaciones que puedan dejar al descubierto extensiones sospechosas de archivos o aplicaciones.

- Seguridad en los correos electrónicos: una de las principales puertas de entrada de ataques cibernéticos es el correo electrónico en las organizaciones, ya que a nivel mundial existen hackers enviando correos masivos a miles de direcciones con el fin de encontrar alguna victima que de clic sobre algún correo maliciosos, y es que es importante implementar herramientas que ayudar a realizar una validación de los tipos de archivos y

mensajes que circulan a través de los correos de la organización, si es posible iniciar a realizar listas de negras y establecer que tipos de extensión de archivos están o no permitidas con el fin de poder evitar que se realicen ataques por este medio

Una recomendación importante es que los usuarios utilicen únicamente cuentas de correo que sean corporativos es decir de uso exclusivo para labores dentro de la empresa y también se recomienda bloquear los dominios de correos personales para evitar que se filtre información o se infecten por esta vía.

Adicional a esto herramientas antivirus como ESET NOD32 o Kaspersky ofrecer plataformas que permiten realizar reglas para el filtrado de correos electrónicos, así mismo los firewall o cortafuegos mencionado en el apunte anterior pueden ayudar a bloquear el uso de correos maliciosos.

- Políticas de contraseñas: es importante que todas las contraseñas generadas para la organización cumplan con unos requisitos establecidos por el departamento de informática de la organización, con el fin de establecer contraseñas que sean difíciles de romper y que realmente sean seguras ya que no es aconsejable dejar que los usuarios las elijan pues habitualmente colocan palabras sencillas o contraseñas demasiado débiles.

- Explotar vulnerabilidades de la red: siempre se debe evaluar la red de la organización, esto puede realizarse aplicando técnicas de hackeo ético para realizar un análisis de vulnerabilidades a nivel interno con el fin de establecer controles y tomar correcciones al respecto para que de esta forma la red este mucho más segura; hoy día existen varias aplicaciones que permiten realizar este tipo de análisis algunas con licenciamiento libre y otras con licencia paga

que generalmente ayudan de cierta forma a realizar un mapa de que tan expuestos estamos antes los hackers.

Entre las herramientas para evolución de vulnerabilidades encontramos metasploit, kali Linux que cuenta con un buen número de herramientas para la explotación y análisis de vulnerabilidades; estas herramientas pueden ser las mismas que utilizan los ciberdelincuentes para generar ataques a las redes, pero a nivel internet se puede utilizar sus funcionalidades a la inversa con el fin de establecer controles que ayuden a mitigar las vulnerabilidades encontradas.

Entre el grupo de herramientas contenidas en la distribución KALI LINUX se pueden mencionar las siguientes.

- Aircrack-ng: Es una de las mejores herramientas para el hackeo de contraseñas de redes inalámbricas puede ser utilizada con el fin de validar que tan potente o no son nuestras contraseñas.
- THC Hydra: Esta aplicación es una aplicación basada en la fuerza bruta mediante la cual se puede llegar a crackear prácticamente cualquier servicio de autenticación remota.
- John the Ripper: Herramienta utilizada para el crackeo de contraseñas, pero basada en pruebas de penetración.
- Netcat: Utilidad de red usada para protocolos TCP/IP que sirve para leer y escribir datos a través de conexiones de red
- Nmap: Herramienta funcional que puede ayudar a descubrir redes y ayudar a auditar la seguridad.
- Nessus: Es una herramienta de escaneo remoto que sirve para descubrir las vulnerabilidades de ordenadores y redes.

Las anteriores son solo algunas de aplicaciones que vienen incorporadas este poderoso paquete de explotación de vulnerabilidades y que puede ser utilizado por los administradores de la red para validar que tan seguros o expuestos se encuentran al navegar en la red.

- Capacitar al personal: [49] de acuerdo al portal apd.es casi el 67% de casos de ciberataques está relacionado con el humanos de las organizaciones mientas que un 18% está ligado a amenazas externas; estas cifras hacen importante que dentro de las organizaciones se tome en serio el tema de la seguridad informática y de la seguridad de la información por consiguiente es necesario que se capaciten las personas en cuanto al uso de correos con el fin de aprendan a identificar corroes sospechosos, enseñarles cuando algunas pistas para que desconfíen de sitios cuando no son seguros e implementar una cultura de navegación por paginas seguras con el fin de que los atacantes no se aprovechen de su ingenuidad.

  En este porcentaje también es importante tener en cuenta las medidas que se toman cuando un empelado es despedido de su cargo pues según el mismo estudio un alto nuero de ataques también se presentar por ex empleados de las organizaciones.

3.4 RECOMENDACIONES ADICIONALES SEGÚN EL TIPO DE

Cuando se busca mejorar la seguridad de una red es importante tener recomendaciones generales que ayudan para que las conexiones sean mucho más seguras, sin embargo, es importante establecer recomendaciones puntuales de

[49] ¿Jornada de puertas abiertas al ciberataque? La gran ciberamenaza para las empresas. (12 febrero 2018). [En Línea]. Disponible en: https://www.apd.es/ciberataques-la-gran-ciberamenaza-empresas/

acuerdo al tipo de ataque que se desea prevenir; a continuación, se darán algunas recomendaciones para prevenir los siguientes ataques:

- Prevenir Ataques de Denegación de Servicio (DDoS)
    - Realizar parametrizaciones en los routers y firewalls para que sean capaz de identificar IP invalidas.
    - Deshabilitar aquellos protocolos que no sean necesarios para evitar inundaciones en los protocolos TCP/UDP
    - Habilitar los logs en los dispositivos de red para tener conocimientos de las conexiones entrantes y salientes.
    - Implementación de un sistema IDS y mantener sus firmas actualizadas.
    - Bloquear aquellas direcciones IP que no se utilizan
    - Establecer reglas de navegación solo para permitir acceso del tráfico deseado
    - Actualizar los sistemas de antivirus y sistemas operativos
    - Establecer parametrizaciones que limiten el ancho de banda en la red.
- Prevenir Ataques Man In The Middle
    - Tener especial cuidado con los correos electrónicos recibidos y que provengan de dominios o remitentes no conocidos
    - Utilizar dispositivos de autenticación adicionales
    - Mantener actualizados los navegadores a su última versión
    - Utilizar el envió de mensajes cifrados donde únicamente el receptor tenga forma de acceder al mensaje con el fin de que no se intercepte la comunicación por terceros y se altere la información.
    - A nivel de desarrolladores u organizaciones implementar certificados de seguridad
    - No solicitar conexiones a través de enlaces enviados por correo electrónico.

- Prevenir Ataques de Malware
    - Instalación de software antivirus o antimalware licenciado y actualizado a la última versión
    - Realizar escaneos de antivirus eventuales con el fin de identificar software malicioso
    - Realizar la actualización del sistema operativo y tener sistemas operativos licenciados
    - Establecer restricciones para instalación de software a través de usuarios administradores
    - Evitar conectarse a redes wifi gratuitas o abiertas
    - Utilizar contraseñas difíciles de romper
    - Contar con una política de copias de seguridad
- Prevenir ataques en Aplicaciones Web
    - Implementar herramientas especiales para seguridad como WAF o firewall de aplicaciones web
    - Definir de forma correcta las consultas dentro del código
    - Usar procedimientos almacenados con parámetros que se parametrizan automáticamente
    - Implementar CAPTCHA o llevar a los usuarios a que respondan preguntas
- Prevenir ataques de tipo ICMP
    - Permitir a los administradores usar mensajes ICMP libremente
    - Permitir el paso del gran tamaño de ICMP
    - Permitir que ICMP funcione incluso en el caso de una fuerte autenticación y carga útil encriptada

- TENDENCIAS EN SEGURIDAD INFORMATICA

El tema de seguridad informática es un tema que es demasiado cambiante y que evoluciona de forma acelerada sin embargo de acuerdo a los análisis realizados por expertos en el tema de seguridad informática es posible hacer un estimado y un futuro para este tema que cada día va en aumento.

De acuerdo a los análisis recopilados de las compañías expertas en seguridad ESET, G DATA, Trend Micro, PANDA, o Check Point se genera un análisis de las principales tendencias a nivel de seguridad informática para los años 2018 y 2019 según el uso y avance de las tecnologías actuales.

4.1 LA EVOLUCIÓN DEL RANSOMWARE

Este tipo de ataques es una de las tendencias en seguridad informática ya que va encaminado a tocar uno de los activos más importantes para las organizaciones a nivel mundial, su información y es que actualmente las organizaciones están dispuestas a pagar con el fin de poder recuperar su información y sus datos en lugar de implementar unas políticas de seguridad establecidas a nivel interno con el fin de mitigar y prevenir los ciberataques.

[50] De acuerdo al informe publicado por la compañía ESET especialista en seguridad informática el uso del Ransomware como una herramienta para la captura de datos de organizaciones a nivel mundial será una tendencia ya que para algunas organizaciones resulta ser menos costoso pagar un rescate que implementar una infraestructura de red solida que cuente con niveles de seguridad y que proteja los

[50] Tendencias en ciberseguridad 2018: El costo de nuestro mundo conectado. [En Línea]. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiOuOnEiuHeAhXiw1kKHRsRA4YQFjAAegQICRAC&url=https%3A%2F%2Fwww.welivesecurity.com%2Fwp-content%2Fuploads%2F2017%2F12%2FTendencias_2018_ESET.pdf&usg=AOvVaw0Z3PZ0n_0QicnnhnNtwiM2

datos; así mismo pone como tendencia los ataques a dispositivos móviles y smartphones enfocado no al tema de robar información o datos personal si no al tema de impedir que la persona utilice el dispositivo lo cual en muchas ocasiones es algo tedioso si tenemos en cuenta que cada dispositivo y cada usuario posee cuentas y configuraciones especificas en sus móviles que de cierta forma perdería.

Otro tema que hace referencia al crecimiento del uso del Ransomware es la llegada del internet de las cosas lo cual el abre un panorama mayor sobre el cual se puede llegar actuar ya que existirán miles de dispositivos conectados en red, sensores integrados en miles de elementos entre otro tipo de elementos importantes como: routers, medidores inteligentes, televisores, juguetes, centrales eléctricas, estaciones de servicios, marcapasos, vehículos entre otros y como cada cosa de estas está conectada entre sí de forma inteligente aumentara este tipo de ataques al tener más terreno que abarcar.

Es así como esta tendencia seguirá en constante aumento de acuerdo a los ataques que se han recibido durante los últimos doce meses y que de una u otra forma se han convertido en una amenaza tanto para usuarios como para empresas, a continuación, se relacionan uno de los cinco casos más importantes y que se han sido tendencia durante el último año.

- Ransomware Cerber: Considerado uno de los más poderosos Ransomware durante los años 2016 y 2017 cuando se dio a conocer y teniendo presencia importante y bastante relevante durante los últimos meses ya que está equipado con nuevas tácticas y técnicas.

- Ransomware Locky: Es un tipo de Ransomware bastante variable ya que siempre está en constante multiplicación y transformación basándose en botnets de spam.

