UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E

INFORMÁTICA PROCESO DE TITULACIÓN

MAYO – SEPTIEMBRE
2019

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE

CARRERA PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

TEMA:

Análisis de Amenazas y Vulnerabilidades del Sistema AlquimiaSoft de la Notaria Primera de la ciudad de Babahoyo

EGRESADO:

MORA CADENA ESTEFANIA DAMARIS

TUTOR:

Ing. León Acurio Joffre

AÑO 2019

INTRODUCCION

Actualmente la tecnología ha contribuido para que los negocios surjan con más rapidez y con mejores resultados, hoy por hoy la implementación ya no es un lujo o una inversión sino una necesidad fundamental. El entorno competitivo en el que se mueven las empresas obliga a cambiar continuamente e invertir en nuevas técnicas, por este motivo está más presente en las empresas por ende es necesario adaptarse a las tendencias y estar lo más actualizado posible.

Los avances científicos se desarrollan en todos los ámbitos de nuestra vida y cada día se descubre o mejora algo gracias a ello podemos decir que al pasar los años nos va facilitando la vida cada vez más y nos ayuda en cada una de las actividades que desempeñamos a diario.

La presente investigación nos indica las actividades de facturación que se realiza en la notaria primera tales como: registro de compra y venta bienes e inmuebles (carro, casa etc.) declaraciones juramentadas, certificación de documentos públicos y privados, terrenos, etc. La facturación electrónica viene de la mano debido a la modernización existente, dentro de esta institución pública trabajan con el software AlquimiaSoft donde ingresan en facturación notarial diseñada para el registro, control y verificación de la información en la cual podrá ser visualizada todos los registros que se efectúan a diario dentro del sistema.

El problema principal radica en posibles vulnerabilidades y amenazas que pueden existir dentro del sistema, debido a que los datos que manejan no son seguros , es por eso que cada

usuario que acceden al sistema pueden observar los diferentes tramites que realizan los trabajadores encargados de ingresar información que se requiere para determinado servicio.

Por ende, se debe de realizar un estudio a través de las herramientas desarrollada por Microsoft como lo son MSBA y SUCURI con las cuales se harán las pruebas necesarias para determinar las amenazas y vulnerabilidad que tiene el software AlquimiaSoft permitiendo determinar con exactitud los riesgos que pueden afectar a la institución.

Los datos se expresarán en términos cualitativos ya que proporcionan una gran cantidad de información valiosa que consiste en la construcción de una teoría a partir de una serie de proposiciones extraídas desde el punto de partida que hemos realizado paso a paso, para lo cual no es necesario extraer una muestra representativa, sino una muestra teórica conformada por uno o más casos. El análisis cualitativo tiene en cuenta las amenazas, las vulnerabilidades, el impacto y ocasionalmente, los controles.

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 Sublinea, Procesos de transmisión de datos y telecomunicaciones.

DESARROLLO

Mediante el presente estudio se determinará las amenazas y vulnerabilidades que pueden existir dentro del sistema de facturación de la Notaria Primera ubicada en la ciudad de Babahoyo

Cabe recalcar que este estudio está estrechamente relacionado o enfocado a tratar del análisis de los procesos que realiza el sistema ya que a través de la investigación que realizamos sabemos lo importante que son los procesos que se dan dentro de un sistema informático. (Ugarte, 2014)

Una vez recopilada la información, se hará uso de una herramienta para el estudio de las amenazas y vulnerabilidades dentro del sistema, logrando conocer los riesgos o problemas que se presenta en la notaria y cuáles serían las medidas a tomar dentro del software. Al momento de realizar el escaneo dentro del software se solicitó el permiso a la encargada para determinar el nivel de riesgo existente. Los principales beneficios al realizar el escaneo son:

Disminución de los riesgos que pueden generar robos de información y garantizar la integridad de la información a través de la red. Para realizar el escaneo del software hemos utilizado las herramientas desarrolladas por Microsoft como lo son el MBSA y SUCURI con las cuales se harán las pruebas necesarias. (Maroto, 2014)

MBSA: Ayuda a encontrar y minimizar los riesgos de seguridad generales, evaluando la falta de actualizaciones de seguridad, MBSA sólo buscará las actualizaciones de seguridad que falten, detectando los errores más comunes de configuración y actualizaciones de seguridad que falten en sus sistemas informáticos. Con esta sencilla herramienta puedes realizar un análisis automático de tu sistema en busca de posibles vulnerabilidades y fallos de seguridad.

Es una de las aplicaciones que ofrece Microsoft para verificar la seguridad de los equipos informáticos. Esta utilidad permite verificar la seguridad de la máquina, o la de un conjunto de ellas dentro de la red, ofreciendo información acerca del estado de los puertos abiertos en la conexión TCP/IP, y toda una serie de vulnerabilidades a las que se pueden ser susceptibles, incluso las que afectan al propio navegador web. Asimismo, de manera adicional, suministra información y recomendaciones que permitirán resolver las incidencias que se presentan.

