UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

JUNIO –SEPTIEMBRE 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCION DEL TITULO DE INGENIERO(A) EN SISTEMAS

TEMA:

ANALISIS DEL SISTEMA MI NEGOCIO EN LA NOTARIA PRIMERA DEL CANTON BABAHOYO

EGRESADA(O):

HARLEN TEODORO CABRERA MACIAS

TUTOR:

ING. NELLY KARINA ESPARZA CRUZ

AÑO 2020

INTRODUCCION

La presente investigación está constituida que en la actualidad la tecnología contribuye a que los negocios y establecimiento surjan con mayor fluidez, implementando la misma, de forma que se ha convertido en una necesidad y no en un luego, porque día a día es descubierto o mejorado para contribuir con la facilidad de la vida.

La notaria realiza actividades como lo son: registrar las compras y a su vez las ventas de bienes muebles e inmuebles, certificaciones de documentación sean públicos o privados, legislaciones de terrenos, declaraciones juramentadas, etc. Una medida innovadora es la facturación electrónica que está sujeta a los cambios tecnológicos del mundo que casa día se desarrolla a través de la modernización, en esta institución pública donde día a día se realizan movimientos con facturación notarial la cual está basada en registrar, controlar y verificar información, la misma que pueda ser mostrada en los registros efectuados con el software Mi Negocio dentro del sistema.

El problema se encuentra en las posibles vulnerabilidades que se puede encontrar en del sistema, por la manera insegura de manejar los datos, a que cada usuario que accede al sistema puede observar los procesos que se encuentran realizando en ese momento el responsable de digitalizar la información requerida para suplir con la necesidad requerida.

Identificar falencias y vulnerabilidades por medio del uso de MBSA la cual es una herramienta creada por Microsoft, debe realizarse un estudio a con la cual se efectuará las evaluaciones necesarias y determinar lo que se encuentre en el software Mi Negocio y a su vez permitirá encontrar riesgos con exactitud, que llegasen a influir en la institución.

De forma cualitativa serán mostrados los datos ya que por la gran cantidad de datos con información se tiene como finalidad construir una teoría partiendo desde punto previamente establecido, que se ha realizado siguiendo una línea determinada, que consiste en extraer una muestra de forma teórica, mas no de forma representativa. Mediante el uso del análisis cualitativo se tendrá en cuenta falencias, debilidades y los que estas ´pueden causar.

La línea de investigación empleada en el presente estudio de caso es desarrollo de sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos; y la sublinea redes y tecnologías inteligentes de software y hardware.

DESARROLLO

En el estudio de caso presente se determinó las debilidades y falencias existentes dentro de la Notaria Primera que se encuentra en la ciudad de Babahoyo que cuenta con la implementación del sistema de facturación Mi Negocio.

Es preciso destacar que el presente estudio está rigurosamente asociado o centrado a la exploración de los protocolos establecidos en el sistema, por medio del estudio que concretamos identificamos lo relevante de los protocolos ejecutados por medio de un sistema informático. (Ugarte, 2014)

Figura: N. º 1 Explicación breve del encargo del uso del software

Elaborado por: Harlen Cabrera

En base a toda la información recopilada, sirvió de mucha ayuda el uso del instrumento para el análisis de las falencias y debilidades existentes en el sistema, obteniendo como resultado el conocer los peligros u obstáculos que se muestren en la notaria y determinar las decisiones a tomar sobre el software. Al instante de efectuar la exploración en el software se gestionó la aprobación de la delegada para especificar la magnitud del riesgo existente.

La utilidad primordial al emplear el escaneo es:

Reducción de las amenazas que pueden producir hurto de datos y resguardar la rectitud de los datos a través de la red. Al momento de emplear el escaneo del software hemos usado el instrumento creado por Microsoft como lo es el MBSA con la cual se realizara las evaluaciones requeridas. (Maroto, 2014)

MBSA: Facilita a localizar y reducir los problemas generales de seguridad, teniendo en cuenta la carencia de reajustes de seguridad, MBSA se centrará en buscar los reajustes o complementos de seguridad inexistentes, descubriendo las equivocaciones más frecuentes de configuración y reajustes de seguridad que sean necesarios en su sistema informático. Mediante esta modesta herramienta puede emplear una evaluación programada del sistema para localizar posibles errores de seguridad.

Este instrumento que brinda Microsoft para examinar la seguridad de los equipos de cómputo. La herramienta facilita examinar la seguridad del computador, o la de un grupo de máquinas conectadas en la red, brindando resultados acerca del estado de los puertos desbloqueados en la conexión TCP/IP, y toda una cadena de debilidades a las que se pueden ser vulneradas, inclusive las que perjudiquen al mismo explorador web. De igual forma, surte resultados y sugerencias que facilitara el solucionar los sucesos que se susciten.

