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 INGENIERÍA EN SISTEMAS

TEMA:

Análisis de Vulnerabilidades de la Red LAN del gobierno Autónomo Descentralizado de la Parroquia Pimocha.

EGRESADA:

Sammy Lorenza Moreno Duarte

TUTORA:

Ing. Ana Fernández Torres

AÑO 2020

INTRODUCCIÓN

En la actualidad, el uso de redes informáticas es muy importante en las organizaciones, porque permite acceder, enviar y recibir información muy valiosa y optimizar el tiempo de ejecución de procesos que anteriormente se realizaban manualmente. Pero, así como esta tecnología ha traído ventajas también tiene sus desventajas debido a consecuencias de algunas vulnerabilidades pueden causar problemas en el funcionamiento de la red, por eso existen políticas que se tienen que aplicar debidamente para evitar fugas de información.

El Gobierno Autónomo Descentralizado de Pimocha es una institución pública que promoverán e implementarán en conjunto con los actores sociales, los espacios, procedimientos institucionales, instrumentos y mecanismos reconocidos expresamente en la Constitución y la ley, así como otras expresiones e iniciativas ciudadanas de participación necesarias para garantizar el ejercicio de este derecho y la democratización de la gestión pública en sus territorios, cumpliendo en su contenido con los parámetros de transparencia, eficiencia y acceso a la información descritos en la ley de Transparencia.

El presente caso de estudio implementa la metodología descriptiva porque se logra entender situaciones sobresalientes a través de los procesos que se realizan en una red informática, y además permite expresar los datos obtenidos en términos cualitativos proporcionando una gran cantidad características de la red muy valiosas. Se utilizará como herramienta a la entrevista para recolección de la información, además del uso de una ficha de observación para detectar las anomalías físicas de la red durante una visita al GAD Parroquia de Pimocha.

En el desarrollo de este estudio de caso se analizan los datos recopilados del GAD Parroquial de Pimocha para lo cual se emplea el método analítico-deductivo de manera que permitirá brindar un análisis respectivo sobre las posibles vulnerabilidades de la red LAN, y así emplear herramientas de recolección de información y análisis como el sistema operativo Kali Linux ya que se harán las pruebas necesarias para decretar el margen de vulnerabilidades que tiene la red LAN del GAD.

Para el desarrollo del presente estudio de caso se debe tomar en consideración la línea de investigación desarrollo de sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos donde la sublínea retribuye a procesos de transmisión de datos y telecomunicaciones, aplicando una metodología de un escaneo en la red LAN del GAD de la parroquia Pimocha.

DESARROLLO

El Gobierno Autónomo Descentralizado de Pimocha es una entidad pública que tiene autonomía administrativa, perteneciendo al nivel de gobierno parroquial. Actualmente esta entidad cuenta con una infraestructura de Red en la cual se gestionan procesos internos en la institución, y en la cual se desea conocer si cumple o no con los parámetros adecuados en su configuración. La red LAN del GAD de Pimocha, cumple su objetivo de transmisión de datos entre departamentos y la información que viaja por los medios de la red es de suma importancia para la institución.

Una red es una colección de computadoras, dispositivos de red, periféricos u otros dispositivos conectados entre sí para permitir el intercambio de datos. Un excelente ejemplo de una red es Internet, que conecta a millones de personas en todo el mundo. Una red consta de dos o más computadoras que están vinculadas para, intercambiar archivos o permitir comunicaciones electrónicas. Las computadoras en una red pueden estar conectadas a través de cables, líneas telefónicas, ondas de radio o satélites. (Caballero González, 2017)

Actualmente, un tema de vital importancia es la seguridad de la información, debido a que la gran mayoría de las instituciones usan en gran parte de sus actividades equipos informáticos. Hacer uso TICS, y el uso de redes de comunicación de datos tolera a tener el riesgo de que la trasmisión de la información sea vulnerada, es por eso que la seguridad de la información se convierte en uno de los temas con mayor preocupación para las instituciones actuales. La seguridad informática significa proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados. Los términos seguridad de la información,

seguridad informática y garantía de la información se usan indistintamente con frecuencia.

Si bien es cierto, en los últimos 20 años se ha adoptado de una forma sistemática el uso de las tecnologías de la información en el sector público. Los procesos que se realizan en el sector público, que antes se basaban archivar los documentos en archiveros, han evolucionado con el uso de las tecnologías de la información hasta convertirse en departamentos que utilizan programas informáticos especiales para garantizar la seguridad de los datos de los ciudadanos. (Baca Urbina, 2016)

La problemática existente en el GAD de la parroquia Pimocha se basa en el bajo cumplimiento de las medidas de seguridad informática que garantizan la seguridad física y lógica de la red. La seguridad de la información tiene que ver con proteger la información del acceso no autorizado. Es parte de la gestión de riesgos de la información e implica prevenir o reducir la probabilidad de acceso, uso, divulgación, interrupción, eliminación, corrupción, modificación, inspección o registro no autorizados. Si ocurre un incidente de seguridad, los profesionales de seguridad de la información están involucrados en la reducción del impacto negativo del incidente. La información de la nota puede ser electrónica o física, tangible o intangible. (Chicano Tejada, 2015)

La información es uno de los activos más importantes de la organización. Para una organización, la información es valiosa y debe protegerse adecuadamente. La seguridad consiste en combinar sistemas, operaciones y controles internos para garantizar la integridad y confidencialidad de los datos y los procedimientos de operación en una organización. El historial de seguridad de la información comienza con el historial de seguridad informática. Una vulnerabilidad es una debilidad de seguridad en un sistema

informático que permite el acceso no autorizado o no deseado. Por ejemplo, un navegador de Internet podría tener una vulnerabilidad que bloquea el navegador o permite que alguien lea o copie archivos de su computadora cuando visita su sitio. (Kremling & Parker, 2017)

Una amenaza, según la seguridad informática, puede ser cualquier cosa que aproveche una vulnerabilidad para violar la seguridad y alterar, borrar, dañar objetos u objetos de interés. La seguridad de la red se compone de componentes de hardware y software diseñados para proteger los datos y la información que se procesan en la red. Además, estos componentes proporcionan medidas preventivas configuradas para proteger la infraestructura de la red y sus datos contra el acceso no autorizado, la modificación de datos, la corrupción y la divulgación inadecuada. En última instancia, la seguridad de la red está diseñada para crear un entorno seguro donde los usuarios de computadoras, programas de software y aplicaciones móviles pueden realizar actividades informáticas o digitales sin vulnerabilidades de red.

