UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2019 – MARZO 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

ANÁLISIS DE AMENAZAS Y VULNERABILIDADES EN LA RED INALÁMBRICA DEL ESTUDIO JURÍDICO "CEDEÑO Y ASOCIADOS" DE LA CIUDAD DE MILAGRO

EGRESADA:

BRYAN LEONEL CAIZA CEDEÑO

TUTOR:

ING. ALCOSER CANTUÑA FABIAN EDUARDO

AÑO 2020

INTRODUCCION

La seguridad informática es unas de las partes más importante dentro de las empresas que existen, porque esta permite dar protección a la integridad, privacidad y confidencialidad de los datos e información que se da uso dentro de ella.

Hoy en día muchos de estos lugares están siendo afectados por no tomar precauciones necesarias, no se le da importancia en lo que respecta a este tema. Piensan que no les ocurrirá algo grave, pero en momentos imprevistos, los equipos y la información se ven afectados por amenazas que asechan a las organizaciones.

Las amenazas y vulnerabilidades están vinculadas a la interceptación de la información que circula dentro de la red, esta es realizada por una persona no autorizada; efectuada en la red informática ya que sobre esta circula toda la información y datos. El estudio jurídico "Cedeño & Asociados" ubicado en la Ciudad de Milagro, el cual brinda asesoría y defensoría legal tanto en el campo civil y penal, cuenta con alrededor de 500 clientes, estos procesos se manejan informaciones personales y documentos privados como documentos personales de los clientes, así también direcciones domiciliarias, numero telefónicos, etc. La misma que es recibida y manipulada a diario.

Este análisis se realizó para evaluar los riesgos que se podrían encontrar expuestos al no contar con una seguridad a nivel de hardware y software, este estudio de caso aplicada las metodologías de investigación cualitativa y de campo que permitirá tener una perspectiva simplificada de los problemas mediante la técnicas de la entrevistas, observación directa, para poder obtener conocimiento sobre el estado en el que se encuentra la red informática; mediante estas metodologías se busca conocer las amenazas y vulnerabilidades distintas que se encuentren, se usó el software Nessus para poder realizar un testeo sobre las vulnerabilidades que pudiera tener la red en la parte intangible.

DESARROLLO

El Estudio Jurídico "Cedeño y Asociados" está ubicado en la Ciudad de Milagro, perteneciente a la provincia del Guayas, dentro del Estudio colaboran tres Abogados principales, dos Asistentes Jurídicas y un ayudante general. Los Abogados son los encargados de la distintas defensas y acusaciones de los casos que se llevan dentro del Estudio, mediante las Asistentes desarrollan diferentes escritos y querellas que son dirigidas a las Unidades Judiciales del Ecuador, en cuanto el ayudante es el encargado de llevar y traer oficios o notificaciones al Estudio.

En cuanto la administración de la red informática dentro del Estudio Jurídico, la maneja una de las Asistentes Jurídicas, no teniendo ella estudios previos sobre Sistemas o Redes, al tener problemas en la red solicitan asistencia técnica externa, la cual no es profesional, solo toma parte de solucionar los problemas principales, es por esto que nos damos cuenta que la red no tiene una atención preferencial, esto sea por pocos conocimientos y lo importante que es mantenerla segura.

En la actualidad Organizaciones y/o Empresas están optando por tecnologías de comunicación e información, estar a un clic de poder conocer, aprender e informarnos es fundamental en un sin número de áreas de trabajos, así también el tener información propia accesible desde cualquier parte del mundo se ha hecho muy necesario.

> La creciente dependencia de las empresas, y de la sociedad en general, de las tecnologías de la información y de las comunicaciones, así como el entorno cada vez más complejo en que estas se desarrollan, ha provocado la aparición de vulnerabilidades en los recursos utilizados que las organizaciones deben minimizar con las medidas de seguridad oportunas. (Heredero, Lopez Hermoso, Romo, & Medina, 2004)

La tecnología que nos permite realizar todo este tipo de acciones es el internet, este servicio es el que permite así también darse a conocer como empresa, ofrecer sus productos y servicios.

Pero así mismo para tener un buen funcionamiento, es necesaria tener una correcta instalación, seguridad ante cualquier problema o riesgo que pueda suscitar es una de las más importante, ya que nos ayudará a tener la información que transita en nuestra red integra y confidencial. Cuando se suscita una ruptura en la seguridad de la red puede ser afectada la estabilidad de la red, así también la pérdida o hurto de la información importante que posea la organización o empresa.

"Aplicando todas las medidas necesarias para evitar riesgos y perdidas de la información y de los equipos en que reside" (Castellanos, 2012).

Para poder estar prevenidos ante cualquier tipo de amenaza o vulnerabilidades es importante saber identificarlas, de esta forma tener una percepción clara sobre la situación actual en la que se encuentra la red informática.

La finalidad de este estudio es analizar e identificar diferentes tipos de amenazas y vulnerabilidades que puedan existir en la red informática del Estudio Jurídico "Cedeño y Asociados" y así también dar posibles soluciones o recomendaciones a estos problemas que se encuentren.

En el Estudio Jurídico actualmente no cuenta con control en la red que facilite la detención de problemas, estos pueden ser las amenazas y vulnerabilidades. Entre los inconvenientes encontrados dentro del Estudio Jurídico son que las Políticas de Seguridad no están siendo aplicadas, este fallo permite infiltraciones de ciertos atacantes con intenciones de hurtar o falsificar información importante del Estudio.