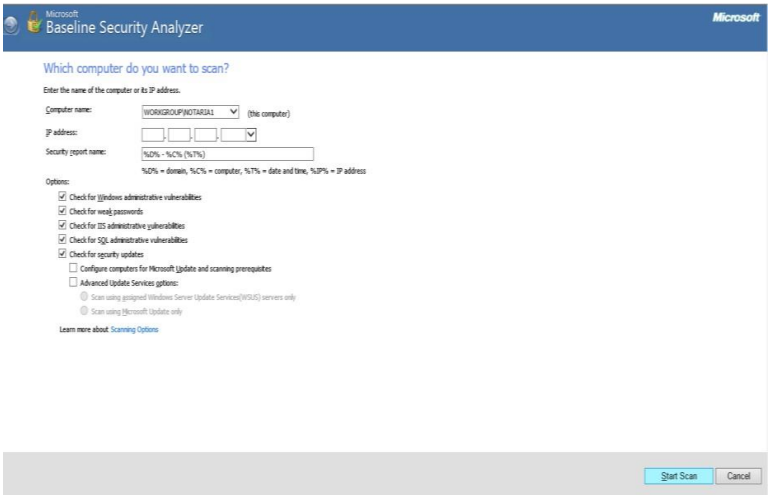

Figura: N.º 1 Para poder arrancar la aplicación se procederá a escoger el nombre del pc

Elaborado por: Estefanía Mora

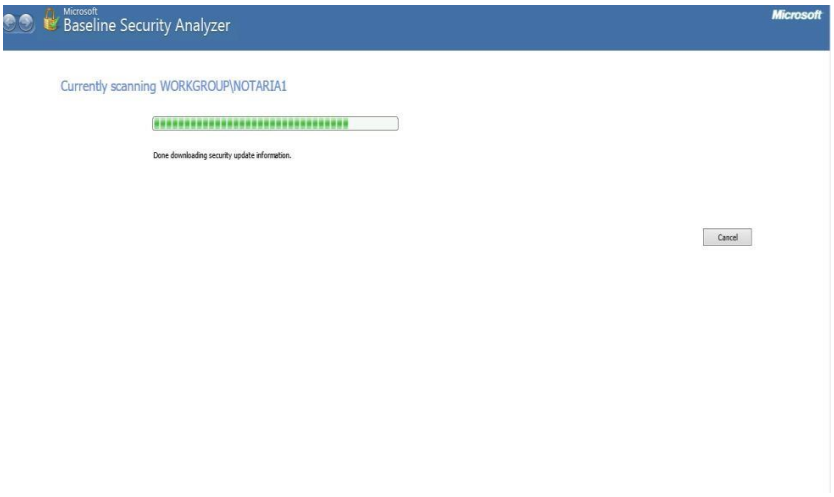

Figura: N.º 2 El programa mostrará una ventana de progreso como esta.

Elaborado por: Estefanía Mora

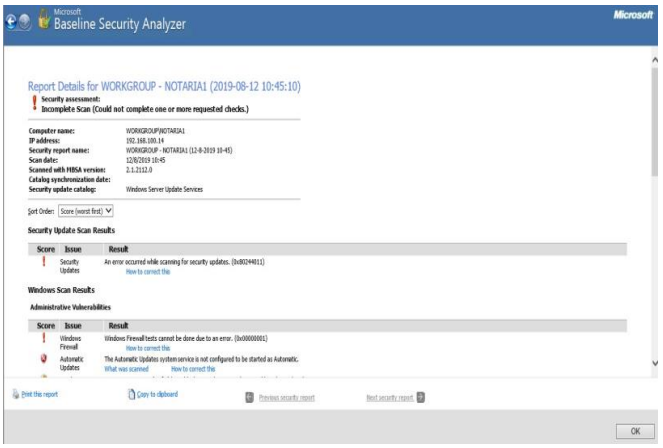

Figura: N.º 3 Muestra los datos del pc y está procediendo a realizar un escaneo dentro del sistema

Elaborado por: Estefanía Mora

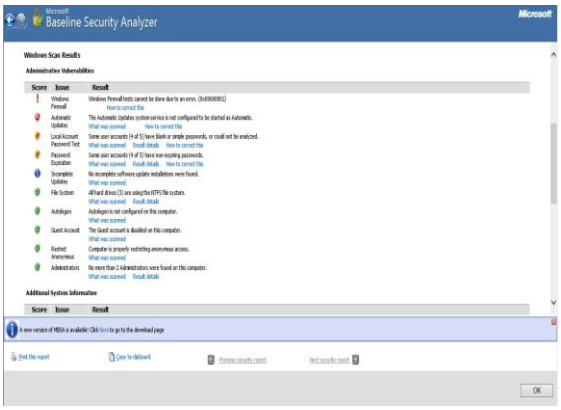

Figura: N. º 4 Cuando MBSA ha terminado de generar los informes, podremos ver un historial en el cual indica el estado en que se encuentra cada uno de ellos

Elaborado por: Estefanía Mora

SUCURI: Monitoriza tu software en busca de malware, a su vez escanea automáticamente en busca de malware y supervisa la web en cuanto a irregularidades. Si se encuentra malware, inmediatamente creará una alerta y enviará una solicitud de limpieza, además proporciona una solución muy potente pero muy sencilla para mantener tu web segura y limpia.