El presente trabajo de investigación, sólo como objetico analizar el estado actual de la red referente a la configuración, transmisión y seguridad de la información del GAD de Pimocha. No se realizarán cambios o modificaciones en dichas configuraciones en la red presente en el GAD de la parroquia Pimocha, debido a que el presente tiene como finalidad identificar, exponer, evaluar y recomendar las soluciones pertinentes para mantener segura la transmisión de los datos y la infraestructura de la red de la institución. Tampoco tiene como objetivo gestionar compras de nuevos equipos tecnológicos de red que sean necesarios para la organización.

Este trabajo de investigación hace uso de la metodología la investigación descriptiva, porque se pretende detallar qué tipos de medidas y protocolos de seguridad se usan en el

GAD de Pimocha, usando como herramienta la entrevista, el cuestionario como instrumento y la observación como técnica, para obtener información más puntual acerca de la red del lugar a analizar. La metodología seleccionada se define en tres etapas: Valoración, ejecución e informe, donde se definen cada una de estas acciones en el orden respectivo que se llevaron a cabo, con el objetivo de mejorar el ambiente de seguridad del GAD de Pimocha y además lograr un resultado eficiente que muestre las vulnerabilidades existentes estableciendo su prioridad para eliminarlas o mitigar sus impactos ante incidentes de seguridad.

En la etapa de valoración se procedió en conocer las actividades de la organización, los recursos humanos y la arquitectura tecnología que tiene la organización para realizar el proceso de comunicación y procesamiento de la información. Para ello se realizó una visita al GAD de la parroquia Pimocha, mediante una entrevista y la observación se pudo reconocer todos estos aspectos.

En la etapa de ejecución, se inició un proceso de escaneo de la red usando la herramienta Nessus y Nmap conjunto al sistema operativo Kali Linux, donde el informe final de cada una de estas herramientas describieron vulnerabilidades existentes en la red, de las cuales las cuales ayudarán corregir errores de configuración y evitar potenciales riesgos afecten a la seguridad de la red del GAD de la parroquia Pimocha. El escaneo se realizó dentro de la institución, con la autorización correspondiente del administrador de la red del GAD de Pimocha, para hacer uso de un punto de red. En la etapa del informe el reporte muestra el resultado de las amenazas y vulnerabilidades presentes después de realizar el escaneo de red con el objetivo de tomar los controles informáticos pertinentes y decidir las medidas que se deben tomar para corregir estas vulnerabilidades con el propósito de garantizar la seguridad de la red.

Durante la visita al GAD de Pimocha, se realizó una entrevista al administrador del Departamento de Sistemas con el objetivo de identificar los procesos que se manejan en la institución, así como identificar los componentes que conforman la red. El administrador supo manifestar que es CNT (Corporación Nacional de Telecomunicaciones) quienes les brindan el servicio de internet, el cual es repartido a cada una de las instancias administrativas de la institución.

Por otro lado, también supo manifestar que tanto los procesos administrativos, operacionales y financieros se realizan a través del uso de la red, por eso es que en esta institución somos muy estrictos con el uso de la red, cualquier persona no tiene acceso a la misma, debido a los procesos que se manejan en la misma. También se gestionan políticas de seguridad para los usuarios de la red, para poder mantener el buen funcionamiento de la misma y así garantizar la seguridad por parte de los usuarios.

También manifestó que cuando se suscita un problema en la red, deben pedir soporte técnico a la ciudad de Quito, porque no cuentan con una persona especializada en seguridad y soporte de redes. Esto conlleve a un gran problema, porque el tiempo de respuesta es muy lento porque al no contar con una persona especializada en la institución el problema puede persistir horas e incluso días. Mediante la observación se pudo constatar que la red está conformada de la siguiente manera: dicha red se encuentra estructurada e instalada con sus respectivas canaletas, puntos de conexión y cable categoría seis. Los componentes tecnológicos que conforman la red tenemos:

- 3 Switch
- 1 conversor de fibra óptica
- 1 rad vertical
- 1 router inalámbrico

- 7 computadoras

Características de los equipos del GAD de la Parroquia Pimocha

Nombre	**Marca**	**Modelo**	**Características**
Switch	Cisco	Sg110-16 16 Puertos 10/100/1000 Mbps Rack	Puertos 10/100 que operan bajo los patrones de 10 BASE-T (con una velocidad de 10 Mbps) y 100BASE-TX (velocidad: 100 Mbps). Puertos 10/100/1000, que añaden el estándar 1000BASE-T (velocidad 1000 Mbps). puertos de fibra óptica usan conectores hembra para fibra óptica. Con puertos 100BASE-FX y 1000BASE-X.
Convertidor de fibra óptica	Tp-Link	MC112CS	Conversor de medios diseñado para convertir el cable de fibra 100BASE-FX a cable de cobre 100Base-TX.
Router	Tp-Link	TL-WA901ND	3 Antenas Una velocidad de transmisión inalámbrica de 450 Mbps

PCs	HP	Hp 260-P100B Pentium 19.5" Negro	Procesador: INTEL Pentium J3710 Sistema Operativo: Windows 10 Home Memoria: 4GB Disco Duro: 500GB Pantalla: 19.5"

El GAD de Pimocha utiliza una topología de red en estrella. La topología en estrella es una topología para una red de área local en la que todos los nodos están conectados individualmente a un punto de conexión central, como un concentrador o un conmutador. Una estrella toma más de cable para un bus, pero el beneficio es que, si falla un cable, solo se derribará un nodo, siendo esto una gran ventaja tecnológica para la institución. (DORDOIGNE, 2015)

La topología en estrella es una de las configuraciones de red más comunes. En esta configuración, cada nodo se conecta a un dispositivo de red central, como un concentrador, conmutador o computadora. El dispositivo de red central actúa como un servidor y los dispositivos periféricos actúan como clientes. La imagen # 1 muestra cómo esta configuración de red recibe su nombre, ya que tiene la forma de una estrella.