A continuación, se incluye una matriz de Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas). Según (Ponce Talancón) en la revista Contribuciones a la Economía indica que: "La matriz FODA: una alternativa para realizar diagnósticos y determinar estrategias de intervención en las organizaciones productivas y sociales"

FORTALEZA	**OPORTUNIDADES**
Cuenta con un internet estable.	Puede optar por renovar equipos y licencias de Software.
DEBILIDADES	**AMENAZAS**
No aplica Políticas de Seguridad. El cableado de la Red se encuentra al alcance de particulares y no se encuentran ordenadamente. Falta de mantenimiento preventivos y correctivos a los equipos informáticos.	Falta de reguladores eléctricos. Excesivo descuido en la limpieza de equipos por el polvo acumulado.

Elaborado por Bryan Caiza Cedeño

La matriz del FODA fue aplicado a los activos del Estudio Jurídico, como se menciona según (Seguridad Informatica, 2010) que: "Todo activo informático de una organización está en peligro de ser robado o manipulado poniendo en riesgo su integridad cuando se encuentra vulnerable, cuando se lleva a cabo un ataque informático y la seguridad presenta falencias pueden ocurrir pérdidas totales de información o ser alterada la integridad y la confidencialidad de los datos". Es así que son los que se encuentran en peligro o vulnerables hacia un ataque.

Es por esta razón que las empresas que cuentan con una red informática deben constar con los servicios de seguridad, de esta forma aseguraría la información transferida por su red y de esta manera no se encuentren vulnerables a personas no autorizadas.

Aplicamos la metodología cualitativa, la cual nos permite aplicar la técnica de entrevista, la misma que fue aplicada en la persona encarga de la red en el Estudio Jurídico, se usó también la metodología de campo, con la técnica de la observación para así poder hacer una valoración visual de los equipos que se encuentran dentro del Estudio, como su cableado estructurado entre otros.

Ya recopilada la información, se dará uso de una herramienta de Software que permite el estudio de la amenazas y vulnerabilidades en la red, así se tendrá a mejor detalle los riesgos y problemas que se suscitan en el Estudio Jurídico "Cedeño y Asociados" y así también cuales serían las medidas a tomar.

Para realizar este análisis y/o escaneo en la red se refirió el correcto oficio, donde se solicitó el permiso al Gerente-Propietario del Estudio para así tener la oportunidad de realizar una valoración más completa dentro del mismo. Entre los principales beneficios que se obtiene a realizar el escaneo tenemos: Reducción de riesgos, que esto conlleva a hurto y falsificación de la información, mejoras en el Estudio Jurídico de esta manera poder dar una protección y garantizar un confidelidad en la red.

Una buena *aplicación de equipos* dentro de una red es un punto importante, ya que de esta también dependerá la estabilidad y confianza que pueda dar al momento de desarrollar algún tipo de actividad.

Así también debe tomarse en cuenta el dinero que se invierte y si cumplirá para el nivel de trabajo que será usado, ya que el buscar el gasto mínimo en equipos puede también traer una serie de problemas, por otro lado el despilfarro de dinero en equipos innecesarios o con un nivel de características que no se le dará uso no conviene en ningún aspecto a una empresa. Los equipos y sus conexiones deben cumplir un estándar de calidad y compatibilidad, se analizaron los equipos y si se cumplían estándares correctos.

En cuanto a la compatibilidad, hoy en día los equipos deben contar con IPv4 e IPv6. En el aspecto de *Wireless* debe ser bajo el cumplimiento de normas: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3.

La parte del cableado es muy estricta, esta es escasa dentro de la red analizada, así también su tipo de ponchado es de mala calidad como su cable. Son puntos a corregir dentro del Bufete que dentro de conclusiones serán señalados. Existen dos tipos de topologías aplicadas en

la parte de cableado estructurados que son: Cables de par trenzado sin blindar (UTP) de 100 ohmios y cuatro pares y Ponchado T-568A y T-568B

A continuación se detalla de manera simplificada los equipos que se encuentran en la red del Estudio Jurídico;

MARCA	**MODELO**	**ESPECIFICACIONES**	**CANTIDAD**
D-Link	Switch Ethernet	10/100 Mb DES-1008DPuertos disponibles: 8	1
D-link	Router Dir-615	4 Puertos RJ-45, 300mbps Inalámbrico	1
Dell	Odell 2 Escritorio	500Gb HDD. 4Gb Ram, Celeron 3.3Ghz	3
Lenovo	Ipad 14 8756	14', 800 GB HDD, 4Gb Ram, Pentium 3.5GHz	1
Epson	L355	Tinta Continua, WI-FI	2

Equipos usados en la red del Estudio Jurídico "Cedeño y Asociados"

Es vital para las personas que están involucradas en poseer, emplear y utilizar una red. Estas personas involucradas van desde altos directivos, administradores no técnicos, administradores y gerentes que poseen responsabilidades orientadas a la seguridad de la red y/o información, el funcionamiento de la red hasta los responsables de los programas de seguridad general de la empresa y el desarrollo de las políticas de seguridad. Además, es muy importante para cualquier persona que está implicada en el diseño, adopción y planificación de los aspectos de tipo arquitectónico de la seguridad en la red.

La norma **ISO 27033**:

- Da el camino que hay que seguir sobre la forma de identificar y estudiar los riesgos de seguridad de red y el concepto de los requisitos de la seguridad de la red en relación a ese análisis.