- Ransomware Badrabbit: Ransomware que se encarga de utilizar ataques drive-by para entregar Ransomware cuentagotas va pidiendo 0.5 bitcoins de rescate de solo cientos de víctimas.

- Ransomware NotPetya: Ransomware que realizo varios incidentes de piratería en organizaciones ucranianas, holandeses y británicas y que estaba relacionado con cifrar el Master Boot Record.

- Ransomware Wannacry: Ransomware que surgió en el año 2017 y ataco en primera instancia hospitales, así como proveedores de internet, telefonía y otros objetivos considerados de alto perfil y a los cuales les solicitaba un rescate pagado en dólares bitcoints.

4.2 REGLAMENTO DE PROTECCIÓN DE DATOS

Otro tema que enmarca las tendencias en seguridad informática es la implementación del GDPR cuyo cumplimiento entra en obligación; [51] este plan es una normativa europea que obligará a las empresas a adaptarse en materia de recopilación, uso, divulgación, retención y protección de datos personales y el cual debe estar estipulado y concentrado en puntos estratégicos que estén relacionados en mantener la privacidad de la información en ámbitos como: consentimiento expreso y no táctico de la información, tiempo y uso concreto de los datos y la información suministrada, legalidad de los emails enviados, aplicación sim importar el país, transparencia en cuanto al tema de robo de datos, derecho al olvido es decir solicitar que sus datos personales sean borrados, protección a los menores, claridad en los textos citados en letra pequeña en los contratos.

[51] Javier Calvo. (11 mayo 2018). Nuevo reglamento de protección de datos: así se deben actualizar los trabajadores. [En Línea]. Disponible en: https://www.eleconomista.es/economia/noticias/9130680/05/18/Nuevo-reglamento-de-proteccion-de-datos-asi-se-deben-actualizar-los-trabajadores.html

Los puntos clave de este acuerdo son:

- Consentimiento para tener y tratar los datos de una persona de forma expresa no táctica.
- Derecho al olvido, este es el derecho a la supresión y hasta ahora esta relacionada con la eliminación de noticias judiciales de Google.
- Portabilidad y limitación, permite a las personas pedir, recibir y transferir directamente sus datos automatizados de una entidad a otra
- DPO, delegado de protección de datos.
- Menores, los menores de 16 años no pueden consentir sobre el tratamiento de sus datos en este caso lo deben hacer sus padres.

4.3 CRIPTOMONEDAS

El aumento del uso de monedas virtuales a nivel mundial para realizar transacciones hace de estas un foco bastante interesante para los ciberdelincuentes teniendo en cuenta su gran demanda pues cada vez es mayor el número de personas que están invirtiendo en las criptomonedas y adicional a esto cada vez más personas están cotizando en este tipo de monedas.

Este crecimiento en el uso de criptomonedas se puede ver reflejado en Colombia en un informa de la revista dinero donde se observa que, [52] en el 2017 las transacciones hechas con pesos colombianos crecieron en 1.200% en transacciones de compra y venta de bitcoins ubicándose en el tercer puesto de los países con mayor crecimiento en los intercambios de moneda local por bitcoins.

Es así como durante el año 2018 se presento un aumento del 51% de ciberataques contra las criptomonedas siendo seis de las mas afectadas las siguientes:

- Electroneum

[52] Cómo Colombia llegó a ser el país latino en el que más crece el mercado del bitcoin. [En Línea]. Disponible en: https://www.dinero.com/economia/articulo/como-en-colombia-crecio-el-mercado-de-bitcoin/256116

- Monacoin
- Bitcoin Gold Double-Dip
- Verge
- Litecoing Cash
- ZenCash

4.4 INTERNET DE LAS COSAS

El crecimiento y evolución de las distintas tecnologías a nivel mundial y la facilidad que están trayendo a los usuarios hace que el internet de las cosas se tome cada vez más la vida cotidiana ya que el crecimiento de hogares digitales y empresas inteligentes cada vez es mayor.

El internet de las cosas es una red de objetos físicos de todo tipo, entre ellos vehículos, máquinas, electrodomésticos, hogares, entre otro que utiliza sensores y API para conectarse a internet y realizar intercambios de datos entres si con el fin aprovechar las funciones ejecutadas por cada uno de los dispositivos con el fin de generar eficiencia y de mantener todo conectado; todo lo anterior gracias a las capacidades que van adquiriendo los robots que se van crean y los dispositivos y pues lógicamente al tener una red completa de dispositivos que funcionan y ejecutan tareas en tiempo real es necesario crear protección para ellos pues van a ser blancos de muchos de los ataques cibernéticos que se presenten en el futuro.

De acuerdo a lo anterior, cualquier dispositivo conectado a internet va poder ser atacado y se va convertir en un blanco para los atacantes pues prácticamente se van poder controlar infraestructuras completas a través de controles y herramientas online; como, por ejemplo:

- Control de plantas de producción a través de dispositivos móviles
- Autos inteligentes
- Casas inteligentes

- Tiendas de venta online y automatizadas.
- Automatización de servicios industriales.

4.5 CIBER ATAQUES BASADOS EN EVENTOS PUBLICOS

Otra de las tendencias en seguridad son las denominadas estafas valiéndose de eventos públicos o de eventos que estén de moda en ese momento donde los atacantes crean todo tipo de publicidad falsa con el fin de lograr robar información y conseguir estafar a las personas ya sea con portales falsos que realmente son una puerta de entrada a malware o también dirigidas a la captura de datos personales.