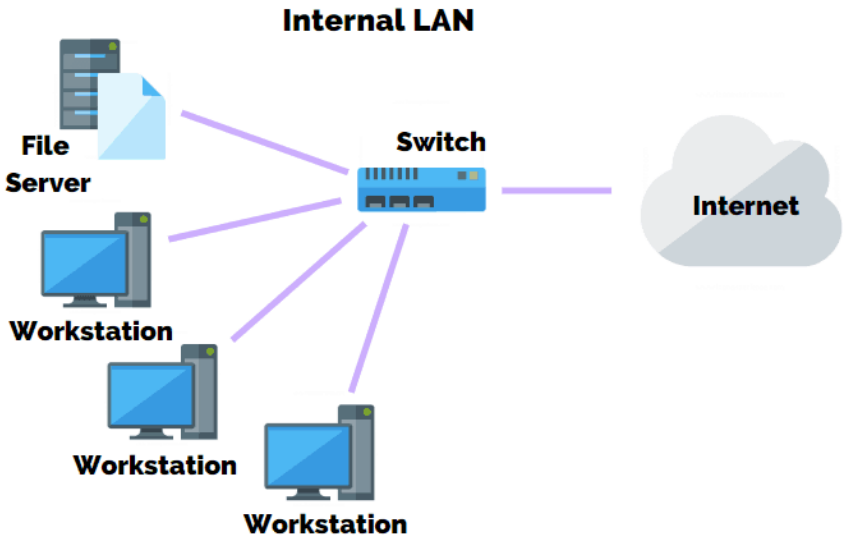


Imagen 1. Topología en estrella – Autor (Computer Hope, 2020)

En lo que respecta a los departamentos la red está correctamente instalada, pero el problema radica en el origen de la red, los switchs se encuentra situados cerca de la entrada de la institución (Ver Foto # 1), a la vista de todos y además con cables dispersos por doquier. Esto puede atribuir un problema en cuanto a la seguridad de la red y generar problemas de transmisión de datos y se generen interferencias en el cumplimiento de los procesos que se realizan en la institución.

Foto 1. Estado de los equipos de red del GAD de Pimocha. Autor - (Moreno, 2020)

Luego de identificar los activos, se solicitó permiso para realizar un escaneo para encontrar vulnerabilidades lógicas en la red. Se utilizó en primera instancia el escáner de puertos Nmap y luego Nessus Scanner para detectar vulnerabilidades en la red, el cual también presenta sugerencias para solucionarlas, luego de realizar es testeo de red.

Nmap es una utilidad de código abierto para explorar redes o realizar una auditoría de seguridad. Está disponible sin cargo y fue desarrollado para escanear rápidamente redes grandes. Se desempeña bien en este entorno, así como con hosts únicos. Nmap utiliza paquetes de IP en bruto de formas novedosas para determinar una serie de cosas, incluidos qué hosts están disponibles en la red, qué servicios ofrece un host (incluido el nombre y la versión de la aplicación), qué software del sistema operativo y versión del sistema operativo se está ejecutando, qué tipo de filtros de paquetes / cortafuegos se están utilizando, y más. (Shaw, 2015)

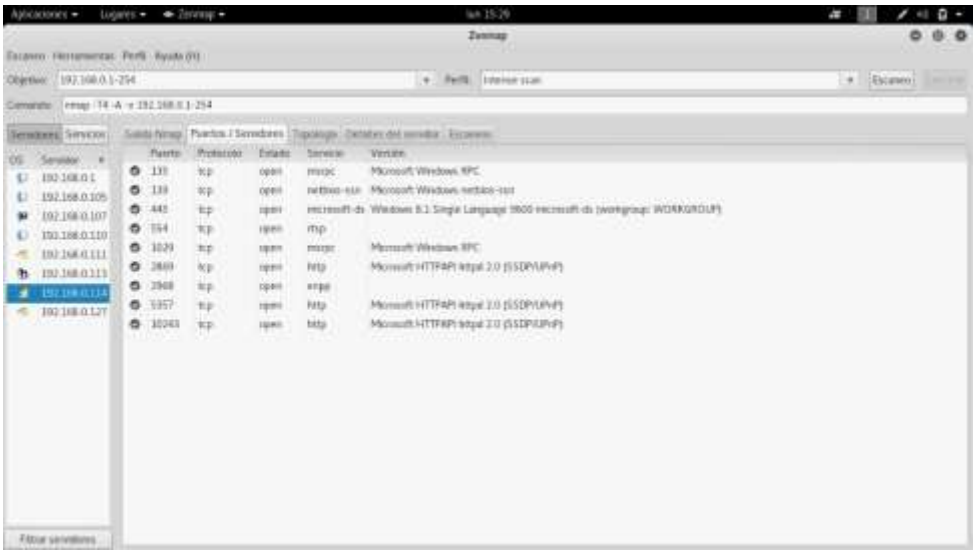


Imagen 2. Inicio del Análisis de red con NMap. Autor - (Moreno, 2020)

Durante el escaneo de red se procedió a colocar el rango completo de IPs para determinar cuántos equipos estaban disponibles durante el análisis. Este análisis tiene como objetivo conocer si existen puertos abiertos que puedan presentar fallas o

representar vulnerabilidades en la red. Se identificaron 7 terminales de red conectados y que mantienen tráfico de datos. En la Imagen # 2 se puede observar que existen puertos abiertos, los cuales representan de diferentes servicios de red activados. Se pudo constatar en compañía del administrador de la red los diferentes servicios que ellos principalmente usan, con lo cual se pudo concluir que hay puertos innecesarios que se encuentran abiertos, como por ejemplo el 5357 y el 10243, por los cuales se gestiona un servidor web, pero según el administrador de la red ellos no manejan este tipo de tecnología dentro de la institución.

Imagen 3. Resultados de escaneo con NMap. Autor - (Moreno, 2020)

En la imagen # 3, se muestra un informe detallado de la información de uno de los terminales testeados por la herramienta Nmap, en este caso es el terminal con más puertos abiertos que tiene la institución, pero la mayoría de esos puertos no son utilizados. Esto puede mantener riesgos, puesto que al mantener puertos abiertos y estos no estén asignado a una aplicación específica, estos pueden usarse para otros fines que puedan atentar con la seguridad de los datos que se transmiten en la red. Se recomienda

corregir estas vulnerabilidades de manera oportuna cerrando puertos sin utilizar, con el objetivo de prevenir riesgos de ataques informáticos a través de los mismos.