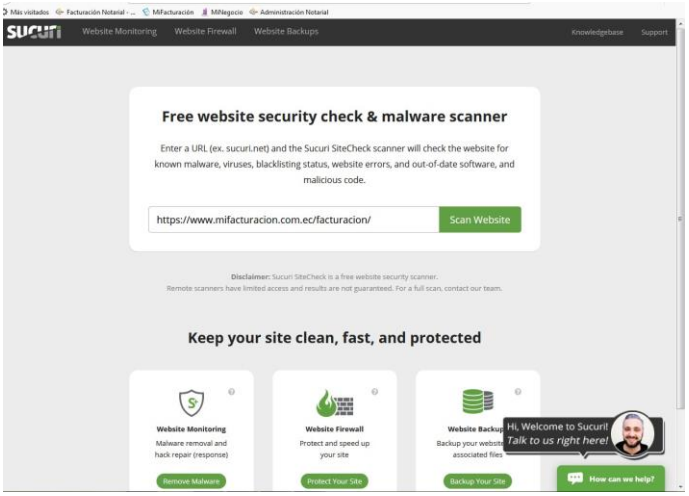

Figura: N.º 4 Pantalla de inicio de la herramienta Sucuri.

Elaborado por: Estefanía Mora

En base a las pruebas realizadas en el sistema pude notar que como resultado de estas pruebas con la herramienta MBSA se pudo evaluar las vulnerabilidades del sistema, y también se detectó dentro de los servicios administrativos como están distribuidos, por lo que esta herramienta contribuye a las empresas a determinar su estado de seguridad acordado a las recomendaciones de seguridad de Microsoft.

Anteriormente, la información de los trámites que se realizaban en las notarías era ingresada de forma manual, lo que daba lugar a errores en los registros de protocolos y diligencias. (Diaz, 2014)

Java es el lenguaje de programación en que esta hecho el software debido a que el código Java, una vez compilado, puede llevarse sin modificación alguna sobre cualquier máquina, y ejecutarlo. Java es un lenguaje de programación de alto nivel orientado a objeto que permite la creación de programas multiplataforma en hardware y software. (Valbuena, 2015)

Alquimiasoft cuenta con los módulos adecuados para poder llevar un registro de todas las actividades que realizan los encargados de manejar el sistema y a su vez este sistema reduce el tiempo de entrega de todo lo que solicitan los usuarios.

Como resultado se obtiene la descripción del sistema y la especificación de lo que debe hacer cada una de sus partes. A continuación, se podrá analizar el sistema en el cual se está trabajando, además analizaremos alguno de sus módulos.

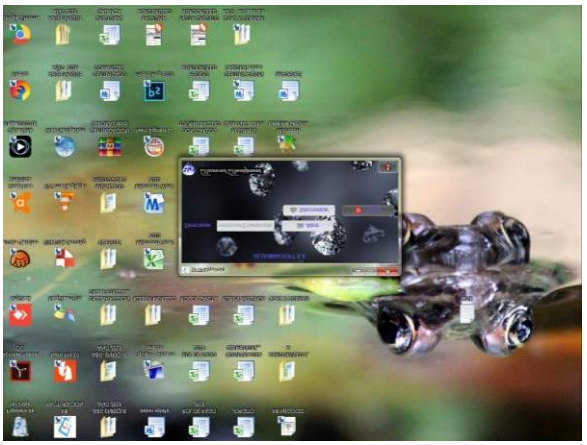

Figura: Nº5 Pantalla de Inicio del Sistema AlquimiaSoft

Elaborado por: Estefanía Mora

Un sistema es un conjunto de partes formados por el hardware parte tangible, software parte lógica de un computador y las personas que lo emplean, que se

relacionan entre sí para almacenar y procesar información con un objetivo en común. (Hammer, 2015)

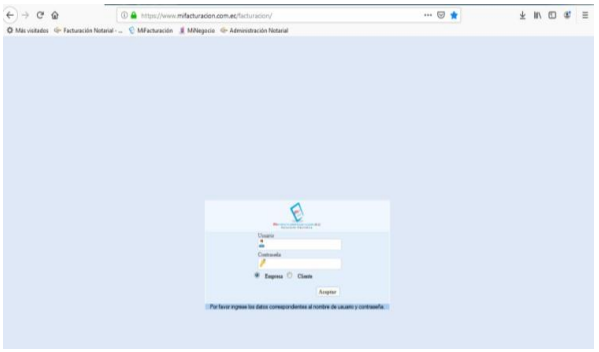

Figura N. º6 Ingreso al sistema
Elaborado por: Estefanía Mora

Una vez que se termina la fase de análisis dentro del sistema se verificara que funcione correctamente. El objetivo de las pruebas es el de obtener información de calidad del software. (Tuya, 2015)

Una vez que se han desarrollado todas las funcionalidades dentro del sistema se debe de comprobar que funcionan correctamente. (Kendall, 2015)

El periodo de mantenimiento puede durar años, para llevar a cabo correctamente la fase de mantenimiento, se necesita trazar un plan de antemano que asegure todos los escenarios que puedan producirse. (Sommerville, 2015)

Es así como se refleja mediante la factura electrónica emitida por el sistema con su respectivo tramite.