Así mimo este tipo de ataques van a estar muy enfocados al sabotaje de eventos democráticos o elecciones ya que muchos países están implementando el uso del voto electrónico como método de elección, lo cual puede llegar a suplantaciones o robo de los datos incluidos por el usuario final y donde no se puede asegurar que tan validos son o no los resultados.

- Elecciones presidenciales a nivel nacional e Internacional
- Sistemas de votación para elecciones de parlamentarios

4.6 ATAQUES DIRIGIDOS A LAS TECNOLOGIAS CLOUD

La evolución y acogida de los servicios cloud a nivel mundial hace de este tipo de tecnologías un blanco interesante para los ciberataques por la gran cantidad y variedad de servicios que actualmente se ofrecen pues muchas organizaciones han migrado sus infraestructuras completas a la nube con el fin de recibir mayor protección y seguridad para sus datos, sin embargo aún existen brechas de seguridad que están siendo explotadas por hackers y mediante las cuales se debe

centrar la preocupación de las organización con el fin de prevenir la fuga y robo de información.

De esta forma las tecnologías cloud se pueden llegar a ver afectadas en los siguientes aspectos:

- Violación de datos
- Gestión de la identidad y los accesos deficientes
- APIs Inseguras
- Vulnerabilidades en los sistemas, hardware y software utilizados en los datacenter
- Robo de cuentas de usuario
- Amenazas persistentes avanzadas
- Perdida de los datos
- Análisis de riesgos insuficientes
- Vulnerabilidades por tecnologías compartidas

4.7 ATAQUES A LAS INFRAESTRUCTURAS CRITICAS

[53] Según el informe de tendencias en seguridad informático por la multinacional en seguridad ESET en el año 2017 las amenazas a infraestructuras críticas fueron noticia por el crecimiento de ataques enfocado a este tipo de infraestructuras; una de las principales razones puede ser que cuando este tipo de infraestructuras fueron creadas no se habían establecidos tan seriamente los ataques cibernéticos por lo cual no están preparas para afrontar este tipo de ataques.

[53] Tendencias en ciberseguridad 2018: El costo de nuestro mundo conectado. [En Línea]. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiOuOnEiuHeAhXiw1kKHRsRA4YQFjAAegQICRAC&url=https%3A%2F%2Fwww.welivesecurity.com%2Fwp-content%2Fuploads%2F2017%2F12%2FTendencias_2018_ESET.pdf&usg=AOvVaw0Z3PZ0n_0QicnnhnNtwiM2

Adicional a que las infraestructuras no están preparadas para protegerse sobre este tipo de ataques tampoco es nada fácil actualizar los equipos antiguos de control industrial con nuevos equipos diseñados con conexión a internet para que se mejore la seguridad en ellos.

Como infraestructuras criticas están catalogadas:

- Los servicios básicos
- Instalaciones eléctricas
- Redes de Información y telecomunicación
- Plantas químicas
- Plantas Nucleares
- Acueductos
- Gasoductos.

4.8 ATAQUES MEDIANTE EXPLOITS KITS

La comercialización de kits que permiten ejecutar ciberataques sin mayores conocimientos sobre ellos es otro que ha tomado fuerza a nivel mundial, pues los hackers han visto en ellos un negocio lucrativo; este consiste en crear kits de herramientas que permitan explotar vulnerabilidades en una red que se promocionando y comercializando en la web.

4.9 FALTA DE CAPACITACIÓN A LOS EMPLEADOS

Este ha sido uno de los temas que muchos de los atacante aprovecha cuando va generar un ataque pues muchos hackers se apoyan en la poca experiencia de los usuarios para hacer que estos caigan en sus trampas; por eso es importante que las organizaciones creen campañas de sensibilización sobre la importancia de la seguridad informática teniendo en cuenta que se les debe orientar a cerca del

contenido del cual deben o no confiar, así mismo enseñarles a identificar amenazas o sitios falsos con el fin de proteger la red de la empresa.

Y finalmente en tendencias sobre la seguridad informática se viene otro tipo de tecnologías que de cierta forman están impactan de forma representativa la vida de miles de usuarios a nivel mundial como es el caso de la inteligencia artificial o maquinas que son capaces de aprender y que utilizan soluciones basadas en conceptos Deep learning o machine learning que permiten detectar nuevas amenazas y evaluar vulnerabilidades y detectar malware; y también es importante recalcar que este tipo tecnologías también pueden ser utilizadas por los hackers en sentido inverso.

Un tema que también va impactar el ámbito de la seguridad informática es el Blockchain que es una revolución en la forma que se realizan transacciones entre dos o más personas de forma confiable donde se todo se realiza sin necesidad de intermediarios.

Sumado a lo anterior y que cada día toma mayor fuerza a nivel empresarial es el uso de dispositivos móviles con este fin pues muchas de las organizaciones tienen permitido el uso de dispositivos personales para el manejo de información de la empresa lo que los ha convertido en un blanco esencial para los hackers pues en la organizaciones aún no se han contemplado políticas de seguridad para regular el uso y la seguridad de este tipo de dispositivos; adicional a esto también se tiene como referencia incrementar el número de ataques a dispositivos Mac ya que el número de ataques efectivo referente a ellos aún es muy bajo.

CONCLUSIONES

El avance de las redes e internet como herramienta fundamental para realizar actividades diarias en personas y organizaciones ha hecho que cada día los ciberdelincuentes se ingenien nuevas formas de lograr violar la seguridad de dispositivos y aplicaciones con el fin de tener acceso a la información de los usuarios y de esta utilizarla para realizar acciones fraudulentas que atenten contra la seguridad de los datos y la información.