- Proporciona una visión total de los controles que la red técnica de arquitecturas, seguridad, controles técnicos asociados, controles no técnicos admiten.

- Proporciona las pautas de conseguir una buena calidad de red arquitecturas técnicas de seguridad y riesgos, control de los aspectos relacionados con los escenarios de la red, el diseño y los escenarios usuales de la red de las zonas de "tecnología".

- Explica de forma muy general los asuntos asociados con los controles de seguridad de la red de operaciones, con la aplicación, y con el seguimiento y evaluación de su aplicación.

La herramienta que nos permitió desarrollar un análisis interno en la red, fue el Software Nessus. según (Sarubbi, 2008) menciona que: "Nessus es una herramienta diseñada para realizar chequeos de vulnerabilidades conocidas de maneras automática y corre sobre múltiples sistemas operativos".

Este software realiza un test del estado de los equipos dentro de la red analizado sus vulnerabilidades, que pueden ser las aprovechadas por personas con mal intencionadas, introduciéndose en la red con intenciones de causar daños, molestar y hasta en ocasiones hurto de la información manejada dentro del Estudio Jurídico.

(Jalca, y otros, 2018) afirma: "Una red informática está conformada por equipos conectados entre sí con el propósito de compartir información; ya que es necesaria para las entidades porque ofrece mucha facilidad en el acceso a la información".

Dentro del Estudio Jurídico analizado, no se ha conocido de un ataque informático, pero este puede haber sucedido sin darse a conocer, es por esto que se enfatiza a tener una seguridad antes de que se agrave la situación.

En el mundo son muchas las empresas que adoptan nuevas medidas de seguridad, en un mundo donde el internet se ha vuelto la principal herramienta de los negocios protegerse es una de las principales medidas que se debe hacer al usar, esto garantizará un mayor nivel de seguridad de la transmisión de información que circula de la red informática de la empresa, además de que optimizará y garantizará un mejor servicio, fiable en cualquier momento.

La información que se maneja y encuentra en el internet es prácticamente ilimitada, esto quiere decir que una persona común puede adquirir conocimientos sobre vulnerabilidades de redes informáticas, conocimientos empíricos y usarlos para acciones delictivas, esto implica que cada vez las redes sean menos seguras y vulnerables a hurto de información y taques que permitan que la red deje de funcionar.

Una red informática dentro de una empresa da muchas facilidades, desde una constante comunicación entre distintos equipos de trabajo y empleados, lo cual reduce gastos y facilita varios procesos que se lleven dentro de la misma, es por la misma razón su importancia de proteger constantemente el acceso y tráfico de la información.

La seguridad aplicada en una red informática se puede clasificar en 4 maneras; la seguridad pasiva, seguridad activa, seguridad física, y seguridad lógica.

La seguridad activa se aplica en medida, siendo usada para la detección de amenazas y si esta se llegara a encontrar generaría mecanismos o procesos que eviten que la amenaza sea un problema en la red, de esta forma evitando inconvenientes. La segura pasiva utiliza medidas que funcionan en forma de contingencia, es decir al momento que se produce un ataque a la red informática esta se encarga que el ataque sea controlado y su daño sea el menor posible por medio de mecanismos de recuperación.

En cuanto a la seguridad física, esta aplica herramientas físicas que permiten proteger físicamente el sistema o la red informática. Y la seguridad lógica tiene la función de asegurar las partes intangibles de la red y sistema informático, estos vienen a ser el Software.

Se ha mencionado diferentes formas de ataque a una red o sistema informático, pero en sí, que se puede decir de ellos teóricamente; una amenaza es el suceso que puede dañar los recursos o procesos que se desarrollen. En cuanto a una vulnerabilidad son errores, fallos o incompetencias del sistema de seguridad que son usados y/o aprovechados por la persona o usuario para efectuar actividades ilícitas que se da paso a que una amenaza tuviere éxito. Es aquí donde entra el personal o persona encarga de la seguridad, este se encarga de evaluar la red e identificar las vulnerabilidades y amenazas, con ese resultado de la evaluación tomar medidas y prevenir riesgos futuros dentro de la red. "Se debe considerar el riesgo como la probabilidad de que una amenaza concreta aproveche una determinada vulnerabilidad." (Castro, y otros, 2018).

Cabe recalcar que estas vulnerabilidades son un fallo en el diseño de la red o de los recursos que pertenecen a ella, estas en ningún momento son creadas, son aprovechadas por el atacante, estos fallos provocan y permiten que el amenazante afecte algún recurso de la red.

Entre las amenazas que pueden existir en una red informática están los eventos naturales, daños físicos, de hardware y software, y de comunicación. Un ejemplo que se puede tomar es la poca o ninguna organización de cableado UTP, protección de energía en los equipos, inundaciones, protección ante incendio, etc.

"Las instalaciones eléctricas son eje fundamental en toda organización debido a que suministra de energía a los diferentes aparatos electrónicos relacionadas a una determinada actividad de una organización" (Castro Gil & otros, 2014)

Una correcta aplicación que se le puede dar al cableado UTP es buscar un cable de categoría correcta para la aplicación del cableado estructurado, así también un ponchado

correcto, en cuanto a la protección de energía, la aplicación de reguladores o UPS para poder dar una mayor vida útil a los equipos informáticos.