NOTARIA PRIMERA
CANTÓN BABAHOYO

ENRIQUE ISIDRO MOREIRA ARRIAGA
NOTARIA PRIMERA - LOS RIOS - BABAHOYO
Dirección Matriz: SUCRE (506) Y GARCIA MORENO
Dirección Sucursal:
OBLIGADO A LLEVAR CONTABILIDAD NO

R.U.C.: 1203738339001
FACTURA
No. 002-002-000045251
NÚMERO DE AUTORIZACIÓN
1507201901120373833900120020020000452510000734413
FECHA Y HORA DE AUTORIZACIÓN 2019-07-15T17:09:45-05:00
AMBIENTE: PRODUCCION
EMISIÓN: NORMAL
CLAVE DE ACCESO
1507201901120373833900120020020000452510000734413

Razón Social / Nombres y Apellidos: LUIS ENRIQUE PAREJA FRANCO
RUC / CI: 1203612260
Fecha Emisión: 15/07/2019
Guia Remisión:

Cod. Principal	Cod. Auxiliar	Cant	Descripción	Precio Unitario	Descuento	Precio Total
		1	(1) CONSULTA DATOS BIOMETRICOS SISTEMA NACIONAL DE IDENTIFICACIÓN CIUDADANA - REGISTRO CIVIL (P)	0.30	0	0.30
		1	ACLARATORIA, AMPLIATORIA, MODIFICATORIA, RECTIFICATORIA O RATIFICATORIA	78.80	0	78.80

SUBTOTAL 12 %	78.8
SUBTOTAL 0%	0.3
SUBTOTAL No objeto de IVA	0.00
SUBTOTAL SIN IMPUESTOS	79.10
DESCUENTO	0

Declare a tiempo su impuesto a la renta.

Información Adicional
Matrizador SARA MERCEDES URCUANGO NARANJO
NÚMERO DE LIBRO 2019126100 1P02072

Figura: N. º 7 Factura emitida por el sistema
Elaborado por: Estefanía Mora

Para evitar futuros conflictos con el cliente, hay que especificar cómo los usuarios solicitarán las modificaciones durante los tramites. (Vera, 2016)

Para poder usar la técnica de observación se debe determinar la investigación, luego la información que se va a recolectar, permitiendo cumplir con el propósito. (Gil, 2016)

Todo en esta vida y conlleva un proceso aún más en los sistemas informáticos que se hacen necesarios, en la actualidad para cualquier empresa con o sin fines de lucro necesita llevar procesos de forma nítida y especifica de manera que sus transacciones se agilicen y sean de beneficio propio. (Olabuénaga, 2014)

La estructura de la red dentro del establecimiento se encuentra estructurado de manera jerárquica debido a que no es más que una red cuya configuración obedece a un conjunto de reglas, por eso es que la topología jerárquica se define como la cadena de comunicación usada por los nodos que la conforman. (Lechtaler, 2015)

Se utilizó cisco Packet Tracer el cual es un programa de simulación de redes que permite mostrar el comportamiento de la red. El cual cuenta con diferentes dispositivos como lo son: router, switchs, hubs etc. A su vez es una herramienta de simulación de redes innovadora y potente que se utiliza para prácticas por lo que a través de esta herramienta se mostrara la estructura de la red dentro del lugar en que se está realizando el estudio de caso. (Piquero, 2015)

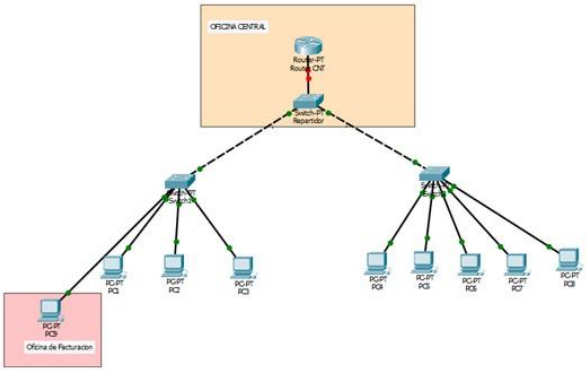

Figura: Nº4 Estructura de la red del establecimiento

Elaborado por: Estefanía Mora

El resultado de esto es una red topológica de tipo árbol, ya que desde el primer Router que se tiene se ramifica la distribución de internet dando lugar a la creación de nuevas redes o subredes tanto internas como externas.

La metodología cualitativa dentro del estudio de caso se encarga de la recolección de datos a partir de la observación realizando una entrevista la cual se caracteriza por ser flexible, debido a que se enfoca más en una conversación que se adapta a la personalidad del encuestado.

Otra metodología utilizada para la investigación es la de campo debido a que obtengo datos e información a través de la técnica de observación, mediante la cual se puede analizar posibles fallos dentro del sistema a través del instrumento de guía de observación. (Hammer, 2015)

En la actualidad, una entrevista es el mejor medio para aquellos funcionarios públicos, puedan dar a conocer información detalladamente.

Algunos de los beneficios de la entrevista son:

- Se tocan temas de gran importancia, los cuales no necesariamente serán positivos.
- Tienen un alto contenido, en especial cuando es revelada información que se mantuvo secreta durante largo tiempo. (Garcia, 2014)

Seguridad de la información / Seguridad informática

La seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene mientras que la seguridad de la información integra toda la información independientemente del medio en el que esté.

En general, un sistema será seguro o fiable si consta de estos tres aspectos:

- **Confidencialidad**: Acceso a la información solo mediante autorización y de forma controlada.
- **Integridad**: Modificación de la información solo con autorización.