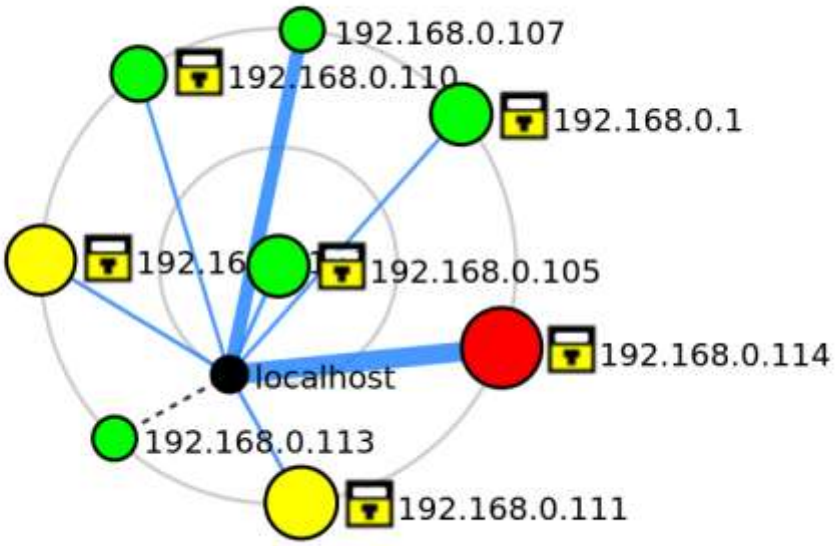


Imagen 4. Resultado de NMap topológico de los equipos del GAD. Autor - (Moreno, 2020)

La imagen # 4, muestra el estado general de los terminales de la red del GAD de Pimocha, se puede observar que sólo 4 equipos se encuentran dentro de los parámetros de seguridad sugeridos por NMap, dos se encuentran en estado de alerta y uno en estado crítico. Este diagrama permite al administrador de la red ver el estado de la red y tomar las medidas pertinentes para mantener la seguridad de la red y de los datos que se transmiten en ella.

Luego del escaneo con NMap, se procedió a realizar un escaneo con Nessus, el cual es uno de los muchos escáneres de vulnerabilidades utilizados durante las evaluaciones de vulnerabilidad y las pruebas de penetración, incluidos los ataques maliciosos. Este artículo se centrará en este escáner de vulnerabilidades, discutiendo los fundamentos que uno debe tener antes de comenzar con la herramienta, las diferentes capacidades de

escaneo que proporciona, lo que se necesita para ejecutar la herramienta y cómo aparecen los resultados una vez que se completan los escaneos del tráfico de la red. (Jetty, 2018)

El tráfico de red o tráfico de datos es la cantidad de datos que se mueven a través de una red en un punto de tiempo dado. Los datos de red en redes informáticas se encapsulan principalmente en paquetes de red, que proporcionan la carga en la red. El tráfico de red es el componente principal para la medición y gestión del ancho de banda. Además, varias topologías de la red solo se pueden implementar en función de la cantidad de tráfico de red en el sistema. (Ariganello, 2016)

El escaneo con Nessus permitió demostrar si hay existencia de amenazas y vulnerabilidades en la transmisión de datos de la red, y desde luego gestionar los posibles riesgos que puedan atentar con la seguridad de los datos que utilizan a través de la red de la institución. El escaneo tuvo una duración de aproximadamente 30 minutos, donde la herramienta seleccionada entregó un informe detallados de las amenazas y vulnerabilidades existentes en la red.

En el Anexo # II, la Imagen # 4 muestra el reporte que Nessus brinda al finalizar escaneo. En este se puede observar que existen servicios de red con configuraciones obsoletas, que aunque no representan problemas críticos en la seguridad de la red, se recomienda corregir dichas configuraciones para prevenir cualquier error en el futuro. Un error con severidad alta está el servicio para compartir recursos de red entre las plataformas Windows y Linux, este usa el protocolo SMB. En este caso no están configurados los privilegios para compartir dichos recursos. Se recomienda que existan roles para distintos tipos de usuarios y que estos no puedan acceder a la misma

información que otros usuarios deberían tener. Esto certifica la integridad de la información y que esta no sea modificada por usuarios no autorizados.

Otra vulnerabilidad encontrada de severidad media es que el protocolo SMB no requiere una firma de seguridad, lo cual puede provocar que personas no autorizadas puedan acceder a los recursos de la red. Al proporcionar una firma e seguridad a cada equipo permite que sólo estos puedan acceder a la información puesto que las firmas permiten identificar qué equipo hace una petición y si este tiene autorización para obtener los datos que solicita.

El informe también arrojó mensajes informativos, los cuales no representan amenazas para la red, pero se deben tomar en cuenta estas recomendaciones para garantizar la correcta gestión de la red del GAD de Pimocha. En la Imagen # 5, se muestra las soluciones que proporciona Nessus para corregir las vulnerabilidades de red encontradas en el escaneo.

Una amenaza, en el contexto de la seguridad informática, se refiere a todo lo que tiene el potencial de causar daños graves a un sistema informático. Una amenaza es un suceso o falla de seguridad que puede ocurrir o no, pero tiene el potencial de causar daños graves en los componentes de la red. Las amenazas pueden provocar ataques a sistemas informáticos, redes y más. Una evaluación de riesgos de seguridad, identifica posibles fuentes de amenazas y puntos de entrada y aísla esos puntos. (Cordero, 2018)

Una vulnerabilidad de red es una debilidad o falla en el software, hardware o procesos organizacionales, que cuando se ve amenazada por una amenaza, puede resultar en una violación de seguridad. Las vulnerabilidades de red no físicas generalmente involucran software o datos. Por ejemplo, un sistema operativo (SO) puede ser vulnerable a ataques de red si no se actualiza con los últimos parches de

seguridad. Si no se repara, un virus podría infectar el sistema operativo, el host en el que se encuentra y potencialmente toda la red. (Romero, 2018)

Las vulnerabilidades de la red vienen en muchas formas, pero los tipos más comunes son:

Los Malware, abreviatura de software malicioso, como troyanos, virus y gusanos que se instalan en la máquina de un usuario o en un servidor host.