Las redes informáticas dentro de una organización o empresa, esta sea de transmisión inalámbrica o por cable, se debe disponer de una optimo y confiable sistema de seguridad ante posibles ataques, ya que un ataque puede generar entre gastos, hurto y alteración de documentos de alta importancia.

Es sabido que dentro de un Estudio Jurídico se manejan mucha documentación importante, ya sea documentos personales como documentos legales que se deben manejar con discreción e internamente en el Estudio Jurídico, es por eso que ser expuestos por un ataque a la red puede resultar afectado en un sin número factores que desacreditarían o afectara de distintas formas la Empresa. Este factor de poca seguridad se podría considerar un riego grave. Según (Tejada, 2019) afirma: "Un riesgo es un evento o conjunto de eventos que pueden poner en peligro la información que posee la entidad; en caso de que se materialice el riesgo, habría varias consecuencias negativas para la entidad".

Se considera un riesgo la probabilidad, sea pequeña o grande de que algo llegase a suceder, ese suceso si ocurriera puede dañar los recursos sean tangibles o intangibles y esto interferir en el desarrollo de las actividades de la empresa. Este riego es medible, pero lo que se busca es que este sea lo más bajo posible.

En la actualidad, ningún sistema es cien por ciento seguro, es por esta razón que se busca que todos los riegos que existan sean controlados. Los riegos siempre podrán existir, pero pueden ser controlados de forma excelente, un ejemplo en riego puede ser un usuario con acceso a gran información que sea engañado por el ataquen haciéndose pasar o suplantando identidad para obtener información delicada de la empresa y así poder infiltrarse, esta información puede ser algún tipo de password o credenciales de accesos.

Para el correcto control de riesgos existen una estandarización o norma que permite regirse en todos los aspectos que se debe tomar encuentra dentro de la empresa para poder obtener un resultado eficiente al tener un incidente que pudiera afectarla.

La norma internacional ISO 27001 es un estándar de seguridad de la información, esta norma fue publicada en el 2005 por la Organización Internacional para Estandarización (ISO), dentro de esta norma se especifica los requisitos necesarios que se deberían cumplir, entre estos son el mantenimiento, implantación y la mejora de un SGSI. Las empresas para obtener esta certificación son evaluadas y así comprobándose su cumplimiento independiente en los controles de seguridad internos.

La norma ISO 27002, en (RAMOS & HURTADO, 2011) especifica lo que debe cumplir la seguridad y estos son; confidencialidad, integridad, disponibilidad, no repudio.

La confidencialidad indica (RAMOS & HURTADO, 2011) según: "que el acceso a la información se realice por la persona adecuada únicamente". La integridad (RAMOS & HURTADO, 2011) concluye: "se refiere a la salvaguardia de la precisión de la información, es decir, asegurarnos que la información se encontrará completa y sin errores." La Disponibilidad (RAMOS & HURTADO, 2011) se refiere a "que las personas autorizadas a acceder a la información lo podrán hacer en el momento en que lo necesiten." (RAMOS & HURTADO, 2011)En cuanto a no repudio hace referencia a garantizar una comunicación en el sistema informático, "que las comunicaciones entre un emisor y un receptor queden garantizadas y que ni el emisor ni el receptor pueden negar que existido la comunicación."

La necesidad e importancia de aplicar una serie de políticas de seguridad en una red conlleva el desarrollo de procedimientos y planes que garantice la protección de los recursos de la red, esta protección incluye en defenderse de posibles amenazas y lo primordial, resguardar los recursos físicos y digitales de la empresa. Así también crear medidas de acción contra incidentes inevitables, como lo pueden ser Desastres Naturales. Incluyendo un constante testeo de la red para saber si existen cambios en la red y posibles mejoras que se puedan aplicar.

La implementación de una política o norma de seguridad se podría tornar difícil si no se tienen los conocimientos necesarios sobre los recursos que se dispone a proteger y los riegos que van a generar las amenazas.

Según (CARPENTIER, 2016) menciono que: “el impacto de las diferentes amenazas varía considerablemente según el efecto sobre la empresa; algunas tienen un impacto sobre la confidencialidad o la integridad de datos, otras actúan sobre la disponibilidad de los sistemas”.

Cumplir estos requisitos dentro de una empresa, como lo es el Estudio Jurídico “Cedeño y Asociados” es de vital importancia ya que este prevendrá sucesos que perjudiquen e estabilicen la red, se produzca algún hurto o plagio de la información, que se den estos sucesos es inevitable por esta razón debe existir un encargado de estos y así mismo tener una capacitación para que no existan problemas y/o si sucedieran le dé solución inmediata al mismo.

Entre las herramientas que se cuenta para el análisis y gestión de los riesgos son los Estándares de seguridad, estos permiten obtener indicios o directrices de la entidad que se administra la seguridad. Así también desarrollar un plan de prevención y contingencia ante cualquier suceso. (López, 2010) nos dice: “El plan de contingencias es un instrumento de gestión que contienes medidas que garantizan la continuidad del negocio protegiendo la información de los peligros que lo amenazan o recuperarlo todo ante un impacto”.

Las herramientas más utilizadas son email, sitios web institucionales, nube, entre otros. Hoy en día el internet a tomado gran campo en los negocios del país como en el mundo, especialmente en trámites legales, sean penales o civiles, consultas de causas, seguimiento de denuncias, notificación de causas legales, entre otras son unas de las principales necesidades de tener un acceso amplio y seguro del internet.