- **Disponibilidad**: La información del sistema debe estar con acceso mediante autorización.

Vulnerabilidades de un sistema informático

En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que conforman el sistema y que podemos agrupar en:

- **Hardware**: Elementos físicos del sistema informático.
- **Software**: Programas que se ejecutan sobre el hardware.
- **Datos**: Comprenden la información lógica que procesa el software haciendo uso del hardware.

De ellos los más críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.

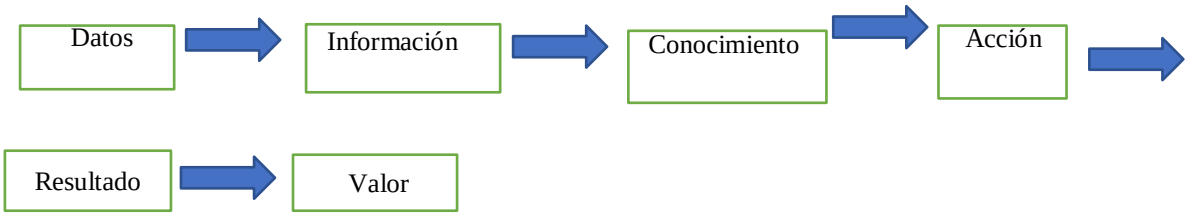

Figura: Nº4 Secuencia de datos

Elaborado por: Estefanía Mora

El activo más crítico son los datos, debido a que el resto se puede reponer con facilidad y los datos sabemos que dependen de la empresa. (Zapata, 2015)

Amenazas y Vulnerabilidades

Los riesgos de la información en la red es más que un problema de protección de datos, y debe estar básicamente orientada a asegurar las amenazas que pueden venir de cualquier parte, sea interna o externa.

Las vulnerabilidades son una debilidad en la tecnología o en los procesos asociados con los datos, y como tal, se consideran características propias de los sistemas o de la infraestructura que lo soporta.

Hay personas que por medio de las tecnologías vulneran los sistemas en la red, robar información o infectarlos con comportamientos dudosos, son comúnmente conocidos como hackers.

Su forma de actuar los determina como:

Hacker de Sombrero Blanco: Son expertos en seguridad informática.

Hacker de Sombrero Negro: Conocidos como crackers, vulneran los sistemas de información con fines maliciosos.

Hacker de Sombrero Gris: No atacan malintencionadamente, sino que sus motivaciones se relacionan a protestas o desafíos personales.

Ataques en la Red

Tenemos como principales atacantes en la red los siguientes:

Malware: Se refiere de forma genérica a cualquier software malicioso que tiene por objetivo infiltrarse en un sistema para dañarlo.

Virus: Es un código que infecta los archivos del sistema mediante un programa maligno, pero para ello necesita que el usuario lo ejecute directamente

Gusanos: Es un programa que, una vez infectado el equipo, realiza copias de sí mismo y las difunde por la red.

Troyanos: Busca es abrir una puerta trasera para favorecer la entrada de otros programas maliciosos.

Prevención de Ataques a una Red

Para mantener un cierto grado de protección de la información conectada a la red, lo principal es entender cómo pueden sucederse estos ataques y en qué consisten dichas amenazas.

Existen diferentes formas efectivas para evitar ataques Tales como:

***Ramsonware*:** Es necesario tener actualizado el sistema operativo y todas las soluciones de seguridad, así como el antivirus y el firewall; evitar los accesos administrativos desde fuera de la entidad, y en caso necesario, permitirlos sólo mediante protocolos seguros.

Escaneo de Puertos: Una forma efectiva es cerrar los puertos o servicios que no se utilizan en los sistemas, siempre que sea posible.

***Phishing*:** Rechazar y no responder ninguna solicitud de información confidencial como contraseñas, así como nunca descargar ni ejecutar archivos adjuntos de personas desconocidas. (BOLAÑOS,
2015)

IDS (IDENTIFICACIÓN DE INTRUSOS)

Hace referencia a un mecanismo que, escucha el tráfico en la red para detectar actividades sospechosas, y de este modo, reducir el riesgo de intrusión. Monitoriza los eventos que ocurren en un sistema informático en busca de intentos de intrusión.

Definimos intento de intrusión como cualquier intento de comprometer la confidencialidad, integridad, disponibilidad o evitar los mecanismos de seguridad de una computadora o red. Las intrusiones se pueden producir de varias formas: atacantes que acceden a los sistemas desde Internet, usuarios autorizados del sistema que intentan ganar privilegios adicionales para los cuales no están autorizados y usuarios autorizados que hacen un mal uso de los privilegios que se les han asignado

Al utilizar un ID protege de las amenazas que aparecen al incrementar la conectividad en red y la dependencia que tenemos hacia los sistemas de información. También un sistema de detección de intrusión debido a la implementación de una buena política de IDS es fundamental en cuanto a seguridad, este recurso si se actualiza constantemente se debe de mantener ataques ya sea desde la red, o por un ordenador. (Alfaro, 2016)

Características de IDS

- Debe ser capaz de sobrevivir a una caída del sistema.

- Debe imponer mínima sobrecarga sobre el sistema.

- Debe observar desviaciones sobre el comportamiento estándar.

- Debe ser fácilmente adaptable al sistema ya instalado

- Debe ser difícil de "engañar".