Los Ataques de ingeniería social, que engañan a los usuarios para que den información personal como un nombre de usuario o contraseña.

Software desactualizado o sin parches que expone los sistemas que ejecutan la aplicación y potencialmente toda la red.

Es importante que el equipo de seguridad de red aborde estos factores al evaluar la postura de seguridad general de sus sistemas. Si no se controla, estas vulnerabilidades pueden conducir a ataques más avanzados, como un ataque DDoS (denegación distribuida de servicios), que puede hacer que una red se detenga o evitar que los usuarios accedan por completo.

Las vulnerabilidades de la red siempre están en peligro de verse comprometidas a medida que los actores maliciosos buscan explotar y obtener acceso al sistema de su empresa. Los ataques de malware y de ingeniería social son la mayor amenaza para una organización y sus usuarios. El software obsoleto a menudo contiene vulnerabilidades que no están presentes en la versión actual y representan un riesgo de seguridad. Finalmente, los cortafuegos mal configurados y las configuraciones de políticas predeterminadas en los sistemas operativos están en grave riesgo de exposición a un actor de amenazas. (Chicano, 2019)

Los resultados del escaneo con Nessus expusieron todas las vulnerabilidades presentes en la red del GAD de Pimocha. En la clasificación de las vulnerabilidades se pudo constatar que no existen vulnerabilidades de severidad crítica, lo que comprueba de que la red no tiene riesgos altos de ser vulnerada, sin embargo, sí existen estas con prioridad alta, media y baja. Estas se presentan debido a la mala configuración de los equipos de red y al mal manejo de protocolos de red específicos.

El reporte demuestra cada una de las vulnerabilidades encontradas y con sus respectivas soluciones, es por eso que se recomienda realizar los cambios sugeridos por la herramienta Nessus, para que en el futuro pueden suceder, en caso de no tomar las medidas pertinentes y que puedan afectar a la seguridad de los procesos, de los equipos y sobre todo a la seguridad de lo información que se maneja en la institución.

Los problemas encontrados en la red del GAD de Pimocha son de tipo físicos y lógicos, aunque no representan posibles riesgos críticos en la seguridad de la información, estos deben ser corregidos de manera inmediata, porque cualquier error, aunque pequeño que sea puede conllevar a pérdidas irreparables en cuanto a seguridad informática se refiere. La seguridad física de la red debe contemplar una buena estructura de la red desde sus inicios hasta cada uno de los terminales que la componen, así como la correcta gestión de cada uno de los usuarios, que estos estén autorizados a manejarla y que estén capacitados con las medidas de seguridad informática con el objetivo de no divulgar información.

En la seguridad lógica entran la correcta configuración de protocolos de red, sistemas operativos, controles de accesos, antivirus y firewalls para garantizar el correcto funcionamiento de la red. Ambos tipos de seguridad se complementan y su función

principal es garantizar la confiabilidad, integridad y disponibilidad de la información, siendo estos tres puntos el objetivo principal de la seguridad informática.

La confidencialidad: garantiza que solo una persona autorizada acceda a la información confidencial y se mantenga alejada de quienes no están autorizados a poseerla. Se implementa utilizando mecanismos de seguridad como nombres de usuario, contraseñas, listas de control de acceso y encriptación. También es común que la información se clasifique de acuerdo con el alcance del daño que podría hacerse si cae en manos no deseadas. Las medidas de seguridad se pueden implementar en consecuencia. (Baca, 2016)

La integridad garantiza que la información esté en un formato que sea verdadero y correcto para sus propósitos originales. El receptor de la información debe tener la información que el creador pretendía que tuviera. La información puede ser editada solo por personas autorizadas y permanece en su estado original cuando está en reposo. La integridad se implementa utilizando mecanismos de seguridad como el cifrado de datos y el hash. Tenga en cuenta que los cambios en los datos también pueden ocurrir como resultado de eventos no causados por el hombre, como un pulso electromagnético o un bloqueo del servidor, por lo que es importante contar con el procedimiento de respaldo y los sistemas redundantes para garantizar la integridad de los datos. (Chicano, 2019)

La disponibilidad garantiza que la información y los recursos estén disponibles para quienes los necesitan. Se implementa utilizando métodos como el mantenimiento de hardware, parches de software y optimización de red. Los procesos como redundancia, conmutación por error, RAID y clústeres de alta disponibilidad se utilizan para mitigar graves consecuencias cuando se producen problemas de hardware. Los dispositivos de hardware dedicados se pueden usar para proteger contra el tiempo de inactividad y los

datos inaccesibles debido a acciones maliciosas como los ataques de denegación de servicio distribuidos. (RAULT, 2015)

Si bien es cierto en la red del GAD de Pimocha se implementan políticas de seguridad informática, estas no sin suficientes para mantener la red al 100% segura. Es por eso que la institución debe adoptar el uso de la norma ISO/ICE 27002 que es una guía de buenas prácticas de seguridad de la información recomendables. Aunque su uso no es certificable, se pueden logran grandes resultados para garantizar el uso adecuado de los recursos y usuarios de la red del GAD de Pimocha.

Al igual que el gobierno y la gestión de riesgos, la gestión de la seguridad de la información es un tema amplio con ramificaciones en todas las organizaciones. La seguridad de la información, y por lo tanto ISO/IEC 27002, es relevante para todo tipo de organización, incluidas las empresas comerciales de todos los tamaños (desde bandas de un solo hombre hasta gigantes multinacionales), organizaciones sin fines de lucro, organizaciones benéficas, departamentos gubernamentales: de hecho, cualquier organización que maneja y depende de la información. (Calder, 2017)

La ISO/IEC 27002 recomienda controles que aborden los objetivos de seguridad involucrados en la gestión de la confidencialidad, integridad y disponibilidad de información. Las organizaciones pueden usar este estándar como guía para evaluar sus propios riesgos de información, identificar objetivos y aplicar controles. Los requisitos específicos de riesgo y control de la información pueden diferir en detalles, pero hay muchos puntos en común, por ejemplo, la mayoría de las organizaciones necesitan abordar los riesgos de información relacionados con sus empleados más contratistas, consultores y proveedores externos de servicios de información.