El aumento de plataformas y tecnologías implementadas a nivel mundial y su conexión hacer mucho más atractivo el mercado para lo ciberdelincuentes ya que van tener mayores opciones de para explotar vulnerabilidades que viene incorporados en los nuevos desarrollos.

En la actualidad uno de los riesgos más importantes en la seguridad de la información es el robo de la información a través del uso de Ransomware o falsificación de plataformas web, así mismo el uso de malware también se ha intensificado durante los últimos años realizando capturas de datos no autorizados.

Es importante tener conocimiento sobre las posibles vulnerabilidades a las que se pueden ver expuestos los usuarios y organizaciones al estar conectados a una red de internet ya que de acuerdo a esto podemos establecer una cultura de uso adecuado de la red y tomando conciencia de la información que comparte o procesa a través de ella, y así mismo tomando medidas y controles que permiten mejorar la seguridad de los datos y de la información.

La tendencia en cuanto a ciberataques refleja que este tipo de ataques seguirá en aumento haciendo uso de tecnologías ya conocidas como el Ransomware, criptomonedas, spam y así mismo se tiene como blanco todos aquellos dispositivos que entren en funcionamiento con el internet de las cosas el cual dejara muchísimas más puertas abiertas para los delincuentes de la red.

BIBLIOGRAFIA

Agencia EFE. (2008, 17 mayo). Internet nació de un proyecto militar y hoy es parte esencial de la vida diaria. Recuperado de: https://www.elespectador.com/noticias/actualidad/articulo-internet-nacio-de-un-proyecto-militar-y-hoy-parte-esencial-de-vida-diar

Albors, J. (2017, 9 febrero). Ataques al DNS: cómo intentan dirigirte a páginas falsas. Recuperado de: https://www.welivesecurity.com/la- es/2017/02/09/ataques-al-dns/

Alegsa.com.ar. Definición de vulnerabilidad. Recuperado de: http://www.alegsa.com.ar/Dic/vulnerabilidad.php

Apd.es (2018, 12 febrero). ¿Jornada de puertas abiertas al ciberataque? La gran ciberamenaza para las empresas. Recuperado de: https://www.apd.es/ciberataques-la-gran-ciberamenaza-empresas/

Avaast.com. Inyección SQL. Recuperado de: https://www.avast.com/es-es/c-sql- injection

Blog.apser.es. (2015, 15 junio). Las redes informáticas: qué son, tipos y topologías. Recuperado de: http://www.apser.es/blog/2015/06/20/las-redes-informaticas-que-son-tipos- topologias/

Calvo, J. (2018, 11 mayo). Nuevo reglamento de protección de datos: así se deben actualizar los trabajadores. Recuperado de: https://www.eleconomista.es/economia/noticias/9130680/05/18/Nuevo-reglamento-de-proteccion-de-datos-

Capacitateparaelempleo.org. Vulnerabilidades informáticas.Recuperado de: https://capacitateparaelempleo.org/assets/4aq4l6q.pdf

Catoira, F. (2012, 18 octubre). Pentesting: Fingerprinting para detectar sistema operativo. Recuperado de: https://www.welivesecurity.com/la-es/2012/10/18/pentesting-fingerprinting-para-detectar-sistema-operativo/

Certsuperior.com. Seguridad en Redes. Recuperado de: https://www.certsuperior.com/SeguridadenRedes.aspx

Cisco.com. (2018). Últimas tendencias de seguridad e inteligencia ante amenazas. Recuperado de: https://www.cisco.com/c/es_co/products/security/security-reports.html

Danny Kevin, R. Internetworking. Recuperado de: https://www.monografias.com/docs110/internetworking/internetworking.shtml

De Blas, D. (2018, 04 septiembre). Servicios cloud: las 12 amenazas de seguridad en la nube que no se deben olvidar. Recuperado de: https://globbsecurity.com/servicios- cloud-las-12-amenazas-de-seguridad-en-la-nube-que-no-se-deben-olvidar-43654/

De Luz, S. (2010, 03 noviembre). Ataques a las redes: Listado de diferentes ataques a las redes de ordenadores. Recuperado de: https://www.redeszone.net/2010/11/03/ataques-a-las-redes-listado-de-diferentes-ataques-a-las-redes-de-ordenadores/

DiarioTI.com. Como protegerse de los ataques man-in-the-middle. Recuperado de: https://diarioti.com/como-protegerse-de-los-ataques-man-in-the-middle/21709

Dinero.com. (2018, 13 junio). Cómo Colombia llegó a ser el país latino en el que más crece el mercado del bitcoin. Recuperado de: https://www.dinero.com/economia/articulo/como-en- colombia-crecio-el-mercado-de-bitcoin/256116

Dunning, D. ¿Qué es una red PAN? Recuperado de: https://techlandia.com/red-pan-info_261597/

Econectiacom. (2017, 22 mayo). Tipos de conexiones a Internet. ¿Cuál te conviene más?. Recuperado de: https://www.econectia.com/blog/tipos-de-conexiones-a-internet-cual-te-conviene-mas

Economiadigital.es. Los ciberenemigos más temidos de las empresas son empleados y despedidos. Recuperado de: https://www.economiadigital.es/tecnologia-y-tendencias/la- mitad-de-los-ciberataques-dentro-de-empresas-son-de- empleados_520085_102.html

Ecured.cu. Red de Computadores. Recuperado de: https://www.ecured.cu/Red_de_computadoras