Para obtener una mejor percepción del entorno de la red informática del Estudio Jurídico “Cedeño y Asociados” se realizó una encuesta al asistente así también una breve entrevista, el cual es la persona encargada que organiza la red de forma empírica ya que no

cuenta con conocimientos ni estudio referente a Redes, en la sección de entrevista ante la pregunta ¿Qué tanto conoce del estado de la red inalámbrica? Expreso lo siguiente:

"En cuando al "WI-FI" tiene una clave asignada que pidió el proveedor al momento de realizar la instalación, no ha sido cambiada. Si algún cliente del Estudio la pide se la facilita sin ningún problema, no tenía conocimiento de que podría causar problemas, a veces se pone lento el internet, pero asumo que es problema del proveedor del internet. El cable de red que se distribuye por el Estudio lo realizo un pasante hace 2 años."

Sobre esto se puede aplicar como principal norma, cambiar las credenciales de acceso al router para así mantener un acceso privado a sus configuraciones, de esta forma evitar que clave y configuraciones del WI-FI sean internas al Estudio Jurídico.

"Los Usuarios o visitantes externos no podrán acceder al área determinada a la TI, sin una previa autorización del Responsable a cargo, o de un empleado de la misma" (Gubernamental, 2012)

Luego el entrevistado respondió a un cuestionario de preguntas mediante la cual se obtuvo la siguiente información:

- El estudio jurídico consta con internet, pero este es pésimo ya que tienen una lentitud y latencia notable lo cual se notó mediante un Test.

  Se le aplico un Test de Velocidad para comprobar la calidad del servicio, la misma que resulto ser pésima, notándose un Ping alto lo que produce una lentitud en la red al momento de hacer uso de servicios Web del Estado.
- No conoce sobre que son Políticas de Seguridad, tampoco la aplican dentro de la res.
- Los equipos no cuentan con un departamento especial donde se encuentren los equipos de la red.

Así también se observó que el cableado no tiene una correcta canalización, tampoco tienen un ponchado de calidad, el cable se nota deteriorado ya que este ha sido de una categoría baja.

- Dentro del Estudio Jurídico si existe una red inalámbrica, cuentan con un Wi-Fi el cual es general y tampoco se encuentra con una seguridad aplicada.
- El encuestado menciono que no está seguro si la información que manejen dentro del Estudio Jurídico sea confidencial o esta se mantenga seguro, agrego que las Pc las usan para desarrollar las actividades, pero no se sabe si al usarla estas se mantenga seguras o expuestas.
- Se mencionó que las maquinas usaban Antivirus, el mismo que se encargaba de la detección de Malware y spyware, pero este al ser de paga ya tiene licencia de uso expirada.

Menciona (Larrocha, 2017) que: "Sistemas de detección de malware y spyware son sistemas de detección de intrusos que es un programa para detectar accesos no autorizados a un computador o a una red".

- Los conocimientos que cuenta la persona que administra la red son básicos y han sido adquiridos empíricamente.
- Entiende que el internet es un mundo extenso donde existen varios peligros, algunos conocidos por la noticia local.

A continuación, detallamos amenazas y vulnerabilidades identificadas dentro del Estudio Jurídico, las mismas que pueden ser perjudiciales.

Según autores las vulnerabilidades se definen como:

"Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas" (López, 2010)

“Estado de insuficiencia en un sistema informático o conjunto de sistemas que permiten la materialización de una amenaza afectando las propiedades de disponibilidad, confidencialidad, integridad, autenticidad, no repudio” (Medina, 2014)

Amenazas	Vulnerabilidades
Eventos Naturales	• Los equipos principales de la red se encuentra susceptibles a goteras.
Daño Eléctricos	• Mala organización del cableado de la red y eléctrica. • Variación eléctrica constante. • Los equipos no se encuentran con algún tipo de regulador que proteja.
Falta de Mantenimiento	• No se lleva un mantenimiento preventivo a los equipos en los periodos recomendados.
Hurto de Información	• No se lleva un respaldo de almacenamiento. • Sin restricción de acceso en los Equipos de Cómputo. • Falta de protección en ventanas y puertas de la edificación. • Inasistencia de algún tipo de control ante ataques
Ataques Informático	• Inasistencia política de seguridad. • No se da uso a un sistema de detección de intrusos para identificar ataques. • Contraseñas con nivel bajo de seguridad
Remote Espionage	• .Falta de Activación de Licencia de Antivirus.
Falla del equipo de telecomunicaciones	• Cableado de Red sin certificaciones. • Internet inestable..

Mal uso de los Equipos	• Falta de capacitación para el uso de los equipos. • Uso de los equipos de trabajo para oscio.

Elaborado por **Bryan Caiza Cedeño**

Estas vulnerabilidades van a beneficiar a un atacante, por esta razón se sugiere como solución aplicar debidamente las Políticas de Seguridad, así mismo contratar a una persona con conocimientos suficientes en el área informática para que dé el correcto control a la red y desarrolle mantenimientos sean preventivos o correctivos.

La tecnología se encuentra en constante evolución es por esto que la persona encargada debe evaluar y actualizar la red para así mantenerla lo suficientemente segura para así no se pueda generar el Riesgo.

Según (Chicano, 2019) afirma: "Un riesgo es un evento o conjunto de eventos que pueden poner en peligro la información que posee la entidad; en caso de que se materialice el riesgo, habría varias consecuencias negativas para la entidad".