La diferencia entre la ISO/ICE 27001 y la ISO/ICE 27002 es que la primera es el estándar internacional que describe los requisitos para un SGSI (sistema de gestión de seguridad de la información). Es el único estándar en la familia ISO/IEC 27000 que proporciona una certificación auditada de forma independiente. (Sabah, 2019)

Lograr la certificación acreditada de ISO 27001 proporciona una evaluación experta e independiente de que la seguridad de la información se gestiona de acuerdo con las mejores prácticas internacionales y los objetivos comerciales. Aunque una organización no puede certificar ISO 27002, el estándar sirve como documento de orientación, ayudando a la implementación de ISO 27001 al proporcionar una guía de mejores prácticas para aplicar los controles enumerados en el Anexo A de ISO 27001.

La ejecución de buenas prácticas para la correcta administración de los recursos informáticos en una institución donde se manejan grandes volúmenes de información, conlleva a garantizar que la información viaje segura desde su origen hacia su destino. Aunque el GAD de Pimocha no se encuentre certificada con la Norma ISO/ICE 27001, esta puede aplicar la Norma ISO/ICE 27002 siguiendo todas las recomendaciones que aparecen estas, tanto para fortalecer la seguridad de la red LAN, así como que esta institución se encuentre preparada en caso en un futuro próximo desee certificarse en seguridad de la información con la ISO/ICE 27001.

Se le recomienda al GAD parroquial de Pimocha que aplique esta Norma ISO/ICE 27002 porque esta norma cuenta con políticas de seguridad de la información donde esta empresa puede crear un documento con sus respectivas políticas que deben contener sus conceptos de seguridad para establecer las formas de control, el compromiso de las políticas.

La aplicación de esta Norma ISO/ICE 27002 nos permitirá constar con el acceso de usuario autorizado y asi prevenir el acceso no autorizado a los sistemas de información, con el fin de evitar daños a documentos y recursos de procesamiento de la información de la organización que estén al alcance de cualquiera.

Por otra parte en lo que es la seguridad física de la empresa empleando esta norma se deben mantener o emplear una área segura, con niveles y control de acceso apropiados para la estuctura de esta red del GAD.

CONCLUSIONES

Se pudo constatar que en el GAD Parroquial de Pimocha no cuenta con políticas para manejar la Red LAN de la institución, pero también se pudo observar que existes pequeñas fallas en su instalación y en su configuración, que, aunque sean de prioridad baja, se deben corregir de una manera oportuna para que en el futuro no existan problemas en la referentes a la seguridad de la información así como en la transmisión de la misma a los diferentes nodos y terminales de la red.

Mediante la observación de la red de la institución, se encontraron con anomalías estructurales en la instalación de la misma. Se notó que los switchs se encuentran cerca de la entrada a la vista de todos, y además los cables de red se encuentran dispersos y también a la vista de todos. Esto puede provocar que los equipos se averíen por el polvo y que haya intermitencias de transmisión por la posición de los cables. Se recomienda reinstalar estos equipos en un rack cerrado y estructurar los cables en canaletas.

Durante los escaneos con las herramientas seleccionadas se encontraron algunos puestos abiertos de algunos terminales de la red de los equipos y con vulnerabilidades de severidad alta, medias y bajas . Aunque estas vulnerabilidades encontradas no representan en el presente un problema critico en la institución, se recomienda aplicar las medidas pertinentes para mantener a la red seguro de futuros ataques o errores en la gestión de los procesos de la red.

La aplicación de la Norma ISO/ICE 27002, por parte del GAD de Pimocha, para estructurar una red segura, permitirá gestionar los recursos informáticos y a sus usuarios de una manera más óptima, ya que se deben seguir políticas de buenas prácticas, que avalen que la información que se maneja en la institución sea confiable, integra y esté

disponible cuando se la solicite, y a su vez la institución esté preparada para que un futuro se califique en seguridad informática.

BIBLIOGRAFÍA

Ariganello, E. (2016). *REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching. 4ª edición actualizada.* Grupo Editorial RA-MA.

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* Grupo Editorial Patria.

Baca, G. (2016). *Introducción a la seguridad informática.* México: Grupo Editorial Patria.

Caballero González, C. M. (2017). *UF0855 - Verificación y resolución de incidencias en una red de área local.* Madrid: Ediciones Paraninfo, S.A.,.

Calder, A. (2017). *Iso27001/Iso27002: Una Guia de Bolsillo.* IT Governance Publishing.

Chicano Tejada, E. (2015). *Gestión de incidentes de seguridad informática. IFCT0109.* IC Editorial.

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

Chicano, E. (2019). *Auditoría de seguridad informática. IFCT0109.* IC Editorial.

Computer Hope. (2020). *Computer Hope*. Obtenido de Star topology: https://www.computerhope.com/jargon/s/startopo.htm

Cordero, T. (2018). *Cibercrimen: Las Amenazas al Navegar en Internet y en las Redes Sociales.* TFJ.

DORDOIGNE, J. (2015). *Redes informáticas - Nociones fundamentales (5ª edición): (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6 ...).* Barcelona: Ediciones ENI.

Jetty, S. (2018). *Network Scanning Cookbook: Practical network security using Nmap and Nessus 7.* Packt Publishing Ltd.

Kremling, J., & Parker, A. M. (2017). *Cyberspace, Cybersecurity, and Cybercrime.* SAGE Publications.

Moreno, S. (2020). Análisis de Vulnerabilidades de la Red LAN del gobierno Autónomo Descentralizado de la Parroquia Pimocha. *Universidad Técnica de Babahoyo*.

RAULT, R. (2015). *Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa (3ª edición).* Ediciones ENI.

Romero, M. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* 3Ciencias.

Sabah, O. (2019). *Information Security Handbook For ISO 27001 Controls.* Helsinki: UR academy.

Shaw, D. (2015). *Nmap Essentials.* Packt Publishing Ltd.

ANEXO I. CUESTIONARIO PREGUNTAS PARA LA ENTREVISTA

¿Cuáles son los servidores implementados?

Actualmente no existen servidores. Todo en la institución se maneja de forma descentralizada, toda la información se encuentra en los diferentes terminales. Existe una carpeta global compartida en red donde se coloca la información necesaria en caso algún usuario la solicite.

¿Cuál es el proveedor de servicios de internet?

Actualmente nuestro proveedor es CNT. Ellos nos entregan internet con fibra óptica a través de un conversor nosotros noes encargamos de distribuir el internet a los diferentes departamentos de la institución.