Eltiempo.com. (2018, 05 marzo). Aumentan los ciberataques para robar dinero a escala mundial. Recuperado de: http://www.eltiempo.com/tecnosfera/videojuegos/entrevista-a-alejandro-gonzalez-y-a-jairo-nieto-creadores-de-estudio-de-videojuegos-colombiano-222336

Es.wikibooks.org. (2017, 16 octubre). Seguridad informática/Vulnerabilidad. Recuperado de: https://es.wikibooks.org/wiki/Seguridad_informática/Vulnerabilidad

Es.wikipedia.org. Ataque de denegación de servicio. Recuperado de: https://es.wikipedia.org/wiki/Ataque_de_denegación_de_servicio

Es.wikipedia.org. Ataque de denegación de servicio. Recuperado de: https://es.wikipedia.org/wiki/Ataque_de_denegación_de_servicio

Es.wikipedia.org.(2019, 25 enero). Red de Computadores. Recuperado de: https://es.wikipedia.org/wiki/Red_de_computadoras

Flowguard.io. ACK Flood Attack. Recuprado de: https://www.flowguard.io/about-ddos/types-of-ddos/ack-flood-attack

Galeano, S. (2019,31 enero). El número de usuarios de internet en el mundo supera el 50% de la población: 4000 millones (2018). Recuperado de: https://marketing4ecommerce.net/usuarios-internet-mundo-2017/

Gestion.pe. (2018, 31 julio). ¿Cuál es la historia del Internet? Recuperado de: https://gestion.pe/tecnologia/historia-internet-240094?ref=gesr

González, A. (2019, 31 enero). El número de usuarios de Internet en España crece en 4 millones: el 93% de la población ya está conectada (We Are Social, 2019). Recuperado de: https://marketing4ecommerce.net/el-numero-de-usuarios-de-internet-en-espana-crece-en-4-millones-el-93-de-la-poblacion-ya-esta-conectada/

Harán, J. (2018, 19 junio). ESET Security Report 2018: el estado de la seguridad de la información en las empresas de la región. Recuperado de: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/

Harley, A. (2018). Tendencias en ciberseguridad 2018: El costo de nuestro mundo conectado. [Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf

Henríquez, S. (2011, 4 octubre). TIPOS DE REDES INFORMATICAS. Recuperado de: https://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/

HistoryPlay. Los seis mayores ciberataques de la historia. Recuperado de: https://mx.tuhistory.com/noticias/los-seis-mayores-ciberataques-de-la-historia

Incibe.com. (2017, 20 marzo). Amenaza vs vulnerabilidad, ¿sabes en qué se diferencia?. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes- se-diferencian

Informaticamilenium.com.mx. Internet. Recuperado de: https://www.informaticamilenium.com.mx/es/temas/que-es-internet.html

Jiménez, J. (2018). Estos han sido los 5 ataques de Ransomware más importantes del año 2017. Recuperado de: https://www.redeszone.net/2017/12/16/estos- los-5-ataques-ransomware-mas-importantes-2017/

Juliá, S. Tipos de redes Informáticas según su alcance. Recuperado de: http://www.gadae.com/blog/tipos-de-redes-informaticas-segun-su-alcance/

Juliá, S. Ventajas de la fibra óptica sobre el cable de cobre. Recuperado de: http://www.gadae.com/blog/ventajas-de-la-fibra-optica-sobre-el- cable-de-cobre/

Julián, G. (2012, 2 febrero). ¿Qué es un ataque de DDoS y cómo pararlo? Recuperado de: https://www.genbeta.com/web/son-los-ataques-ddos- efectivos-como-medio-de-protesta

Latam.kaspersky.com. ¿Qué es un keylogger?. Recuperado de: https://latam.kaspersky.com/resource-center/definitions/keylogger

Lorenzana, D. (2012, 27 septiembre). Consejos para implementar una segura red informática en nuestra empresa. Recuperado de: https://www.pymesyautonomos.com/consejos-practicos/consejos-para-implementar-una-segura-red-informática-en-nuestra-empresa

Malenkovich, S. (2013, 10 abril). ¿Qué es un ataque MAN-IN-THE-MIDDLE? Recuperado de: https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469

Mariño, M. (2018). GDPR: claves del reglamento europeo de protección de datos 2018. Recuperado de: https://www.20minutos.es/noticia/3348576/0/gdpr-reglamento-europeo-proteccion-datos-2018/

Maugard, J. (2017, 07 marzo). Todo lo que necesitas saber sobre tecnología ADSL. Recuperado de: https://www.killmybill.es/tecnologia-adsl/

Mesía, D. Vulnerabilidad de Seguridad. Recuperado de: http://diegomesia.com/vulnerabilidad-de-seguridad/

Millán, R. (2008). RDSI (Red Digital de Servicios Integrados. Recuperado de: https://www.ramonmillan.com/tutoriales/rdsi.php

Netspotapp.com. Lo que necesita saber acerca d WiFi Hotspot. Recuperado de: https://www.netspotapp.com/es/wifi-hotspot.html

Okoi, M. (2018, 13 septiembre). Las mejores 20 herramientas de hacking y penetración para Kali Linux. Recuperado de: https://maslinux.es/las- mejores-20-herramientas-de-hacking-y-penetracion-para-kali-linux/

Ortego, D. (2017, 09 mayo). Las 8 mejores herramientas open source de detección de intrusión. Recuperado de: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

Pandasecurity.com. ¿Cuál es la diferencia entre un IDS Y un IPS?. Recuperado de: https://www.pandasecurity.com/peru/support/card?id=31463

Pandasecurity.com. ¿Qué es IP Spoofing?. Recuperado de: https://www.pandasecurity.com/peru/support/card?id=31442

