UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2018 – MARZO 2019

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

TEMA:

ESTUDIO DE LAS AMENAZAS Y VULNERABILIDADES DE LA RED INFORMÁTICA DEL CENTRO DE SALUD DE BARREIRO

EGRESADA:

JULISSA MICHELLE PIZA DÍAZ

TUTORA:

ING. ANA DEL ROCIÓ FERNÁNDEZ TORRES

AÑO 2019

TEMA: ESTUDIO DE LAS AMENAZAS Y VULNERABILIDADES DE LA RED INFORMÁTICA DEL CENTRO DE SALUD BARREIRO.

INTRODUCCIÓN

En la actualidad la red informática se considera muy importante para cualquier institución por los beneficios contribuyen a la sociedad, es de mucha importancia conocer las amenazas que pudieran afectar la red ya que a consecuencia de algunas vulnerabilidades podrían aparecer amenazas que pueden crear problemas para que no tenga un buen funcionamiento la red

Todas las redes pueden llegar a ser vulnerables porque existen muchos equipos conectados entre sí compartiendo información existe el riesgo de que un atacante pueda vulnerar la red accediendo a un equipo y después propagarse al resto de los equipos conectados a la red.

Las amenazas y vulnerabilidades están relacionadas con la intercepción de los datos de la entidad por personas no autorizadas; ya que la prioridad de la red informática es la transmisión de los datos.

En el Centro de Salud Barreiro se realizó un estudio de las amenazas y vulnerabilidades de la red informática para conocer los riesgos que esta expuesta la red.

Este estudio se basará en el uso de las metodologías de investigación lo cuales son cualitativa y de campo que ayudarán a la resolución del mismo donde se utilizó las siguientes técnicas la entrevistas, observación directa, con la finalidad de tener conocimiento sobre la situación actual de la red informática; y a su vez cumplir con el objetivo de identificar las amenazas y vulnerabilidades que afectan el funcionamiento de las red, además se realizó un escaneo mediante la herramienta conocida en cuanto a seguridad la cual es Nessus, para de esta manera determinar las vulnerabilidades de la red informática.

La línea de investigación que está regido el estudio de caso es Desarrollo de sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos; y como sublínea, Procesos de transmisión de datos y telecomunicaciones.

DESARROLLO

El Centro de Salud Barreiro está ubicado en la Parroquia Barreiro Viejo perteneciente al cantón Babahoyo Provincia Los Ríos.

Hoy en día las organizaciones están adoptando tecnologías para estar comunicados en cualquier lugar del mundo y a su vez acceder a su información. También existen servicios y equipos que brindan la capacidad de almacenar toda la información y sus páginas web que posee la organización.

Muchas organizaciones utilizan el internet para darse a conocer y a su vez promocionar sus servicios o productos que ofrecen.

Para tener un buen funcionamiento de la red informática debemos de tenerla segura para cualquier problema o riesgo que puedan afectarla, ya que la seguridad de la red es de mucha importancia porque nos ayuda a respaldar la confidencialidad e integridad de los datos de la organización. Cuando existe un abuso a la seguridad de la red pueden existir daños a la estabilidad de la red y pérdida de información importante que posee la organización. Surge la necesidad de identificar las amenazas y vulnerabilidades en la red informática en las que se encuentra expuesta, para tener así una percepción sobre la situación actual de la red.

La finalidad de este estudio de caso es identificar las amenazas y vulnerabilidades existentes en la red informática del Centro de Salud Barreiro y dar posibles soluciones a dichos inconvenientes.

Este estudio de caso se trata de dar a conocer las amenazas y vulnerabilidades que tiene la red informática y también para mantenerla segura la red; así como también se procura no indagar sobre la existencia (cantidad y descripción) de equipos y software, que posea la entidad.

El Centro de Salud Barreiro en la actualidad no cuenta con un monitoreo constante de la red que ayude a determinar las amenazas y vulnerabilidades que pueda tener la red informática.

Unos de los problemas del Centro de Salud es que no existen políticas de seguridad en la red informática lo cual puede ocasionar infiltración de ciertos atacantes que podrían sustraer o divulgar la información importante de la entidad.