¿Se está utilizando software adicional?

No, todo lo manejamos a través del paquete de Microsoft Office.

¿Se está alquilando equipo adicional para atender la solicitud?

No, solo trabajamos con el equipo tecnológico que pertenece a la institución.

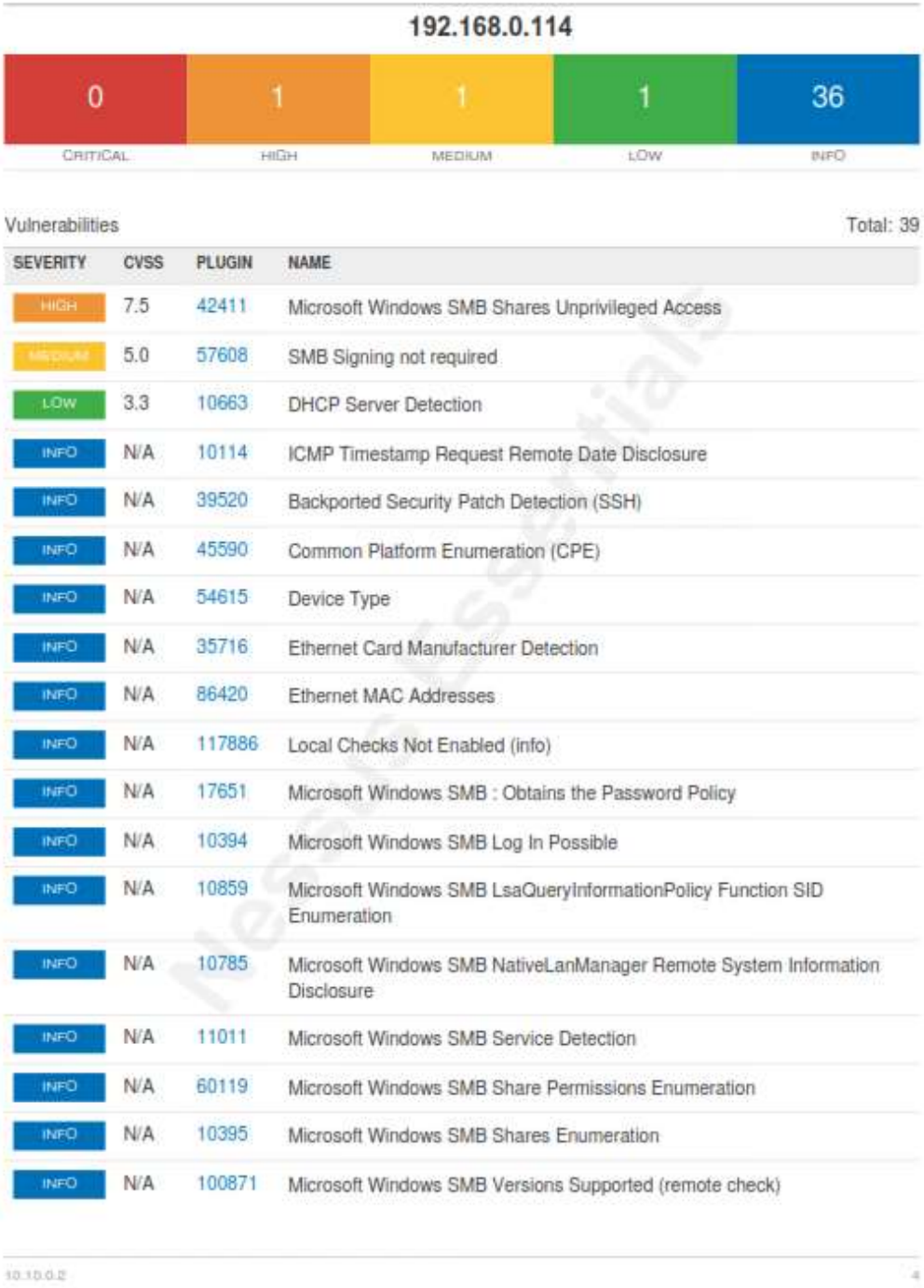
¿Se definieron usuarios de acuerdo a las políticas de la empresa?

Si existen usuarios que se encargan en la administración y gestión de los procesos de la institución, pero no existen técnicos que se encarguen en atender los problemas que se susciten en la institución, para eso pedimos soporte a la ciudad de Quito.

¿Qué protocolos de red tienen actualmente configurados?

Hemos aplicado protocolos de control de acceso a los usuarios. Existe una configuración de filtrado de MAC, para que solo los equipos autorizados puedan acceder a los recursos de la red. Si bien es cierto aun nos falta para mantener esta red segura, pero cada día se está trabajando para garantizar la calidad de los servicios.

ANEXO II



192.168.0.114

0	1	1	1	36
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 39

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	5.0	57608	SMB Signing not required
LOW	3.3	10663	DHCP Server Detection
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	60119	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)

10.10.0.2 4

Imagen 5. Resultado del Análisis con Nessus – Autor (Moreno, 2020)

0	1	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Thu Jan 16 11:55:34 2020
End time: Thu Jan 16 11:59:56 2020

Host Information

IP: 10.10.0.14
MAC Address: FC:AA:14:90:9A:31
OS: Linux Kernel 3.10, Linux Kernel 3.5, Linux Kernel 3.8, Linux Kernel 3.9

Vulnerabilities

26925 - VNC Server Unauthenticated Access

Synopsis

The remote VNC server does not require authentication.

Description

The VNC server installed on the remote host allows an attacker to connect to the remote host as no authentication is required to access this service.

** The VNC server sometimes sends the connected user to the XDM login
** screen. Unfortunately, Nessus cannot identify this situation.
** In such a case, it is not possible to go further without valid
** credentials and this alert may be ignored.

Solution

Disable the No Authentication security type.

Risk Factor

High

CVSS Base Score

10.10.0.14 4

Imagen 6.Reporte de sugerencias de solución de vulnerabilidades propuestas por Nessus. Autor (Moreno, 2020)

ANEXO III

Fotos realizando el escaneo de la red del GAD de Pimocha.