Además, se procedió a realizar un Análisis con el Software Nessus, antes ya mencionado y como resultado obtuvimos lo siguiente:

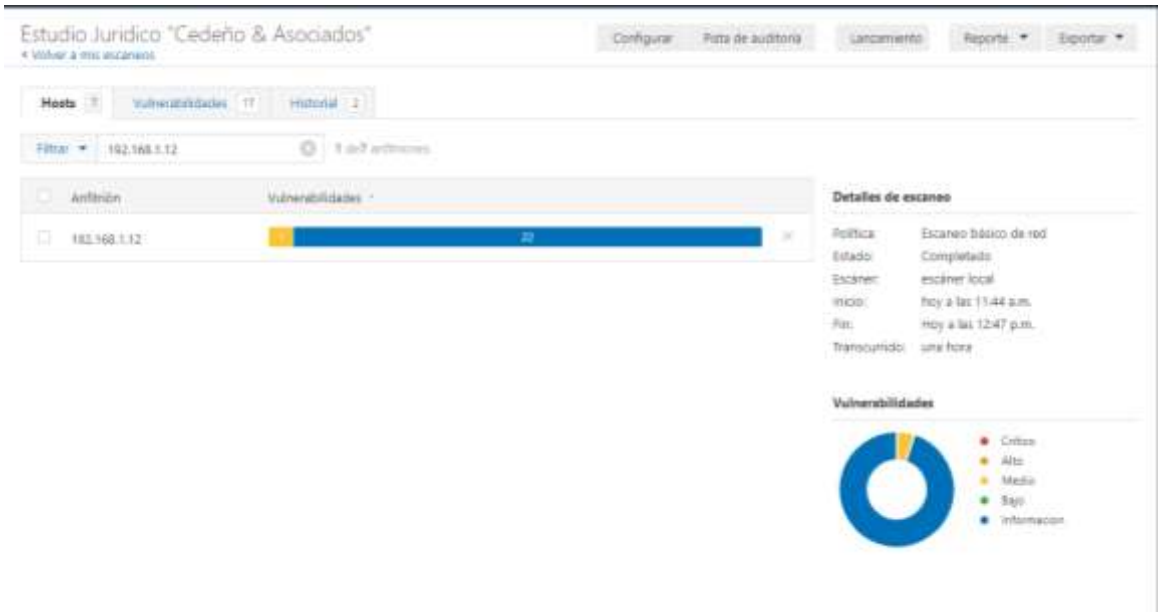

Figura 1 *Escaneo de Vulnerabilidades por medio de la Ip.*

Elaborado por *Bryan Caiza Cedeño*

El análisis se realizó en a la computadora de escritorio principal, la cual es la más expuesta dentro de la red, por medio de su IP se obtuvo el resultado del nivel de vulnerabilidades que tiene el equipo.

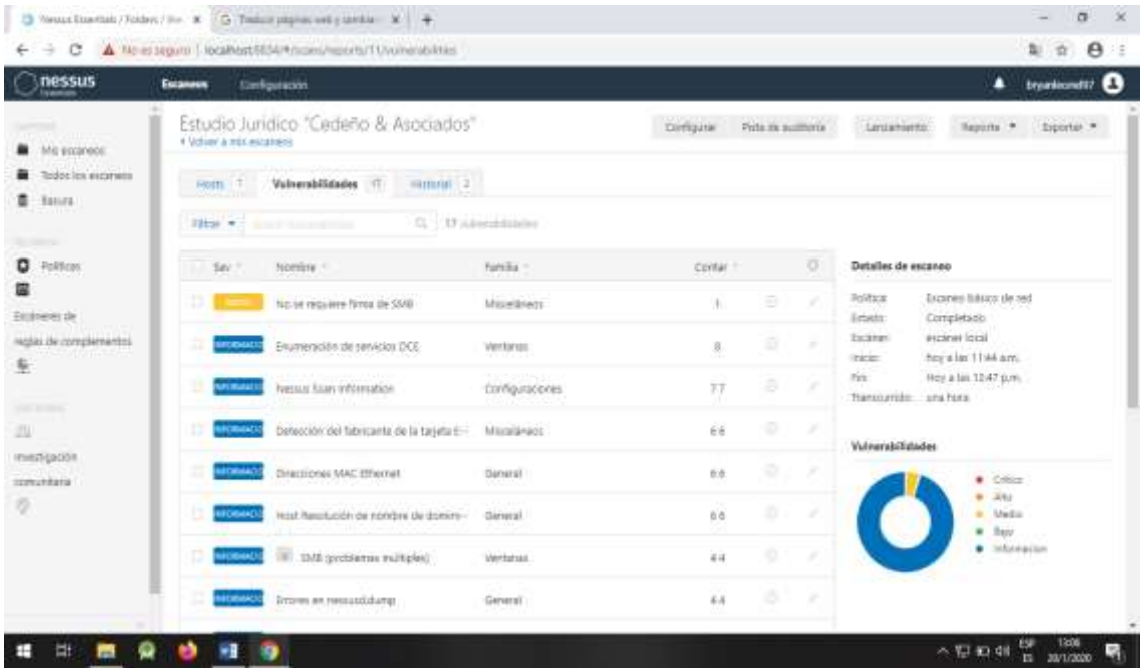

Figura 2 *Resultado de Análisis de vulnerabilidades.*
Elaborado por *Bryan Caiza Cedeño*

En la ***figura 2*** se muestra a detalle las descripciones del análisis realizado al equipo.