En La siguiente matriz se muestra el análisis FODA que identifican las principales fortalezas, oportunidades, debilidades y amenazas que tiene la red informática y la entidad.

FORTALEZAS	**OPORTUNIDADES**
Uso de antivirus. Uso de firewalls.	Pueden adoptar nuevas tecnologías dentro de la entidad.
DEBILIDADES	**AMENAZAS**
No constan con políticas de seguridad. El cableado del internet se encuentra en lugares que están disponible para el usuario y desorganizados. Déficit en el acondicionamiento de aire para los equipos.	Daños eléctricos. Suciedad en el área donde se encuentran los equipos.

Elaborado por Julissa Piza Díaz

"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.” (Noticias de Seguridad Informática, 2016)

Debido a esto toda entidad que presta este servicio, tiene que asegurar que la información transmitida por este medio no sea accesible ni manipulada por personas que no estén autorizadas.

El presente caso de estudio se desarrolló mediante la metodología cualitativa, donde se utilizó la técnica de la entrevista realizada a la persona que es encargada de la red informática en el Centro de Salud Barreiro para tener datos exactos del problema, así como también se obtuvo información mediante la metodología de campo con la técnica de la observación que nos permitió conocer todos los equipos que posee la entidad y sus conexiones que forman parte de la red informática.

Una vez recopilada la información, se hará uso de una herramienta para el estudio de las amenazas y vulnerabilidades en la red informática, así se podrá conocer los riesgos o problemas que se presenta en el Centro de Salud Barreiro y cuáles serían las medidas a tomar del personal que labora en el mismo.

Al momento de realizar el escaneo de la red se solicitó el permiso al encargado del Centro de Salud para determinar el nivel de amenazas y vulnerabilidades que existe en la red informática. Los principales beneficios al realizar el escaneo tenemos: Reducción de los riesgos que pueden generar robos o divulgación de información, Mejoras en el Centro de Salud permitiendo garantizar la integridad, confidencialidad de la información a través de la red.

Para realizar el escaneo de la red informática se utilizó el programa Nessus. “Nessus es una herramienta diseñada para realizar chequeos de vulnerabilidades conocidas de maneras automática y corre sobre múltiples sistemas operativos” (Sarubbi, 2014)

Este programa encuentra las posibles vulnerabilidades, que pueden ser aprovechadas por terceros para introducirse en la red para causar daños, molestias y en ocasiones el plagio de información.

"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." (Regalado, y otros, 2018)

En los países están adoptando nuevas medidas de protección contra amenazas informáticas lo cual le va garantizar un nivel de protección adecuada y segura en la transmisión de información a través de la red informática; además brindar un mejor servicio y así la comunicación bilateral sea fiable en cualquier momento." (Ortiz, 2014)

Actualmente las redes informáticas manejan una cantidad de información prácticamente ilimitada, resultando esto en que los usuarios tienen acceso a información sobre vulnerabilidades motivo por el cual tienen cada vez más experiencia y permite que personas las conozcan. Esto vuelve a las redes cada vez menos seguras y más vulnerables a robos de información o ataques que pueden inhabilitar la red.

La utilización de las redes informáticas en una entidad facilita la comunicación entre los empleados, la cual reduce gastos tanto hardware como de software y ayuda a mejorar la integridad de los datos y la seguridad en el acceso de la información.

Las redes informáticas son uno de los mayores peligros que existen en la seguridad de un sistema informático, ya que en la actualidad la mayoría de las amenazas provienen desde el exterior, a través de la red. Para proteger y preservar la seguridad en una red informática se dispone de una serie de herramientas del sistema operativo y dispositivos de red. (Valdivia, 2015)

La seguridad en la red se clasifica de la siguiente manera: seguridad activa, pasiva, física y lógica. La seguridad activa son medidas que se utilizan para detectar amenazas y en el caso de detectarla generar mecanismos para evitar el problema. La seguridad pasiva son medidas utilizadas para que una vez que se produzca el ataque en la seguridad hacer que el impacto sea menor posible y activar mecanismos de recuperación. Seguridad física se utilizan barreras físicas para proteger físicamente el sistema informático y a la red. Seguridad lógica se encarga de asegurar la parte del software de los equipos informáticos y de la red.