Foto 2. Escaneo de Vulnebilidades en el GAD de Pimocha - (Moreno, 2020)

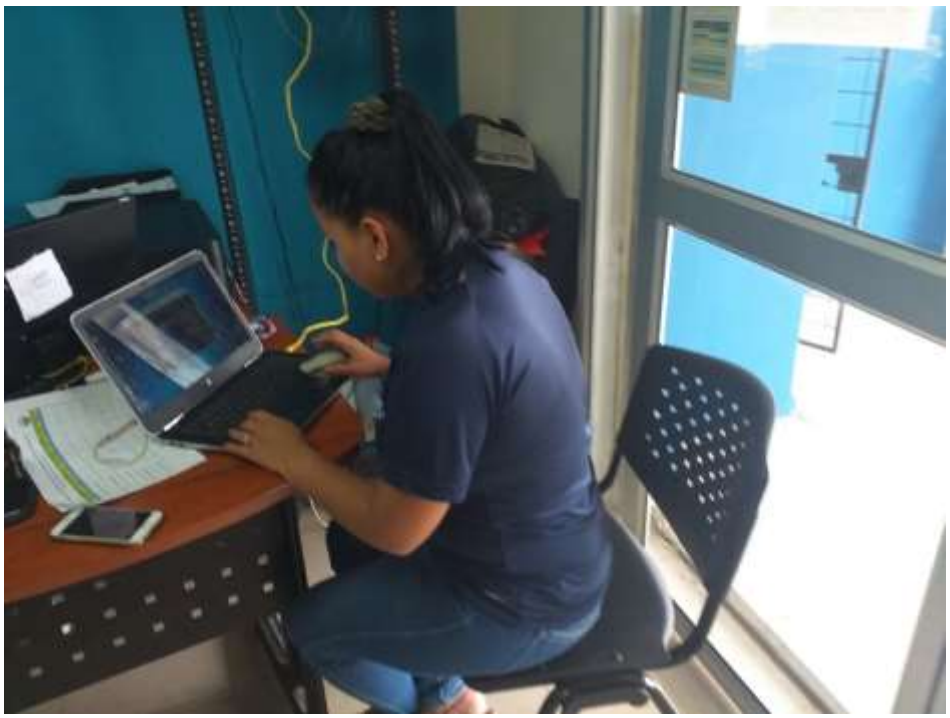


Foto 3. Escaneo de Vulnebilidades en el GAD de Pimocha - (Moreno, 2020)

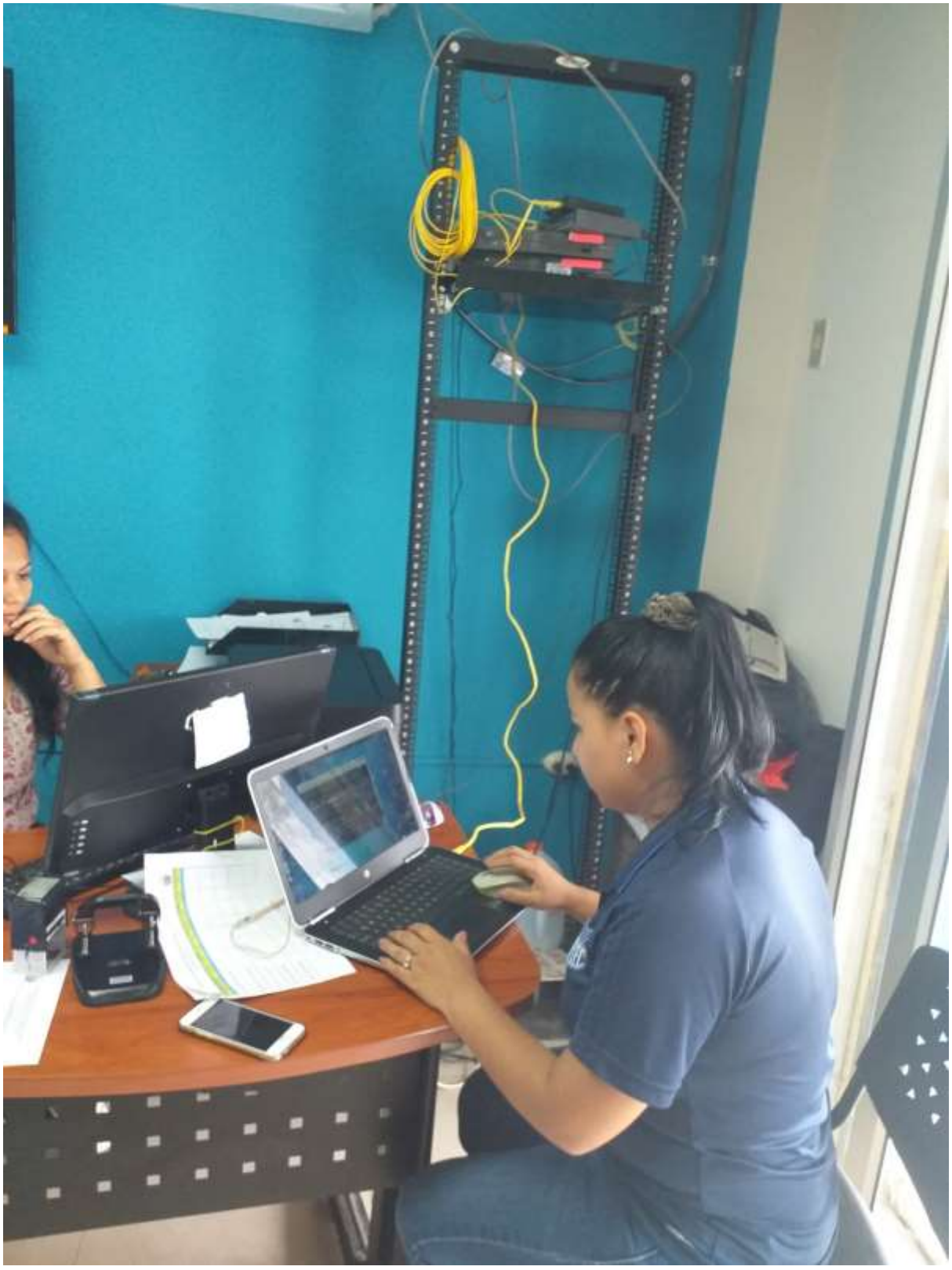


Foto 4. Escaneo de Vulnebilidades en el GAD de Pimocha - (Moreno, 2020)