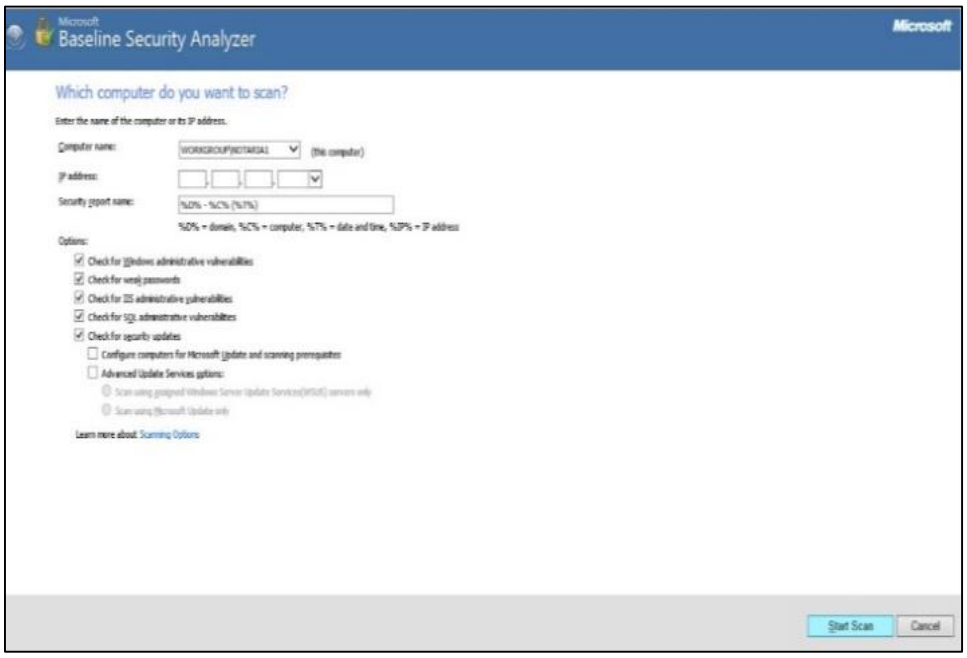

Figura: N. º 2 Inicio de la aplicación MBSA escogiendo el nombre del pc "WORKGROUP(NOTARIA1)"