Las amenaza son sucesos que pueden dañar a los procedimientos o recursos, mientras las vulnerabilidades son los fallos de los sistemas de seguridad o en los propios que el usuario utiliza para desarrollar las actividades que permitirán que una amenaza tuviese éxito a la hora de generar un problema. El principal trabajo de un responsable de la seguridad es la evaluación de los riesgos identificando las vulnerabilidades, amenazas y en base a esta información evaluar los riesgos a los que están sujetos las actividades y recursos. Se debe considerar el riesgo como la probabilidad de que una amenaza concreta aproveche una determinada vulnerabilidad. (Romero, y otros, 2018)

Las vulnerabilidades son fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso.

Existen diferentes amenazas como daños físicos, eventos naturales, de hardware, de software y de comunicación por ejemplo: Mala organización del cableado de red y de energía; Incendios; Inundaciones, Desastres provocados por la naturaleza; Mala conservación de los equipos; Instalación y configuración de programas que pueden ser perjudiciales para la entidad; Líneas de comunicación sin protección.

Las redes informáticas de una entidad, ya sea por cableado o inalámbricas, es indispensable disponer de un óptimo servicio informático para evitar posible amenazas. Los posibles ataques a una red pueden ocasionar perdidas de dinero debido a los daños o robos de información.

"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." (Chicano, 2014)

El análisis de riesgos informáticos es un proceso que identifica los activos de la entidad, sus amenazas y vulnerabilidades así de como su probabilidad de que ocurran y el impacto que ello tendría en la entidad con el fin de determinar los controles adecuados para disminuir o evitar amenazas. (Menéndez, 2016)

El riesgo es la probabilidad de que algo negativo suceda dañando los recursos tangibles o intangibles y por tanto impidiendo desarrollar la labor profesional.

La entidad siempre esta amenazada de sufrir algún daño en su sistema informático, daño que pueden provocar pérdidas de muchos tipos, y las amenazas son mayores cuando los sistemas de información presentan ciertos puntos débiles llamados vulnerabilidades de manera que se tiene mayor o menor riesgo dependiendo de la cantidad de vulnerabilidades que se tengan. (Baca Urbina, 2016)

Para proteger la información que poseen las entidades existe un estándar o norma que acoge todos los aspectos que deben tener en consideración las entidades para asegurar eficientemente sus datos frente a todos los probables incidentes que pudieran afectarla.

La norma internacional ISO 27001 es una norma relativa a la seguridad de la información publicada en 2005 por la Organización Internacional para la Estandarización (ISO). Esta norma

específica los requisitos necesarios para el establecimiento, implantación, mantenimiento y mejora de un Sistema de Gestión para la Seguridad de la Información (SGSI). La entidad que se certifica en esta ISO demuestra que los controles de seguridad internos se realizan de forma independientes, Cumple con los requisitos de la gestión corporativa. (Peña Calvo, 2015)

En la norma ISO 27002 describe los pilares fundamentales de la seguridad informática que son la Confidencialidad que significa que el acceso de la información se realice por la persona adecuada únicamente; Integridad que salvaguarda la precisión de la información; Disponibilidad que las personas autorizadas a acceder a la información lo podrían hacer en el momento en que lo necesiten; No repudio garantiza la comunicación en un sistema informático. (Garcia, Hurtado, & Alegre, 2014)

Definir políticas de seguridad en la red informática significa desarrollar procedimientos y planes que resguarden los recursos de la red en contra de la perdida y daño de la misma. Para la creación de políticas; se debe tomar en cuenta los recursos que se tratan de proteger, las posibles amenazas, la importancia del recurso a proteger y las medidas que se pueden ejecutar para proteger los recursos. Luego examinar periódicamente la red para observar si deben realizar cambios en los objetivos de trabajo de la política de seguridad.

Puede llegar a ser difícil la implementación de una política de seguridad si no cuentan con los conocimientos necesarios sobre lo que se desea proteger y de los orígenes de amenazas.