Políticas de seguridad de la información ISO 27001 – 27002

ISO 27001: Permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El estándar ISO 27001 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos, esta norma ayuda a empresas a manejar tanto las incidencias de seguridad de una forma más eficaz, como los eventos de seguridad, incidentes de seguridad y no cumplimientos.

Como beneficios dentro de la norma ISO 27001 tenemos:

- Identificar los riesgos y establecer controles para gestionarlos.

- Confidencialidad asegurando que sólo quienes estén autorizados puedan acceder a la información.
- Flexibilidad para adaptar los controles a todas las áreas de su empresa o solo a algunas seleccionadas
- Alcanzar las expectativas demostrando conformidad.

Estructura de la Norma ISO 27001

Objeto y campo de aplicación: La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.

Referencias Normativas: Recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO27001.

Términos y Definiciones: Describe la terminología aplicable a este estándar.

Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto.

Liderazgo: Elabora una política de seguridad que conozca toda la organización y asigna roles, responsabilidades y autoridades dentro de la misma.

Planificación: Es la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información.

Soporte: La norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, pertinente para cada caso.

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: Proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión.

Se la define en el estándar como la preservación de la confidencialidad, integridad y disponibilidad. Para saber más sobre los demás dominios es importante conocer sobre la norma ISO 27002 complemento para la ISO 27001.

La importancia de disponer de una completa información es la clave para realizar todas las actividades en las diferentes áreas. Sin embargo, es más importante mantener dicha información con seguridad para que no se pierda, o se deteriore de cualquier forma. Al fin y al cabo, la información y los datos de los que dispone la organización y que recopila en su día son uno de los activos más valiosos que pueden marcar el futuro de la organización. (Calder, 2017)

Seguridad en Redes

El no tener una buena seguridad en la red implica que un hacker pueda acceder fácilmente a la red interna. Se debe de tener en cuenta que tampoco es muy fiable conformarse con un antivirus ya que no son capaces de detectar todas las amenazas e infecciones dentro del sistema además son vulnerables que hacen que la seguridad se vea afectada. (Stallings, 2014)

Normas de Seguridad en Redes

En cuanto normas tenemos lo siguiente:

- Evitar situaciones que afecten a la seguridad de las redes.
- Deben aplicarse todas las actualizaciones de seguridad que necesite el sistema operativo.
- Se utilizarán protocolos seguros que permitan el cifrado y guardado de las contraseñas.
- Instalar solo el software que se vaya a necesitar.
- Se debe tener la seguridad de servidores de cualquier tipo (FTP, Web, NTP, etc.) de los que sean responsables.

Beneficios de aplicar las herramientas anteriormente mencionadas en las pruebas realizadas al software

Es que gracias al análisis que se realizó dentro del software se podrá mejor la seguridad dentro del mismo, por ejemplo en las contraseñas reflejo que podría ser vulnerada por cualquier usuario. Además cabe recalcar que es muy importante conservar la integridad de los datos es decir que se debe de tomar medidas de precaución para que la información no sea filtrada ni le den un mal uso.

Conclusiones

En base a la información recopilada es necesario dentro de esta institución la facturación electrónica debido a que permitirá avanzar en los procesos diarios, prueba de ello es que ayudará de manera eficiente lo que es la búsqueda y localización rápida de los documentos; además este sistema garantiza un procedimiento ágil en los servicios que prestan a diario.

Al aplicar la herramienta MBSA ayuda a encontrar y minimizar los riesgos generales, se encarga de buscar actualizaciones de seguridad que falten.

Por ende, esta herramienta mejorara el proceso de administración de seguridad para detectar errores de configuración de seguridad e identificar los fallos dentro del sistema.

Referencias

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.* Bogotá: 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.

García, 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.* México: Pearson Educación.

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

Maroto, J. C. (2014). *Estrategia: de la visión a la acción.* España: Paraninfos S.A.

Olabuénaga, J. I. (2014). *Metodología de la investigación cualitativa.* E.E.U.U: Universidad de Deusto.

Piquero, J. V. (2015). *Practica de Redes.* Perú: 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. En S. J. Valbuena, *Programación Avanzada en Java.* Colombia: ISBN.

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

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

ANEXOS

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
ESCUELA DE SISTEMAS

Entrevista dirigida a la Ing. Mariela Malta García encargada del uso del sistema en la Notaria Primera de la Ciudad de Babahoyo.

1. ¿Considera usted que el sistema con el que se trabaja está acorde con todo lo que realizan dentro de la institución?

2. ¿Cada que tiempo le dan soporte técnico al sistema?

3. ¿Qué la motivo a usted ser parte de este equipo de trabajo?

4. ¿Con que sistema Operativo trabajan dentro de la institución?

5. ¿Considera usted que cada trabajador cuenta con conocimientos adecuados para poder laboral con el sistema?

6. ¿Ha existido algún tipo de perdida de información dentro del sistema?

7. ¿Lleva usted algún control de las actividades que realizan a diario?

8. ¿Cree usted que el software con el que trabajan es el adecuado?

9. ¿Les ha dado problemas el sistema en algún momento?

10. ¿Por qué trabajan con este software?