Elaborado por: Harlen Cabrera

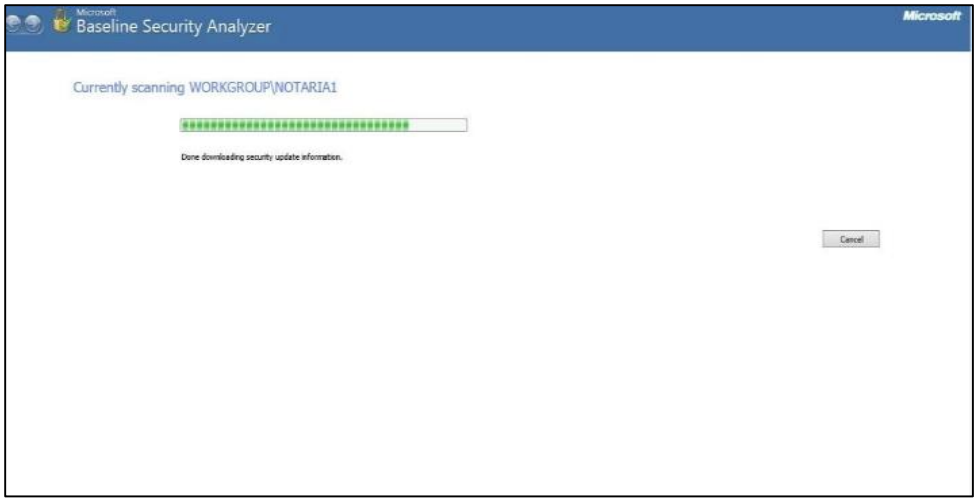

Figura: N. º 3 Ventana de escaneo

Elaborado por: Harlen Cabrera

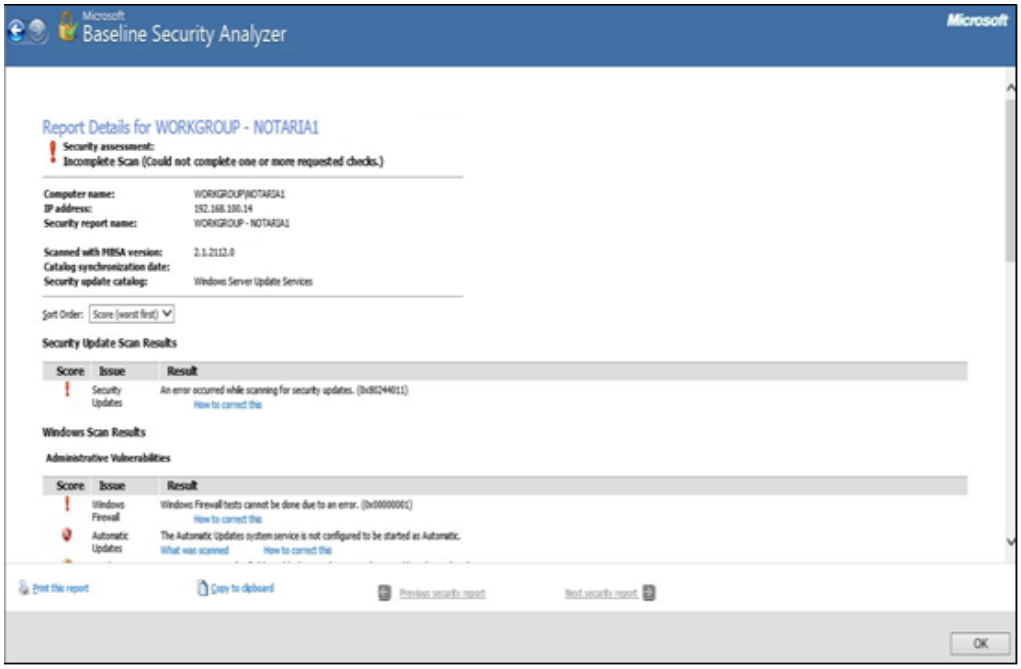

Figura: N. º 4 Muestra los datos del pc y está procediendo a realizar un escaneo dentro del sistema

Elaborado por: Harlen Cabrera

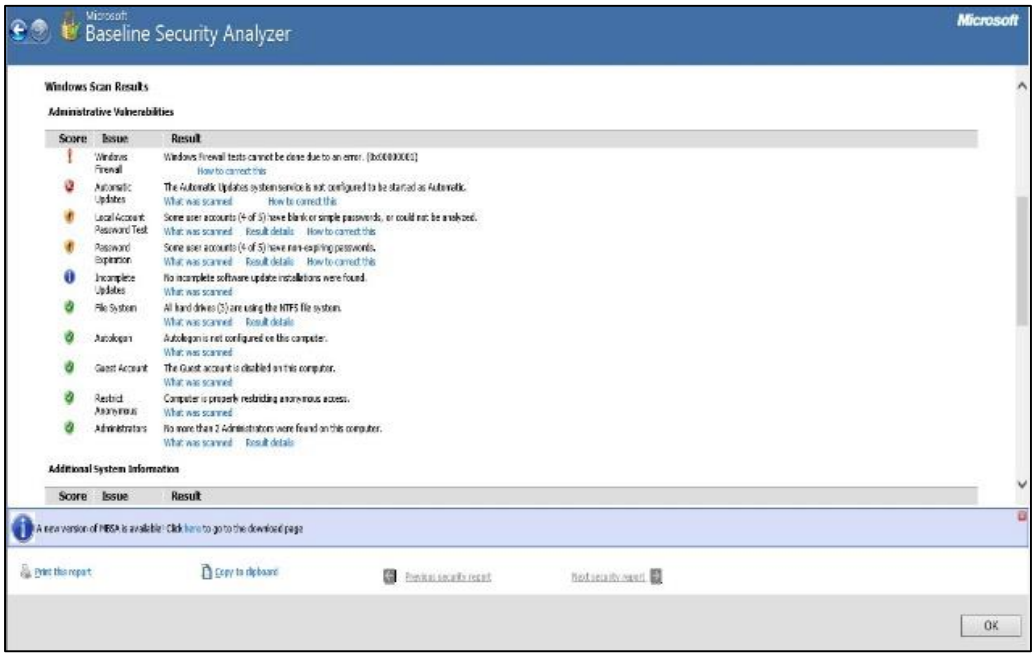

Figura: N. º 5 Informe de estado que se encuentra la maquina

Elaborado por: Harlen Cabrera

En base a los resultados obtenidos luego de realizar esta prueba con la herramienta MBSA demostró las falencias del sistema, y también se identificó la distribución de los servicios administrativos, sirviendo esta herramienta como contribuyente a la empresa a identificar el estado de seguridad que se encuentra en base a las sugerencias de seguridad de Microsoft.

En años anteriores, los datos de los procesos que se efectuaban en las notarías era registrada a mano , que a su vez generara errores en los registros de procesos y tramites. (Diaz.C, 2014)

El lenguaje de programación empleado para la creación del software es Java dado el caso que este código, una vez agrado, puede trasladarse si cambio alguno en cualquier computador, y emplearlo. Java es un lenguaje de programación de alto nivel orientado a objeto que permite la creación de softwares multiplataforma tanto en hardware y software. (Valbuena, 2015)

Mi Negocio brinda parámetros apropiados para facilitar el registro de todas las labores que emplea el encargado de manipular el sistema y asimismo este sistema minimiza la espera en cesión de los tramites requieren los usuarios.

El detalle del sistema y la descripción de lo que debe realizar cada una de sus partes es la consecuencia del examen realizado. En el transcurso, se podrá examinar y mostrar el sistema en el cual se está elaborando, además así mismo se lo realizo alguno de sus módulos.