La política de seguridad tiene como objetivo definir la protección de los sistemas de información de la entidad. Comprende un conjunto de bases para definir estrategia, directrices, procedimientos, códigos de conducta y normas organizativa y técnica. Implica la implementación de una seguridad al uso de los equipos y de la red informática. (Carpentier, 2016)

Los requerimientos para la seguridad dentro de la entidad son de mucha importancia porque nos permite elaboras normas para evitar sucesos perjudiciales como inestabilidad de la red, divulgación o plagio de la información; es inevitable que en la entidad ocurran riesgos por lo cual es de mucha importancia que el personal que laboran en la entidad estén debidamente capacitados para que no existan problemas o puedan solucionarlos de manera adecuada.

Una de las herramientas para el análisis y gestión de riesgos son las políticas de seguridad que recoge las directrices de una entidad con respecto a la seguridad de la información, así como el plan de contingencias.

"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." (Aguilera López, 2015)

Las herramientas más utilizadas en la web son: correos electrónicos, inteligencia de negocios y la nube; las tecnologías de la información y la comunicación (TIC) han logrado una gran notabilidad, especialmente al volverse el uso de internet en el ámbito de la salud.

Para obtener una percepción general sobre el funcionamiento de la red informática en el Centro de Salud Barreiro, se realizó la entrevista a la persona encargada de la red lo cual expresó lo siguiente:

"Existen muchas personas que tienen acceso a la red de la entidad debido que el router no se encontraba protegido por lo que la clave del dispositivo estaba expuesta y esto generaba que la red sea lenta e inconsistente."

Luego el entrevistado respondió el cuestionario de preguntas mediante las cuales se obtuvo la siguiente información:

- Utiliza firewall para proteger la red contra ataques o infecciones por virus.

"Firewall permite definir distintos niveles de acceso a la información de manera que en una entidad dada, cada grupo de usuarios tendrá acceso solo a servicio e información que le son estrictamente necesarios. (Junta de Adalucia, 2016).

- Utiliza antivirus.
- Dispone de conexión inalámbrica.
- No cuentan con sistemas de detección de malware y spyware para identificar los ataques a la seguridad.

  "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." (Ruiz, 2017)
- El cableado del internet y el router no están en lugares cerrados por lo cual pueden ser vulnerables.
- Falta del acondicionamiento de aire para los equipos lo que pudiera causar el deterioro o bajo rendimiento de los mismos.
- No constan de políticas de seguridad.
- No se mantiene confidencialidad de los datos en la red.
- El nivel de velocidad de la red es lenta.

A continuación se muestra la tabla donde se detalla las amenazas y vulnerabilidades identificadas para la red informática del Centro de Salud Barreiro que pueden ser perjudiciales.

Tabla 1. *Identificación de amenazas y vulnerabilidades*

AMENAZAS	**VULNERABILIDADES**
Eventos naturales	• Ubicación en un área susceptible de inundación. • Variaciones de temperatura.
Daños eléctricos	• Red energética inestable. • Variaciones de tensión. • Mala organización del cableado de la red y de la energía.
Destrucción de los equipos Polvo	• Falta de esquemas de remplazo periódico • Susceptibilidad a la humedad, el polvo y a la suciedad.
Hurto de información	• Almacenamiento sin protección. • Falta de cuidado en la disposición final. • Copia no controlada. • Falta de protección física de las puertas y ventanas de la edificación. • Falta de autorización de los recursos de procesamiento de la información. • Falta de mecanismos de monitoreo establecidos para las brechas en la seguridad.

Procesamiento ilegal de datos	• Habilitación de servicios innecesarios. • Falta de mecanismos de monitoreo.
Ataques informáticos	• No existen políticas de seguridad • No utilizan sistemas de detección de intrusos para identificar ataques. • Contraseñas predeterminadas o débiles en seguridad.
Espionaje remoto	• Líneas de comunicación sin protección. • Trafico sensible sin protección. • Arquitectura insegura de la red. • Transferencia de contraseñas autorizadas. • No cuenta con un antivirus actualizado
Falla del equipo de telecomunicaciones	• Conexión deficiente de los cables. • Existe inestabilidad en el internet.
Saturación del sistema de información	• Gestión inadecuada de la red (capacidad de recuperación de enrutamiento).
Falla en los equipos	• Falta de planes de continuidad • Falta de mantenimiento correctivo y preventivo.