Pérez, I . (2015, 21 abril). ¿En qué consiste la vulnerabilidad Cross Site Request Forgery (CSRF)?. Recuperado de: https://www.welivesecurity.com/la-es/2015/04/21/vulnerabilidad-cross-site-request- forgery-csrf/

Pérez, J. (2014). Definición de Red Informática. Recuperado de: https://definicion.de/red-informatica/

Ramiro, R. (2018, 20 enero). 25 tipos de ataques informáticos y como prevenirlos. Recuperado de: https://ciberseguridad.blog/25-tipos-de- ataques-informaticos-y-como-prevenirlos/

Ros, I. (2018, 6 mayo). Conexiones cableadas a Internet, ¿conoces los tipos que existen?. Recuperado de: https://www.muycomputer.com/2018/05/06/tipos-conexiones-cableadas-internet/

Sap.com. Definición de internet de las cosas. Recuperado de: https://www.sap.com/latinamerica/trends/internet-of-things.html

Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? Recuperado de: https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

Sites.google. Informática redes de computadores, Orígenes y evolución. Recuperado de: https://sites.google.com/site/informaticaredesdecomputadoras/unidad-1-Introduccin-a-las-redes-de-datos/1-1-origenes-y-evolucion

Underc0de.org. Loki en la plantilla. Recuperado de: https://underc0de.org/foro/hacking/loki/

Varela, V. (2018, 16 septiembre). Top 6 51% de Ataques que Afectan Las Criptomonedas en 2018. Recuperado de: https://www.criptomonedaseico.com/noticias/top-6-51-de- ataques-que-afectan-las-criptomonedas-en-2018/

RESUMEN ANALÍTICO ESPECIALIZADO	
1. Tema	Seguridad en redes de Internet
2. Título.	Estudio Monográfico: Vulnerabilidades en redes de internet alámbricas e inalámbricas
3. Autor:	Arley Guillermo Restrepo Zuluaga
4. Edición	1
5. Año	2019
6. Palabras Claves	Red, LAN, MAN, WAM, VLAN, Internet, Informática, Network, Conexión, Topología, Datos, Autenticación, Alámbrica, Inalámbrica, Digital, WiFi, Vulnerabilidades, Ataque, Servicio, Tecnología, Autorización, Ciberataque, Seguridad, Políticas, Contraseñas, Software, Hardware, Licencia, Confidencialidad, Integridad, Disponibilidad, Malware, Ransomware, Ciberseguridad, Ataques, Web, Organizaciones, ICPM, Puertos, TCP, ARP, Spoofing, Aplicaciones.
7. Descripción	Este estudio monográfico es una investigación en fuentes bibliográficas sobre las vulnerabilidades en las redes de Internet alámbricas y inalámbricas con el fin de realizar un documento que contenga los aspectos generales sobre redes y los protocolos de comunicación, analizando aquellas posibles vulnerabilidades que una red puede llegar a tener de acuerdo al tipo de conexión que se emplee en una organización, así mismo servir como guía de referencia para mitigar ataques y crear ambientes de red mucho más seguros. Finalmente se analizan las tendencias sobre seguridad informática para los próximos años con el fin de mejorar la seguridad en las organizaciones.
8. Objetivo General	Realizar un estudio monográfico sobre las vulnerabilidades en redes de telecomunicaciones alámbricas e inalámbricas
9. Objetivos Específicos	Realizar un estudio e identificar aspectos generales sobre redes y sus protocolos de acuerdo los tipos de conexión alámbricos e inalámbricos Analizar e identificar sobre las vulnerabilidades más aprovechadas por los ciberdelincuentes para generar ciberataques en organizaciones y usuarios finales Elaborar una guía de referencia donde se establezcan parámetros generales de seguridad en la implementación de una conexión de red segura Realizar un estudio sobres las tendencias en seguridad para la implementación de redes de telecomunicaciones seguras e inalámbricas
10. Fuentes.	El presente documento se basó en una investigación realizada en 53 fuentes bibliográficas tomadas de internet en las cuales se abordan los temas contenidos en este documento, adicionalmente gran parte de los textos y párrafos fueron complementados con la experiencia y conocimiento del autor de este documento monográfico
	El uso del internet ha impulsado el avance tecnológico a nivel mundial presentando su crecimiento mayor en los últimos años y llevando a un era de digitalización donde se es posible acceder a cualquier tipo de información sin importar el lugar físico o geográfico donde esta se encuentre lo, único que debe existir es una conexión a internet ya sea alámbrica o inalámbrica entre los dispositivos que contengan la información con el fin de poder consultar, modificar o incluso eliminar los datos que se deseen consultar. El termino red es utilizado desde hace muchos años atrás incluso antes del nacimiento de lo que hoy en día conocemos con como internet; es así como el concepto de red con el propósito de abarcar un área amplia que pudiera establecer comunicaciones de forma estable a lo largo de un territorio nacional, se produce en Suecia y Francia a principio del siglo XIX.