Al realizar esta entrevista se obtuvieron resultados positivos, debido a que cuentan con el personal adecuado, y también con las herramientas y equipos necesarios que ayudan de una u otra manera y son de gran aporte para poder prestar un buen servicio a los usuarios que lo requieren.

GUÍA DE OBSERVACIÓN

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
ESCUELA DE SISTEMAS

Guía de observación para el análisis de amenazas y vulnerabilidades dentro del sistema de Facturación de la Notaria Primera ubicada en la Ciudad de Babahoyo.

Fecha:		Página _____ de _____
Auditor:		

Actividad / Proceso/ ítem a revisar	**Cumple**	**No cumple**	**Comentarios**
Verificar si el sistema de Facturación cuenta con un buen mantenimiento técnico.			
Cuenta con seguridad el sistema.			
Da reporte mensual sobre las transacciones ejecutadas dentro de la entidad.			
Los datos ingresados son validados correctamente.			
Cuenta con las herramientas adecuadas para las transacciones.			

CAPTURAS DEL SISTEMAS

Nº1 Ingreso al sistema Alquimiasoft
Elaborado por: Estefanía Mora

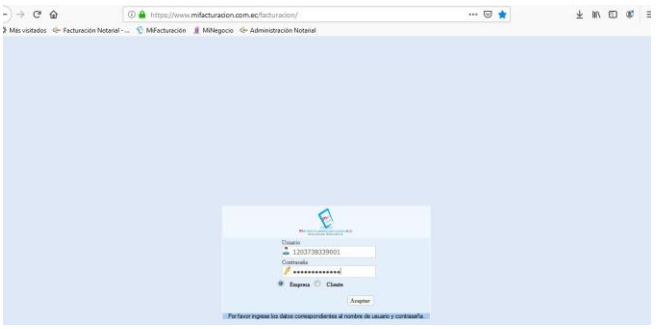

FIGURA Nº2 Ingreso con el respectivo usuario y contraseña para tener acceso al sistema

Elaborado por: Estefanía Mora

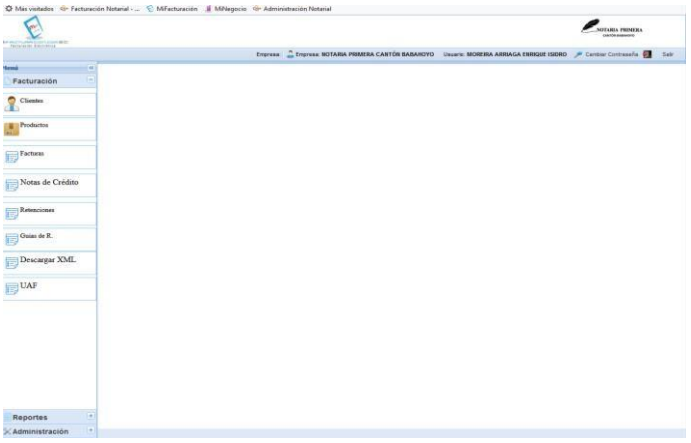

Figura Nº3 Módulos con la cuenta el sistema
Elaborado por: Estefanía Mora

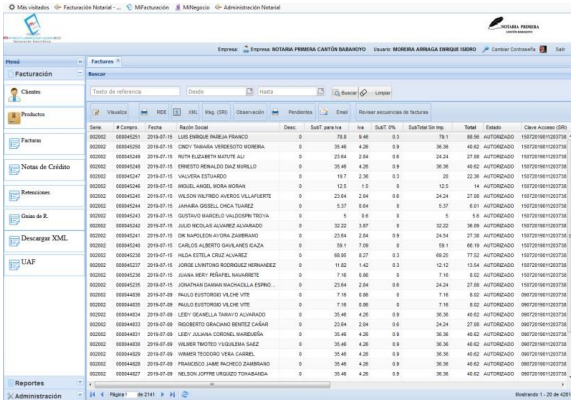

FIGURA Nº4 Registro de Facturación de cada usuario
Elaborado por: Estefanía Mora


NOTARIA PRIMERA
CANTÓN BABAHOYO

R.U.C.: 1203738339001

FACTURA

No. 002-002-000045251

NÚMERO DE AUTORIZACIÓN

1507201901120373833900120020020000452510000734413

FECHA Y HORA DE AUTORIZACIÓN 2019-07-15117:09:45-05:00

AMBIENTE: PRODUCCION

EMISIÓN: NORMAL

CLAVE DE ACCESO

1507201901120373833900120020020000452510000734413

ENRIQUE ISIDRO MOREIRA ARRIAGA

NOTARIA PRIMERA - LOS RIOS - BABAHOYO

Dirección Matriz: SUCRE (506) Y GARCIA MORENO

Dirección Sucursal:

OBLIGADO A LLEVAR CONTABILIDAD NO

Razón Social / Nombres y Apellidos: LUIS ENRIQUE PAREJA FRANCO RUC / CI: 1203612260

Fecha Emisión: 15/07/2019 Guía Remisión:

Cód. Principal	Cód. Auxiliar	Cant	Descripción	Precio Unitario	Descuento	Precio Total
		1	11) CONSULTA DATOS BIOMETRICOS SISTEMA NACIONAL DE IDENTIFICACIÓN CIUDADANA - REGISTRO CIVIL (D)	0.00	0	0.00
		1	12) JUDICATORIA AMPLIATORIA, MODIFICATORIA, RECTIFICATORIA O RATIFICATORIA	70.00	0	70.00

Declare a tiempo su impuesto a la renta.