Error en el uso de los equipos	• Entrenamiento insuficiente de seguridad. • Uso incorrecto del software y hardware. • Falta de conciencia acerca de la seguridad. • Falta de políticas sobre el uso de correos electrónicos. • Falta de procedimientos para el manejo de información clasificada.

Elaborado por Julissa Piza Díaz

Además al realizar el escaneo de la red informática del Centro de Salud Barreiro se procedió a utilizar el programa Nessus se pudo evidenciar los siguientes resultados:

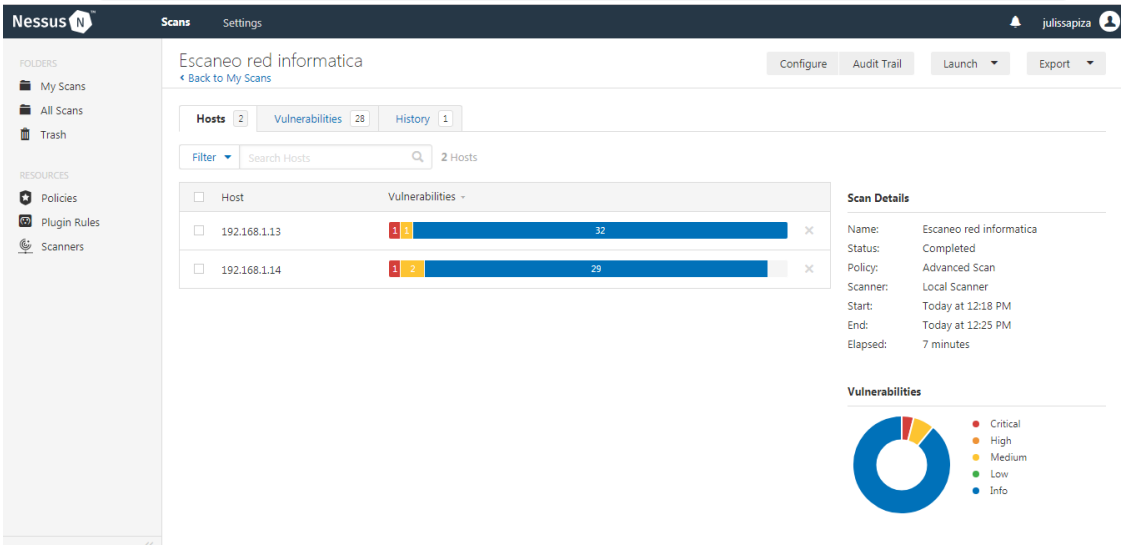

Figura 1 *Escaneo de Vulnerabilidades con Nessus*
Elaborado por *Julissa Piza Díaz*

Como se muestra en la imagen se hizo el escaneo de vulnerabilidades al rango de IPs que tiene la red informática con Nessus, dando como resultado el nivel de vulnerabilidades que tiene cada equipo.

En la ***figura 2*** se muestran un desglose del análisis de uno de los equipos.