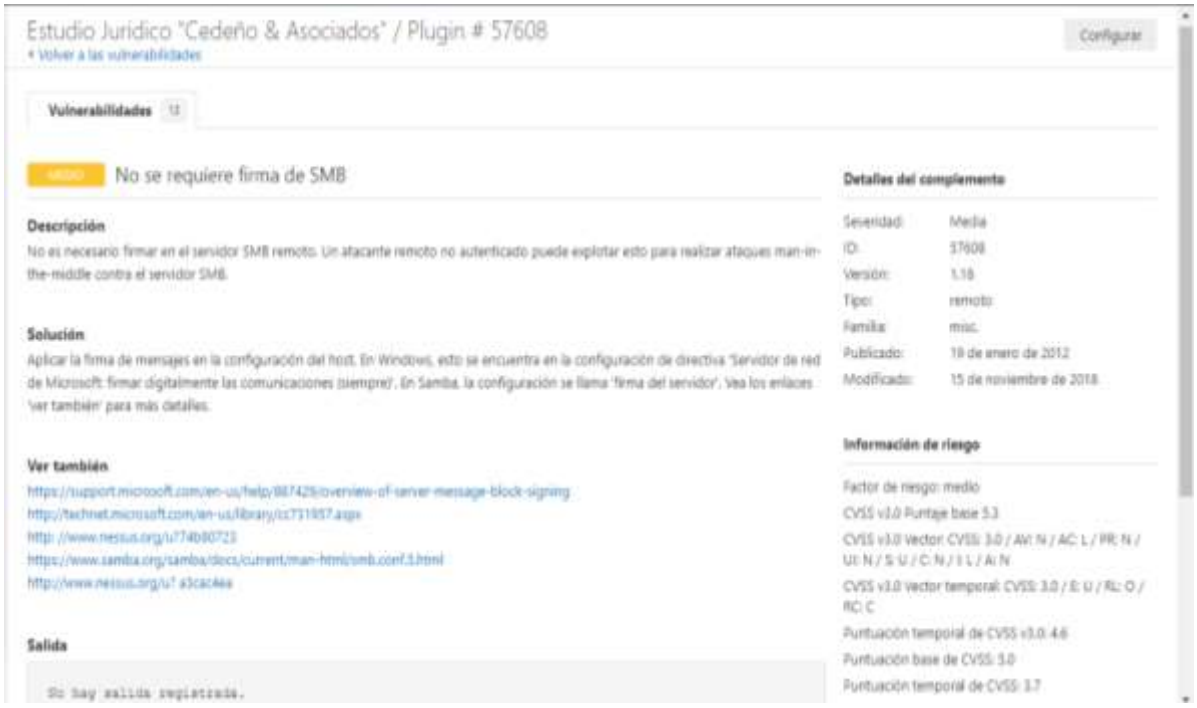

Figura 3 *Vulnerabilidad Media obtenida en el Análisis*
Elaborado por *Bryan Caiza Cedeño*

En la ***figura 3*** tenemos el resultado el análisis de nivel medio, el cual muestra una vulnerabilidad en la parte de la Firma SMB, la cual nos describe que es un Protocolo innecesario de uso, lo que esto ocasionaría es que un atacante remoto explote esa vulnerabilidad para realizar ataques man-in-the-middle contra el servidor SMB.

También nos facilita la solución de *Aplicar la firma de mensajes en la configuración del host.* De esta forma nos podemos apoyar para referir una solución óptima al problema encontrado.

Tenemos el resultado del segundo análisis realizado a la maquina secundaria, del cual obtuvimos mejores resultados. En la ***Figura 4*** el resultado refleja que no tenemos problemas, ósea no se encontró vulnerabilidades existentes.