Información Adicional

Notarizador SARA MERCEDES URQUIAGO NARANJO

NÚMERO DE LIBRO

SUBTOTAL 12 %	70.0
SUBTOTAL 0%	0.0
SUBTOTAL No objeto de IVA	0.00
SUBTOTAL SIN IMPUESTOS	70.00
DESCUENTO	0

Figura Nº5 Factura que emite el sistema
Elaborado por: Estefanía Mora

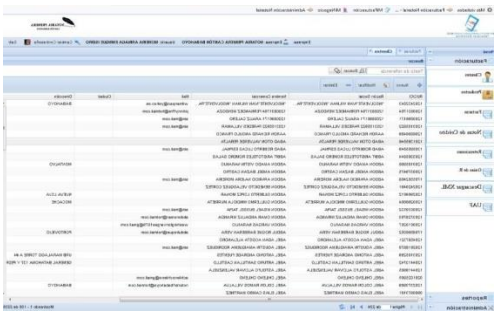

Figura Nº6 Búsqueda de Usuario
Elaborado por: Estefanía Mora

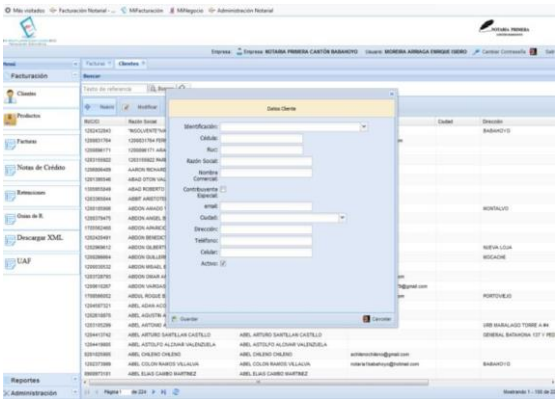

Figura Nº7 Ingreso de datos de un nuevo cliente

Elaborado por: Estefanía Mora

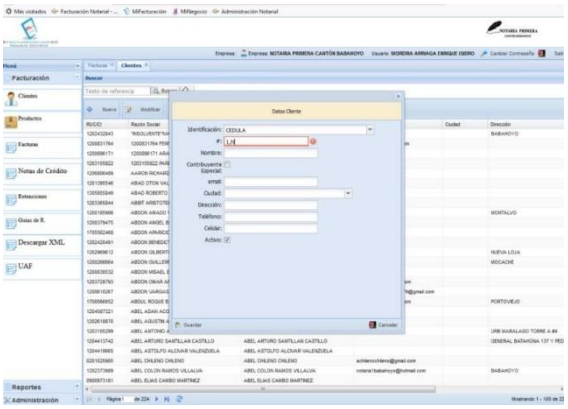

Figura Nº8 Todos los campos cuentan con sus validaciones correctas

Elaborado por: Estefanía Mora

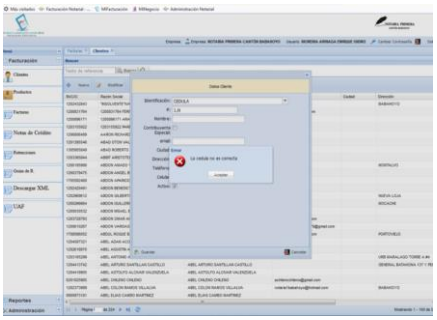

Figura Nº9 Campos validados al ingresar datos incorrectos
Elaborado por: Estefanía Mora

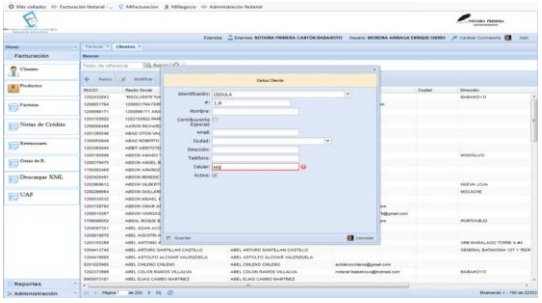

Figura Nº10 No se registran datos incompletos
Elaborado por: Estefanía Mora

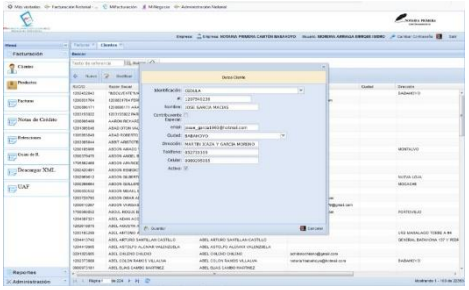

Figura Nº11 Ingreso de datos del usuario

Elaborado por: Estefanía Mora

Figura Nº12 Ingreso a la Notaria
Elaborado por: Estefanía Mora

Figura Nº13 Departamento de Facturación
Elaborado por: Estefanía Mora

Figura Nº14 Oficina del Notario Abg.
Enrique Arriaga
Elaborado por: Estefanía Mora

FiguraNº15 Entrevista a la Ing. Mariela Malta encargada del manejo del sistema
Elaborado por: Estefanía Mora