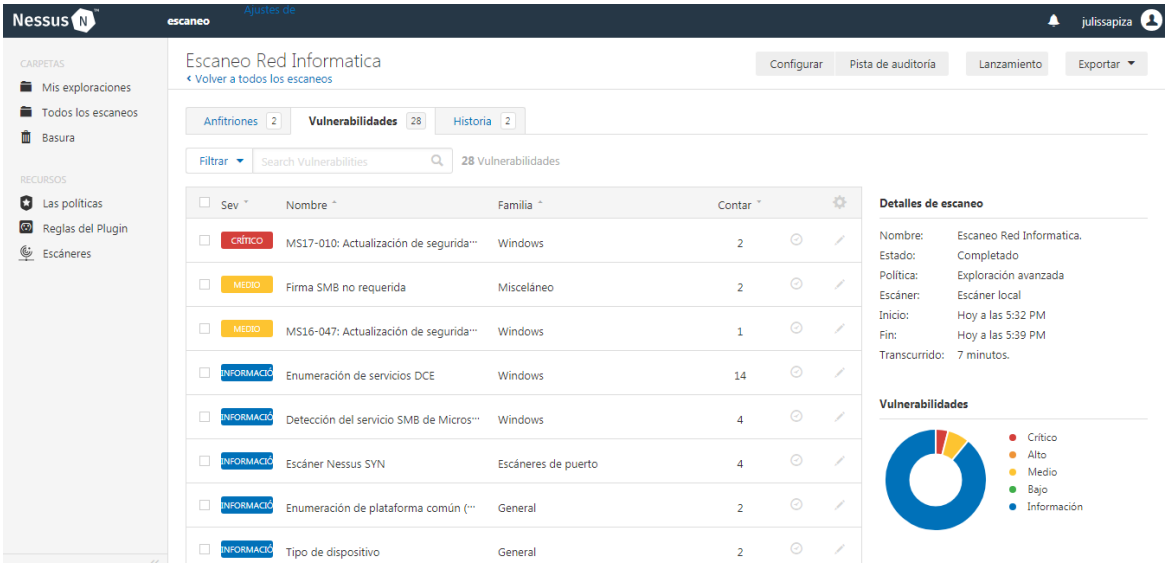

Figura 2 *Análisis de la IP del equipo*
Elaborado por *Julissa Piza Díaz*

En la ***figura 3*** se visualiza el análisis de una vulnerabilidad critica que se trata sobre Actualización de seguridad para el servidor de Microsoft Windows, cuya vulnerabilidad es que el host remoto de Windows se ve afectado por ejecuciones remotas de código debido al manejo inadecuado de ciertas solicitudes y también de divulgación de información debido a un manejo inadecuado de ciertas peticiones.

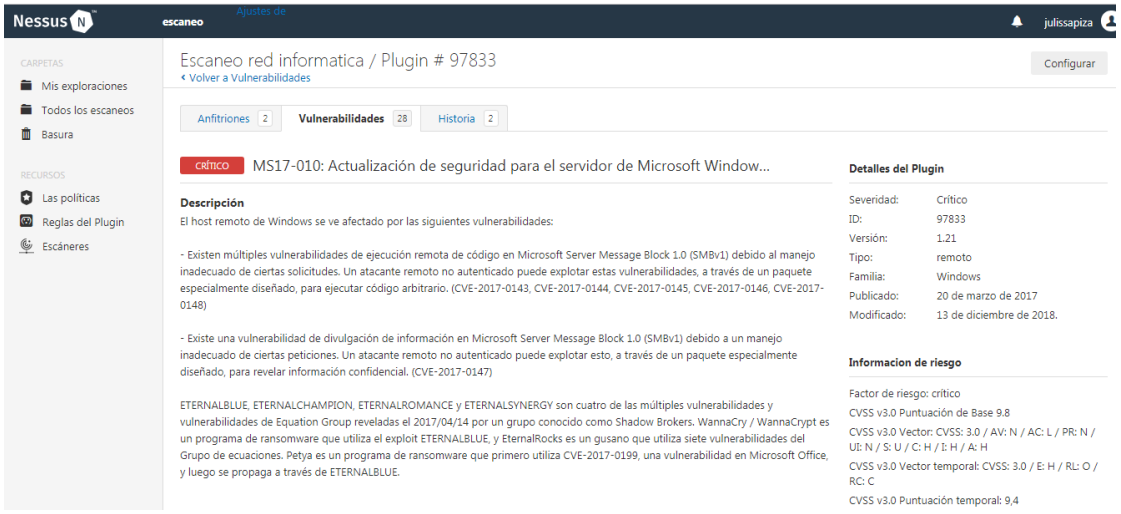

Figura 3 *Vulnerabilidad Crítica*
Elaborado por *Julissa Piza Díaz*

En la ***figura 4*** se visualiza el análisis de una vulnerabilidad media que se trata sobre Firma SMB no requerida, cuya vulnerabilidad es que la firma no es necesaria en el servidor SMB remoto y un atacante puede realizar ataques de intermediario contra el servidor SMB.

Figura 4 *Vulnerabilidad Media*
Elaborado por *Julissa Piza Díaz*

En la ***figura 5*** se visualiza el análisis de una vulnerabilidad media que se trata sobre Actualización de seguridad para protocolos remotos SAM y LSAD, cuya vulnerabilidad es que el host remoto de Windows se ve afectado por elevación de privilegios en los protocolos ya mencionados debido a una negociación de nivel de autenticación incorrecta en los canales de llamada a procedimiento remoto (RPC).