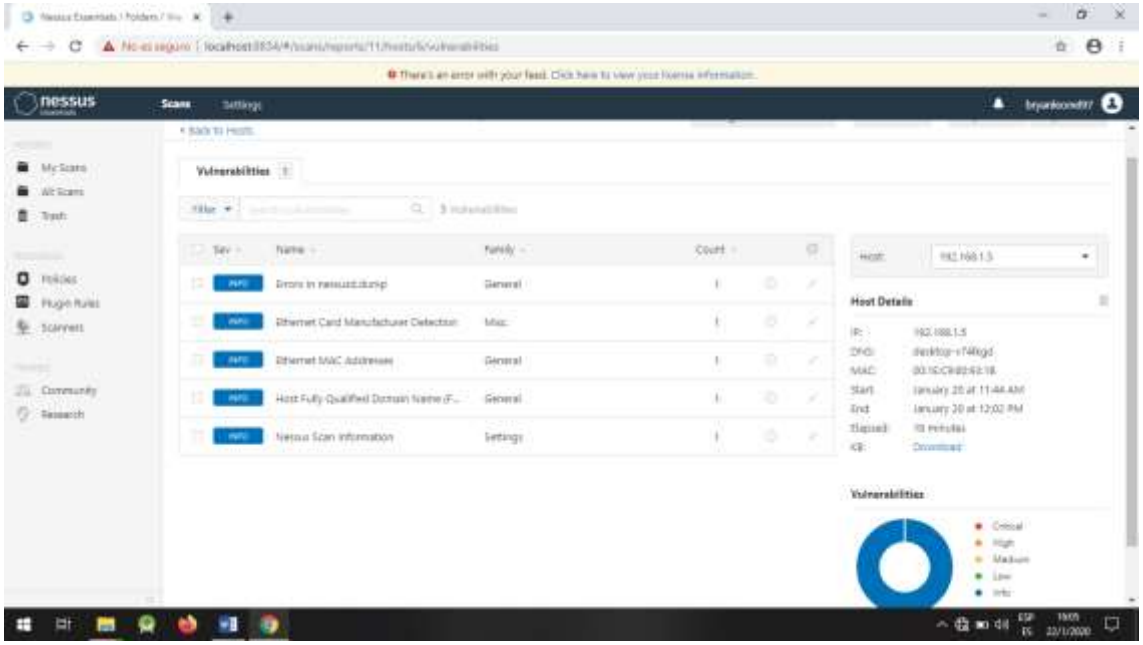

Figura 4 *Resultado del Análisis a la maquina secundaria*
Elaborado por *Bryan Caiza Cedeño*

Este resultado se debe a que la maquina analizada en la ***Figura 4*** no se enfrenta a un constante uso y un alto tráfico en la red, también se notó que es nueva y cuenta con su licencia de Windows vigente. Por lo tanto no devuelve una solución recomendada.

CONCLUSIONES

En este análisis realizado por medio del Estudio de Caso encontramos diferentes vulnerabilidades de nivel alto y medio, estas mismas son ocasionadas por la poca importancia y desconocimiento que se tiene en este aspecto de la Red Informática dentro del Estudio Jurídico.

Una correcta instalación de cableado estructurado, compra de licencias de Software y la aplicación de Políticas de Seguridad es una solución óptima que dará la seguridad a los datos e información que circulen dentro de la red de la entidad mencionada.

Se debe contratar un profesional a fin al área de sistemas, que le dé un monitoreo y prevenga algún tipo de amenaza que pueda ocurrir, una infiltración provocará malestar y esta persona encargada será la que actuará para que el impacto del malestar sea lo menos efectivo.

De las dos máquinas principales analizadas con el Software Nessus, tenemos más vulnerabilidades a ataques en la principal, esto es por que recibe mayor afluencia de tráfico en la red, a diferencia de la maquina secundaria la cual es usada para ámbitos de ofimática, es por esta razón que no arrojó resultados negativos en el Software de análisis.

Bibliografía

CARPENTIER, J.-F. (2016). *La seguridad informática en la PYME.* ENI.

Castellanos, L. (2012). *Seguridad en informática.* Maracaibo.

Castro Gil, M. A., & otros, y. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* Madrid: UNED. UNIVERSIDAD NACIONAL DE EDUCACION A DISTANCIA.

Castro, M. I., Morán, G. L., Navarrete, D. S., Cruzatty, J. E., Anzúles, G. R., Mero, C. J., . . . Merino, M. A. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Alicante: ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.

Chicano, T. E. (2019). *Auditoría de seguridad informática.* IC Editorial.

Gubernamental, D. G. (2012). *MANUAL DE POLÍTICAS DE TECNOLOGÍA*, 28.

Heredero, C. d., Lopez Hermoso, J. J., Romo, S. M., & Medina, S. (2004). *INFORMÁTICA Y COMUNICACIONES EN LA EMPRESA.* Madrid: ESIC.

Jalca, J. J., Castro, V. F., Menéndez, M. D., Quimiz, L. R., Anzúles, G. R., Pilay, Y. H., & Pin, Á. L. (2018). *REDES DE COMPUTADORAS.* Alicante: Área de Innovación y Desarrollo.

Larrocha, E. R. (2017). *Nuevas tendencias en los sistemas de información.* Madrid: Universitaria Ramón Areces.

López, P. A. (2010). *Seguridad Informatica.* Madrid: Editex.

Medina, J. (2014). *Evaluacion de Vulnerabilidades Tic.* Lulu.com.

Ponce Talancón, H. (2006). *Contribuciones a la Economía*, 16.

RAMOS, M. D., & HURTADO, A. G.-C. (2011). *SEGURIDAD INFORMATICA ED.11.* Paraninfo.

Sarubbi, J. P. (2008). *Seguridad Informática: Técnicas de defensa comunes bajo variantes del sistema operativo Unix.* Lujan, Buenos Aires.

Tejada, E. C. (2019). *Auditoría de seguridad informática. IFCT0109.* Malaga: IC Editorial.

ANEXOS

1. **¿El Estudio Jurídico cuenta con internet estable y rapido?**

SI NO

2. **¿Existe alguna política de seguridad informática aplicada?**

SI NO

3. **¿Los equipos informáticos se mantienen en un cuarto con un ambiente adecuado, esto sea un departamento o cuarto el cual permita tenerlo seguros y restringidos?**

SI NO

4. **¿La red informática cuenta con una red inalámbrica?**

SI NO

5. **¿Cree que se mantiene una confiabilidad de los datos e información que transitan dentro de la red?**

SI NO

6. **¿Qué tipo de seguridad poseen o a usado en los ordenadores del Estudio para evitar ataques?**

Antivirus Firewall Software de detención de Malware

Software de Detención de Spyware Ninguno

7. **¿Usted tiene conocimiento acerca de la seguridad informática?**

SI NO

8. **¿Tiene idea de los peligros que puede ocurrir al no contar con una seguridad dentro de la red?**

SI NO