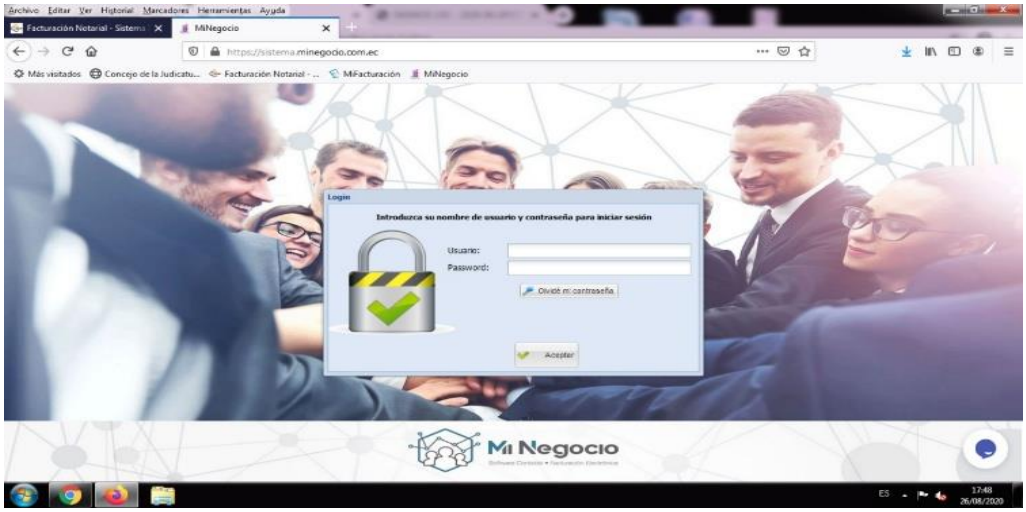

Figura: Nº6 Inicio del Sistema Mi Negocio

Elaborado por: Harlen Cabrera

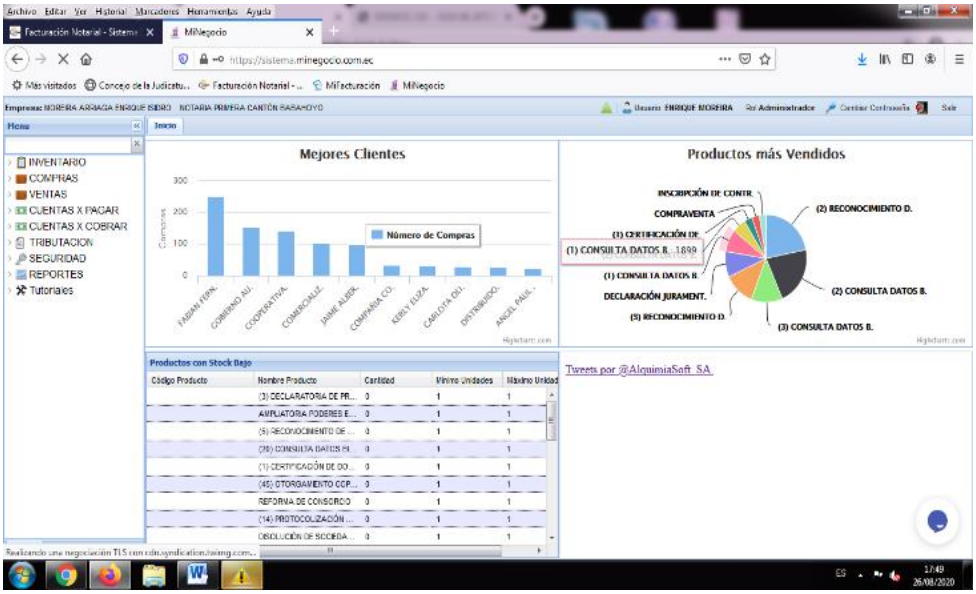

Figura N. º7 Ingreso al sistema
Elaborado por: Harlen Cabrera

Un sistema está compuesto de partes tangibles como lo es el hardware, y una parte lógica de un equipo como es el software y los individuos que lo manipulan, que interactúan entre sí para guardar y administrar datos con un propósito general. (Hammer, 2015)

Al finalizar la fase de evaluación en el sistema se constatará el correcto funcionamiento del mismo. La finalidad de las evaluaciones es el de generar excelentes resultados del software. (Tuya, 2015)

Al dejar expuesto todas la operatividad del sistema se debe de verificar su correcto funcionamiento. (Kendall, 2015)

El tiempo de mantenimiento puede durar años, para emplear correctamente la fase de mantenimiento, se necesita diseñar un cronograma con anterioridad que puedan solucionar todos los sucesos que se llegasen a presentar. (Sommerville, 2015)

Así, es como se muestra una factura electrónica arrojada mediante el sistema con su trámite respectivo.