Figura 5 *Vulnerabilidad Media*
Elaborado por *Julissa Piza Díaz*

Los problemas encontrados en la red informática son los siguientes: No constan con políticas de seguridad; No contar con un programa de protección contra los ataques; Falta de conocimiento en el personal encargado del área; No existe cambio de los equipos que se encuentra deteriorados; Contraseñas predeterminadas o débiles en seguridad; Inestabilidad en el servicio de internet; No cuenta con un antivirus actualizado; Conexión deficiente de los cables.

CONCLUSIONES

Las amenazas y vulnerabilidades que se encontraron en este estudio de caso se muestra que un alto nivel de vulnerabilidad y existe escaso nivel de seguridad debido a la poca importancia que tiene la red informática del Centro de Salud Barreiro.

La implementación de políticas de seguridad informáticas en el Centro de Salud Barreiro es una solución integral que asegura la protección y resguardo de la información administrada en toda la entidad; con ello se debe de tener un método de prevención y control de daños e incidencias que afecte el correcto desempeño de la red informática y demás equipos directamente conectados en la red.

La red informática no se encuentra totalmente segura debido a que no existe un monitoreo constante para identificar las posibles infiltraciones de atacante.

BIBLIOGRAFÍA

Aguilera López, P. (2015). *Seguridad Informática.* Editex.

Baca Urbina, G. (2016). *Introducción a la Seguridad Informática.* México: Grupo Editorial Patria.

Carpentier, J.-F. (12 de Noviembre de 2016). *La seguridad informática en la PYME.* Barcelona: Ediciones ENI.

Chicano, E. (2014). *Auditoría de seguridad informática* . Málaga: IC Editorial.

Garcia, A., Hurtado, C., & Alegre, M. (2014). *Seguridad Informatica.* Madrid: Parainfo, SA.

Junta de Adalucia. (2016). *Auxiliar Administrativo.* Madrid: Editorial CEP S.L.

Menéndez, S. (2016). *Gestión de redes telemáticas.* España: Elearning S.L.

Noticias de Seguridad Informática. (2 de Marzo de 2016). *Noticias de Seguridad Informática*. Obtenido de http://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/

Ortiz, A. (2014). *Seguridad de la Información.* Guatemala: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.

Peña Calvo, N. (2015). *Gestión y control de los sistemas de informacion.* España: Elearning S.L.

Regalado, J., Romero, V., Azúa, M., Murrilo, L., Parrales, G., Campozano, Y., y otros. (2018). *Redes de Computadoras.* España: Area de Innovacion y Desarrollom S.L.

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, y otros. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Área de Innovación y Desarrollo,S.L.

Ruiz, E. (2017). *Nuevas tendencias en los sistemas de información.* Madrid: Centro de estudios Ramón Areces, S. A.

Sarubbi, J. P. (2014). *Seguridad Informatica.Tecnicas de Defensa.* Buenos Aires: Universidad Nacional de Lujan.

Valdivia, C. M. (2015). *Redes Telemáticas.* Madrid: Parainfo.

ANEXOS

1. **¿La entidad tiene conexión permanente a Internet?**

   Si No

2. **¿Existen políticas de seguridad informática?**

   Si No

3. **¿Los equipos informáticos cuentan con un acondicionamiento de aire adecuado?**

   Si No

4. **¿La red dispone de conexión inalámbrica?**

   Si No

5. **¿Los equipos de red (router, cableado, conexiones a Internet) se encuentran en lugares cerrados con llaves y con acceso restringido?**

   Si No

6. **¿Cree que se mantiene la confidencialidad de los datos en la red del Centro de Salud?**

   Si No

7. **¿Qué tipo de seguridad poseen los ordenadores para evitar robos de información?**

   Firewall Antivirus

   Software de detección de malware Ninguna

   Software de detección de spyware

8. **¿Cómo considera el nivel de velocidad de la red?**

   Rápida Normal Lenta

9. **¿Usted tiene conocimiento acerca de seguridad de información?**

   Sí No