11. Contenidos.	Lo anterior se reconocía como un telégrafo óptico que consistía en una serie de torres que tenían una seria de brazos similares a las persianas los cuales se encargaban de codificar la información que transmitía la torre anterior usándose hasta mediados del siglo XIX cuando tiene su nacimiento el telégrafo. La palabra red se define como la estructura que dispone de un patrón que la caracteriza, y por su parte el termino Informática hace referencia a los saberes de la ciencia que posibilitar el tratamiento de datos de manera automatizada a través de computadores u ordenadores; de acuerdo a lo anterior el termino de Red Informática según el portal definición. Con el avance de las tecnologías y la necesidad de lograr una mejor velocidad a la hora de realizar conexiones inalámbricas en dispositivos se creó la familia de estándares 802.11que consta de una serie de técnicas de modulación semidúplex por medio del aire que utilizan el mismo protocolo básico; esta familia de protocolos define el uso de los niveles inferiores de la arquitectura o modelo OSI mediante el cual se especifican las normas de funcionamiento de una red de área local inalámbrica, su primera versión se dio en 1197 y fue creado por el instituto de ingenieros eléctricos y electrónicos (IEEE) y que actualmente aún se encarga de realizar su mantenimiento y mejoras. Fue gracias a la evolución de las redes como plataformas tecnológicas de servicios que se empezó a hablar de seguridad de la información pues a medida que se presentaban nuevas tecnologías estos permitían ir compartiendo más información valiosa y sensible de los clientes, de igual forma se empezaron a integrar plataformas bancarias, tiendas online, pasarelas de transacciones monetarias, bolsa entre otro número grande opciones que la red puede llegar ofrecer; esta acogida a nivel mundial de plataformas hizo ver para los hackers un mundo lleno oportunidades de obtener ganancia si explotaban, vulneraban o robaban la información que circulaba por las redes pues y al fin y al cabo esos se convirtieron en un activo más para las compañías las actuales las cuales deben velar y comprometerse a mantener segura y sin verse afectada por nadie más, es decir firmar cláusulas de privacidad. Según el reporte de seguridad emitido por la multinacional en seguridad ESET para Latinoamérica emitido en el 2018 donde se refleja un panorama general de la situación y evolución de la ciberseguridad y el cual está dividido en preocupaciones de las organizaciones, incidentes, implementación de controles por parte de las organizaciones y panoramas de seguridad en cuanto a las situaciones detectadas. El incremento de los ataques de ciberseguridad a nivel mundial ha despertado una serie de preocupaciones en las organizaciones actuales y según el reporte de ESET las principales preocupaciones de las organizaciones a nivel de Latinoamérica son en primer lugar Ransomware con un 57%, seguido de las Vulnerabilidades con un 55% y en tercer lugar el Malware con un 53%. La seguridad informática es de suma importancia en las organizaciones actuales ya que se enfoca en cumplir con los pilares que son fundamentales para la comunicación y el funcionamiento de las infraestructuras de red; estos pilares son: • Confidencialidad: debe velar porque únicamente los usuarios autorizados puedan tener acceso a la información. • Integridad: únicamente aquellos usuarios que tengan permisos y privilegios pueden realizar modificaciones de la información • Disponibilidad: los datos deben permanecer disponibles en cada momento y durante el tiempo cuando el usuario requiera acceder a ellos

	De acuerdo al informe publicado por la compañía ESET especialista en seguridad informática el uso del Ransomware como una herramienta para la captura de datos de organizaciones a nivel mundial será una tendencia ya que para algunas organizaciones resulta ser menos costo pagar un rescate que implementar una infraestructura de red solidad que proteja sus datos; así mismo pone como tendencia los ataques a dispositivos móviles y smartphones enfocado no al tema de robar información o datos personal si no al tema de impedir que la persona utilice el dispositivo lo cual en muchas ocasiones es algo tedioso si tenemos en cuenta que cada dispositivo y cada usuario posee cuentas y configuraciones especificas en sus móviles que de cierta forma perdería
12. Metodología.	Este documento no denota ninguna metodología específica, se basa directamente en las fuentes bibliográficas que se consultaron y en la experiencia del autor
13. Principales referentes bibliográficos	¿Qué es la seguridad informática y cómo puede ayudarme? [En Línea]. Disponible en: https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/ Últimas tendencias de seguridad e inteligencia ante amenazas. [En Línea]. Disponible en: https://www.cisco.com/c/es_co/products/security/security-reports.html ESET Security Report 2018: el estado de la seguridad de la información en las empresas de la región. [En Línea]. Disponible en: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-región/
14.Conclusiones.	• El avance tecnológico es un factor clave en la evolución de los países como sociedad y como medio de interacción a nivel mundial ya que a través de él se han dado grandes desarrollos tanto en hardware y software que entrar a facilitar los procesos y las comunicaciones bidireccionales tanto de organizaciones como de personas que buscan de cierta forma suplir una necesidad o prestar un servicio. • El internet es otro factor de gran importancia en la evolución de las tecnologías a nivel mundial pues es el encargado de conectar lugares remotos a través de la red mediante la cual se puede encontrar cualquier tipo de contenido y servicio incluso en países diferentes generando accesibilidad de la información y disponibilidad. • El número de usuarios en las plataformas tecnológicas está en constante crecimiento, si bien ya no a un ritmo tan acelerado se sigue notando una interacción mayor por parte de los usuarios con las tecnologías utilizando tanto plataformas móviles como las habituales de escritorio que ya conocemos, lo cual genera un mayor tráfico de información y de datos a través de la red. • La mayor parte de las compañías a nivel nacional e internacional buscan sistematizar la prestación de sus servicios brindando de esta forma mejores posibilidades de acceso a los datos y al procesamiento de solicitudes según sea el área de prestación de servicio de cada organización.
15. Resultado	Como resultado se obtiene una monografía que contiene los diferentes conceptos de red y sus principales vulnerabilidades en las organizaciones, así mismo una serie de herramientas y recomendaciones que se pueden utilizar con el fin de mitigar el riesgo y así trata de mantener segura la información a nivel empresarial y personal
16. Autor del RAE.	Arley Guillermo Restrepo Zuluaga