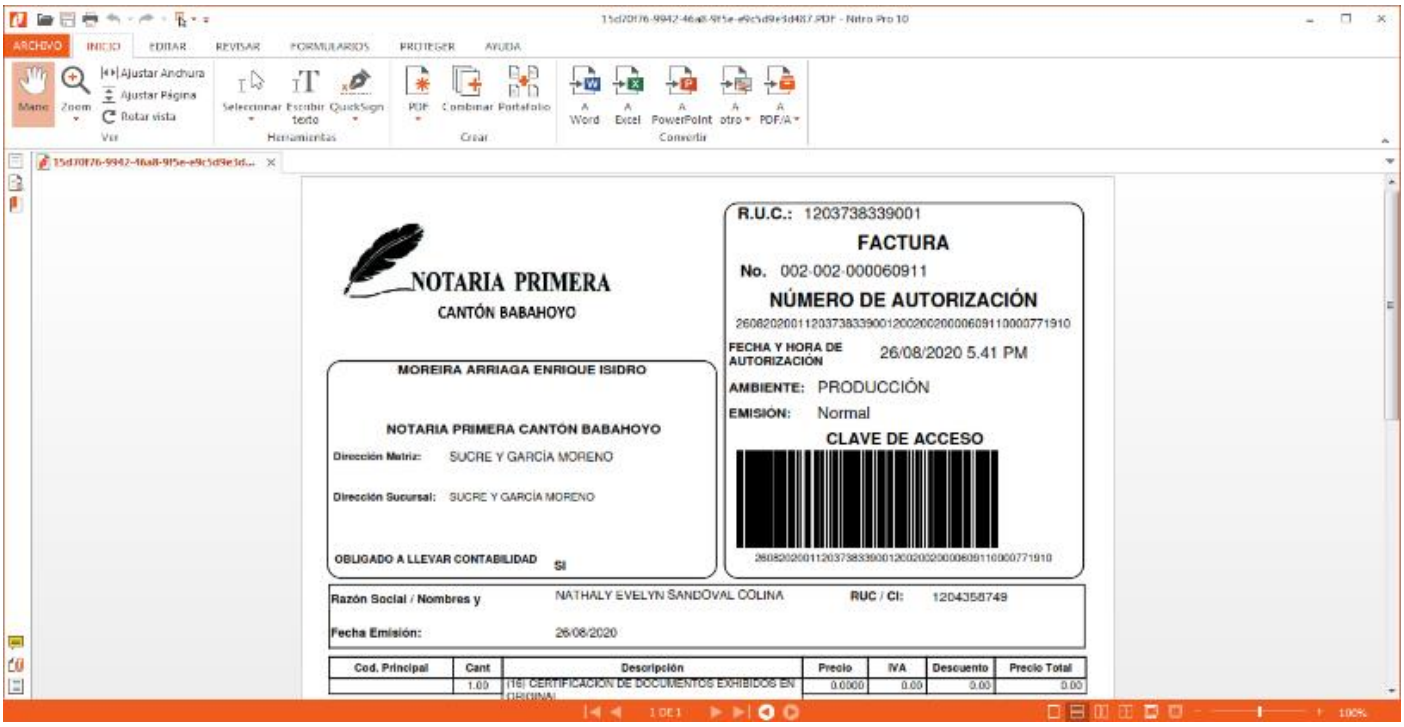

Figura: N. º 8 Factura emitida por el sistema
Elaborado por: Harlen Cabrera

Con la finalidad de evadir problemas futuros con el usuario, se debe detallar cómo los solicitantes pedirán las alteraciones en los procesos. (Vera, 2016)

Con respecto a la capacidad de emplear la destreza de reconocimiento se debe precisar el estudio, luego los datos que se van a obtener, favoreciendo suplir con la meta. (Gil, 2016)

En esta vida todo va implicado por una procedimiento más en los sistemas computacionales los cuales se han convertido en una prioridad, actualmente toda entidad con o sin fines de lucro debe manejar sus procesos de manera clara y concisa para que sus movimientos se efectúen de manera ágil y se conviertan en un beneficio. (Olebau, 2014)

La configuración de la red empleada en el lugar ,se encuentra organizado de manera jerárquica dado el caso que no es más que una red cuya configuración está basada en normativas de ahí surge la topología jerárquica se establece como la red de comunicación usada por los nodos que la constituyen. (Lechtaler, 2015)

Cisco Packet Tracer es el simulador usado, ya que brinda visualizar la postura de la red. En la cual existen varios dispositivos como switch, router, etc.

Así mismo es un instrumento de simulación de redes actualizadas y eficientes que se emplea en pruebas por lo que mediante de este instrumento reflejara la postura de la red en el establecimiento que se está efectuando el estudio de caso. (Piquero, 2015)

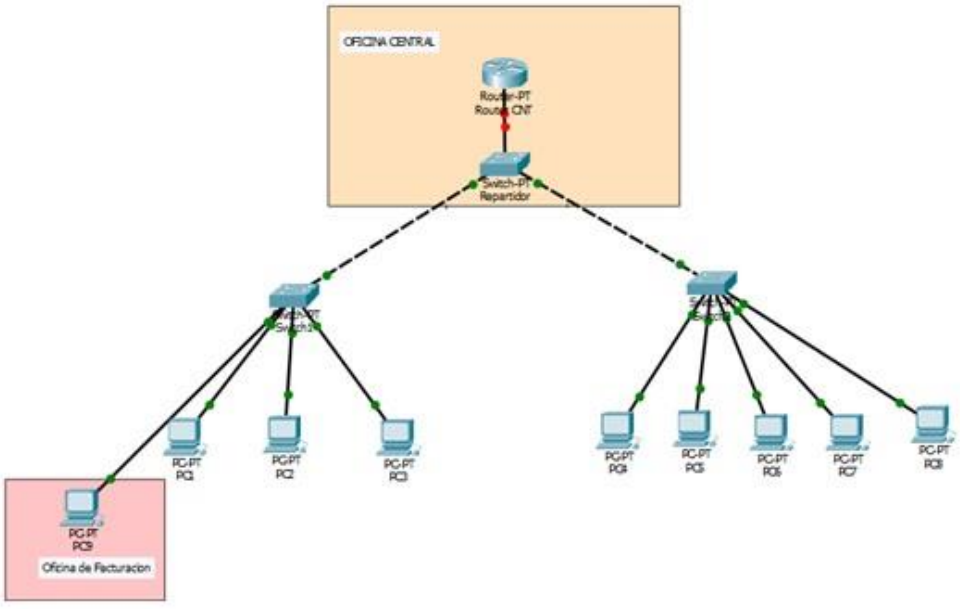

Figura: Nº 9 Estructura de la red del establecimiento

Elaborado por: Harlen Cabrera

Con el uso Packet Tracer el resultado fue reconocer el modelo de red de la notaria, la cual utilizada una red topológica de modo árbol, porque desde el router principal que tienen, se distribuye en ramificaciones las conexiones de internet permitiendo la incorporación de redes y subredes nuevas sean internas o externas.

En el estudio de caso presente la designada de la recopilación de datos es la metodología cualitativa la cual parte de la observación, y luego haciendo una entrevista que tiene como característica la flexibilidad, porque está centrada más en una conversación amena la cual se acopla a las actitudes del entrevistado.

La metodología de campo es otra que a su vez ha sido utilizada ya que, mediante la observación, se da a notar posibles errores en el sistema siguiendo los parámetros de observación basados en la guía. (Hammer, 2015)

Figura: Nº 10 Entrevista con el encargado de uso del software
Elaborado por: Harlen Cabrera

Ciertas utilidades de la entrevista son:

- Los temas tratados son de suma importancia, y no serán siempre buenos.
- El contenido tratado es de nivel muy alto, y mucho más cuando se la información que se revela se ha mantenido a través del tiempo en secreto (Garcia, 2014)

Seguridad informática/Seguridad de la información

La seguridad informática resguarda el sistema informático, con el fin de salvaguardar la integridad y los datos que contiene, por otro lado, seguridad de la información reúne todos los datos que estén a su alrededor de forma independiente.

Habitualmente, un sistema será confiable e íntegro si tiene de estos tres puntos concretos:

- **Confidencial**: Acceder a los datos debe ser por medio de permisos y controlada.
- **Integra**: Los datos solo pueden ser modificados con permiso.
- **Disponible**: Acceder a los datos solo mediante previo permiso.

Sistema informático y sus vulnerabilidades

El objetivo principal de un sistema informático es la protección de sus activos, es decir, los elementos que componen el sistema y se puedan asociar en:

- **Hardware**: Elementos tangibles que componen el sistema.
- **Software**: Elementos intangibles ejecutables.
- **Datos**: Captan los datos de forma lógica procesada por el software utilizando elementos del hardware.

Podría decirse que, los datos se encuentran localizados en el hardware y pueden ser manipulados a través de las herramientas del software.

Los datos son los activos más importantes, dado el caso de que los elementos tangibles cumplen con su tiempo de vida y se pueden renovar, pero la empresa depende de los datos. (Zapata, 2015)

Debilidades y Amenazas

La información en una red es un inconveniente de la protección de los datos, y fundamentalmente debe estar encaminada a resguardar los datos de los posibles ataques que se puedan presentar en cualquier momento, ya sea interna o externa. Las debilidades son la primera vulnerabilidad en los procesos relacionados en interacción con la información, y esta a su vez es innata de los sistemas que se la considera una característica.

En la actualidad existen individuos que mediante el uso de medidas tecnológicas innovadoras logran burlas los sistemas de seguridad en la red, con el fin de sustraer información o alojar virus con comportamientos dudosos, que en el mundo informáticos son los denominados hackers.

Su identificación por color de sombrero define su propósito:

Sombrero Blanco: La seguridad informática es su característica principal.

Sombrero Negro: Tienen como característica burlar la seguridad de los sistemas de información con fines malicioso.

Sombrero Gris: Son grupos que tienen como motivación protestar sobre las inconformidades, no generan ataques de forma malintencionada.

Ataques en la Red

Los atacantes principales en una red son:

Malware: Software malicioso infiltrado con finalidad de dañar el sistema.

Virus: Infecta los datos, pero solo si es ejecutado por el usuario.

Gusanos: Software clonador de sí mismo para difundirse por la red y posteriormente infectarla.

Troyanos: Trata de buscar una ruta para posterior, acceso de más programas con fines maliciosos.

Prevención de Ataques a una Red

Con el fin de sostener la información conectada a la red a un cierto grado de protección, lo primordial es tener en cuenta de que forma pueden suscitarse estos hechos y con qué finalidad se presente este riesgo.

Formas efectivas de evitar ataques:

***Ransomware*:** Es un malware que tiene como propósito salvaguardar la información y requiere un sistema operativo actualizado, de igual manera contar con un antivirus; para impedir el acceso remoto desde sitios no establecidos dentro del establecimiento el firewall, y de ser así, mediante protocolos seguros serán permitidos.

Escáner de puertos: Este procedimiento permite identificar servicios y puertos que el sistema no utilice y cerrarlas.

***Phishing*:** Declinar todo tipo de petición de información y a su vez negación de descargar archivos de individuos no identificados (Bolaños, 2015)

SISTEMA DE IDENTIFICACIÓN DE INTRUSOS(IDS)

Corresponde a un dispositivo que, oye la circulación en la red para encontrar acciones inciertas, y de esta forma minimizar las probabilidades de entrometimiento. Controla los sucesos que se presentan en el sistema informático en localización de intentos de entrometerse.

Hablamos como sucesos a toda actividad que trate de exponer la confidencialidad, integridad, disponibilidad o evadir los protocolos seguridad de una red o un computador. Los entrometimientos se pueden presentar de varias modalidades: intrusos que ingresan al sistema a través de la internet, usuarios autorizados tratan de obtener beneficios extras a los cuales no

cuentan con autorización y usuarios autorizados que ejecutan de forma equivocada los beneficios que se les ha otorgado.

Al implementar el ID ampara de los riesgos que se presentan al aumentar los vínculos en una red y la relación que existe hacia los sistemas de información. El sistema de detección de intrusión basado en implementar los IDS con una buena política es esencial en base a la seguridad, esta herramienta al estar actualizada puede defender antes los constantes ataques ya sea desde la red, o por un computador. (Alfaro, 2016)

Características de IDS

- Capacidad de mantenerse durante una caída del sistema.
- Identificar irregularidades no comunes sobre el estándar.
- Adaptación fácil al sistema previamente instalado
- Mostrar complejidad al tratar "burlar".

Políticas de seguridad de la información norma ISO 27001 - 27002

ISO 27001: Concede la garantizarían, la confidencialidad e integridad de la información y a su vez de los datos, de igual forma como lo es con los sistemas encargados de procesarla. La norma ISO 27001 para los sistemas gestión de la seguridad de la información brinda a las entidades la valoración del riesgo y la aplicación de los controles necesarios para eliminarlos, de esto modo ayuda a las empresas con el manejo de los acontecimientos de seguridad, e incumplimientos de una forma eficaz.

Entra ciertos beneficios de la norma ISO 27001 se encuentran:

- Hallar problemas y tomar medidas necesarias contra estos.
- Total privacidad para asegurar que la información pueda ser tomada solo por permitidos.
- Flexibilidad para adecuar el control a una o varias áreas de la empresa.
- Lograr las metas demostrando satisfacción.

Estructura de la Norma ISO 27001

Objeto y campo de aplicación: La norma empieza colaborando con unas guías sobre el uso, finalidad y el modo de aplicación del estándar.

Referencias Normativas: Sugiere analizar algunos documentos importantes para la posterior implementación de ISO27001.

Términos y Definiciones: Detalla la terminología para la cual aplicar este estándar.

Contexto de la Organización: Requisito primordial de la norma, el cual recolecta instrucciones con respecto al conocimiento de la organización y su contexto.

Liderazgo: Construye una normativa de seguridad que este al tanto toda la organización y delegue roles, responsabilidades y autoridades dentro de la misma.

Planificación: Imprescindible sobre la toma de decisiones sobre las amenazas y oportunidades al momento de estructurar un sistema de gestión de seguridad de la información.

Soporte: Indica que para que funcione de forma correcta el SGSI la entidad debe tener los recursos relacionados para la situación.

Operación: Se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.

Evaluación del Desempeño: Se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, y el análisis.

Mejora: Se presentan las obligaciones que tendrá una organización cuando encuentre una inconformidad.

Norma ISO 27002: Suministra varias sugerencias para la administración de la seguridad de los datos a todos los involucrados para comenzar, ejecutar o conservar sistemas de gestión.

Para tener más conocimiento sobre los demás dominios es imprescindible informarse sobre la norma ISO 27002 añadidura para la ISO 27001.

El valor de contar de una información integra es primer paso para ejecutar todas las funciones en las distintas áreas. No obstante, es muy valioso conservar aquella información con respaldo para que no se extravié, o se desgaste de alguna manera. En sí, los datos y la información con la que cuenta la organización y que recolecta con las labores diarias es uno de sus activos con más valor ya que pueden trazar la ruta de la organización con cara al futuro. (Calder, 2017)

Seguridad en Redes

Al no contar con una seguridad buena en la red se está expuesto que un hacker pueda ingresar de manera fácil al sistema. Cabe recalcar que no debe existir conformidad con un antivirus ya que no son capaces de identificar en su totalidad infecciones dentro del sistema además su fragilidad hace que la seguridad se vea con falencias. (Stallings, 2014)

Normas de Seguridad en Redes

- Eludir acciones que puedan influir con las redes y su seguridad.
- Instalar archivos de actualización faltantes del sistema.
- Emplear protocolos de seguridad con cifrado de datos.
- Disponer de programas solo necesarios.
- Implementar seguridad en los servidores (FTP, Web, etc.).

Al aplicar el instrumento citado con anterioridad en la evaluación del software

Debido a la evaluación que se ejecutó en el software será posible aumentar la seguridad, por ejemplo, en las contraseñas reflejo que podría ser vulnerada por cualquier usuario ya que la seguridad de la contraseña es muy frágil. Por ende, cabe recalcar con suma importancia guardar la integridad de la información, es decir, implementar protocolos de precaución para que la información no sea usada con fines maliciosos.

Conclusiones

Con los resultados obtenidos se concluye que debe aumentarse la seguridad, ya que por medio de las pruebas del sistema se pudo observar que tiene la limitación de un usuario y a su vez no permitirá avanzar en los procesos diarios eficientemente, se probó el posible acceso de 2 personas a la vez al mismo sistema y generó errores.

Empleando MBSA como instrumento se pudo detectar y reducir los peligros generales ya que ayudo a optimizar los procesos de seguridad para identificar errores de configuración de seguridad y encontrar errores en del sistema.

Con los objetivos previamente planteados cumplidos posterior al uso de la herramienta de identificación de errores se logró detectar falencias en el sistema para tomar las medidas necesarias y tener mayor confidencialidad en los datos.

Bibliografía

Alfaro, E. J. (2016). *Implantación de un Sistema de Detección de Intruso.* Valencia: Copyright.

Bolaños, D. E. (2015). *Riesgos, amenazas y vulnerabilidades de los sistemas de información.* Bogota: Paraninfos S.A.

Calder, A. (2017). *Sistema de Gestión de Seguridad de la Información.* Reino Unido: Publishing.

Diaz.C. (2014). *Normas dentro de un Sistema de Facturación.* Venezuela: Paraninfos S.A.

Garcia, J. (2014). *Estudios de Evaluación Específicos.* New York: Naciones Unidas.

Gil, J. A. (2016). *TÉCNICAS E INSTRUMENTOS PARA LA RECOGIDA DE INFORMACIÓN.* Madrid.

Hammer, M. (2015). *La Revolución de la reingeniería: un manual de trabajo.* Madrid: Diaz de Santos S.A.

Kendall, K. E. (2015). *Análisis y Diseño de Sistema.* Mexico: Pearson Educación.

Lechtaler, A. R. (2015). *Comunicaciones - Una introducción a las redes digitales de.* Argentina: Alfaomega.

Maroto, J. (2014). *Estrategia de la visión a la acción.* España.

Olebau, J. I. (2014). *Metodología de la investigación cualitativa.* E.E U.U.

Piquero, J. V. (2015). *Practica de Redes.* Peru: Paraninfos S.A.

Sommerville, I. (2015). *Ingeniería del Software Séptima Edición.* Madrid: PEARSON EDUCACION S.A. .

Stallings, W. (2014). *Fundamentos en Seguridad en Redes Aplicaciones y Estándares.* Madrid: Pearson Educación S.A.

Tuya, J. (2015). *Técnicas cuantitativas para la gestión en la ingeniería del software.* España: NETBIBLO S.A.

Ugarte, J. (2014). *Discurso historia informática: la palabra economía en los textos económicos.* Colombia: Paraninfos S.A.

Valbuena, S. J. (2015). *Programación Avanzada en Java.* Colombia: ISBN.

Vera, A. (2016). *Ventajas y Desventajas de un Sistema.* Mexico: ARP. S.A.

Zapata, A. O. (2015). *Herramientas para elaborar investigaciones.* Mexico: Pax Mexico.