Análisis de amenazas y vulnerabilidades de la gestión de procesos del sistema informático en la Cooperativa de Taxis San Fernando de Babahoyo

Analysis of threats and vulnerabilities of the process management of the computer system in the San Fernando de Babahoyo Taxi Cooperative

https://doi.org/10.5281/zenodo.7726451

AUTORES: Fabián Eduardo Alcoser Cantuña[1]*

Raúl Armando Ramos Morocho[2]

Paulino Javier Suárez Guamán[3]

Jasume Nayeli Crespo Orozco[4]

DIRECCIÓN PARA CORRESPONDENCIA: falcoserc@utb.edu.ec

Fecha de recepción: 01 / 09 / 2022

Fecha de aceptación: 21 / 11 / 2022

RESUMEN

Durante años las aplicaciones web han sido vulneradas, admitiendo que elementos no autorizados consigan acceso a la información confidencial, ocasionando una serie de inconvenientes dentro las organizaciones y Cooperativas de nuestro país. Actualmente la seguridad en aplicaciones web es de vital importancia, se están invirtiendo un gran número de recursos para poder neutralizar los ataques a los cuales se encuentran expuestos. El problema de la cooperativa de taxis San Fernando de la ciudad de Babahoyo, es que no tiene determinadas las amenazas y vulnerabilidades a las que se encuentran expuestas diariamente en su sitio web, un usuario no autorizado puede acceder al sitio y modificar la información,

[1]* Universidad Técnica de Babahoyo, Facultad de Administración Finanzas e Informática (FAFI), Babahoyo, Ecuador, falcoserc@utb.edu.ec

[2] Universidad Técnica de Babahoyo, Facultad de Administración Finanzas e Informática (FAFI), Babahoyo, Ecuador, rramos@utb.edu.ec

[3] Universidad Técnica de Babahoyo, Facultad de Ciencias de la Salud (FCS), Babahoyo, Ecuador, jsuarez@utb.edu.ec

[4] Empresa privada: Jsstechnologies, Analista de multifacturación y firmas electrónicas, Email: jcrespo129@fafi.utb.edu.ec

así como llevarse información sensible y confidencial de la Cooperativa y de los Socios. Tienen recelo por la triada CID (Confidencialidad, Integridad, Disponibilidad) de la información que es utilizada en la aplicación Web. En la actualidad dicho software no cuenta con un administrador de Software, que efectúe los mantenimiento y mejoras del mismo, ocasionando un retardo en los procesos administrativos de la cooperativa. Con este propósito sé delimitó el caso de estudio que permitió estudiar la disponibilidad del sistema Web y valorar los mecanismos de ciberseguridad en el mismo; para lo cual, se utilizó la técnica de investigación relacionada al análisis de gestión de riesgos dentro de los sistemas informáticos aplicándose la metodología MAGERIT.

Palabras claves: Información, amenazas, vulnerabilidades, sistemas, riesgos.

ABSTRACT

For years web applications have been violated, allowing unauthorized elements to gain access to confidential information, causing a series of problems within organizations and Cooperatives in our country. Security in web applications is currently of vital importance, a large number of resources are being invested in order to neutralize the attacks to which they are exposed. The problem of the San Fernando taxi cooperative in the city of Babahoyo, is that it does not have certain threats and vulnerabilities to which they are exposed daily on its website, an unauthorized user can access the site and modify the information, as well how to take sensitive and confidential information from the Cooperative and its Members. They are suspicious of the CID triad (Confidentiality, Integrity, Availability) of the information that is used in the Web application. Currently, said software does not have a Software administrator, who performs its maintenance and improvements, causing a delay in the administrative processes of the cooperative. For this purpose, the case study was delimited, which allowed studying the availability of the Web system and assessing the cybersecurity mechanisms in it; for which, the research technique related to risk management analysis within computer systems was used, which is referred to as the MAGERIT methodology.

Keywords: Information, threats, vulnerabilities, systems, risks.

INTRODUCCIÓN

El análisis de riesgo, se refiere al estudio de posibles amenazas y vulnerabilidades existentes dentro de los sistemas informáticos, además de los daños y secuelas que éstas puedan producir. Vamos a utilizar el método cuantitativo por cuanto la información fue obtenida a

través de encuestas y adicionalmente una de las técnicas de investigación que se utiliza con mayor frecuencia para el análisis de gestión de riesgos dentro de los sistemas informáticos que es la metodología MAGERIT, para analizar, identificar y evaluar los riesgos que se enfrenta una aplicación web, evitar la ocurrencia de ciertas pérdidas y minimizar el impacto de otros. Así el costo del riesgo puede gestionarse y reducirse a sus niveles mínimos.

El problema de la cooperativa de taxis San Fernando de la ciudad de Babahoyo, es que no tiene determinadas las amenazas y vulnerabilidades a las que se encuentran expuestas diariamente en su sitio web. Tienen recelo por la triada CID (Confidencialidad, Integridad, Disponibilidad) de la información que es utilizada en la aplicación Web. En la actualidad dicho software no cuenta con un administrador de Software, que efectúe los mantenimientos y mejoras del mismo, ocasionando un retardo en los procesos administrativos de la cooperativa.

La información que publican corre el riesgo de no ser confidencial, debido a que la persona contratante para esta actividad no hace parte de la corporación y este proceso lo hace esporádicamente. Viéndose afectados de esta manera el personal de la Cooperativa por la demora y dificultad en el acceso a la información, riesgo de robo o corrupción de datos personales, interceptación de datos confidenciales, entre otros.

En los tiempos actuales las organizaciones ya sean públicas o privadas operan a través de sistemas informáticos para poder tener una eficiente administración de la información y de la gestión de los procesos, la mayor parte de estos sistemas se encuentran enlazados a la red por lo cual son vulnerables a diversos tipos de amenazas cibernéticas muchas veces ocasionadas por su mala utilización, estas amenazas pueden comprometer y ocasionar pérdida de integridad de los datos dentro de una organización.

Una planificación acorde a los estándares de ciber seguridad referente a la información de la organización, es necesaria por cuanto permite prevenir el constante crecimiento de las amenazas inducidas a los sistemas informáticos. Se ha identificado que el sistema informático se encuentra expuesto a diferentes tipos de amenazas y vulnerabilidades por parte de personas ajenas a la institución, situación que impide el correcto funcionamiento del mismo ocasionando la deficiente comunicación entre socios y el área administrativa, produciendo retrasos en la recaudación de los aportes y mantenimiento vehicular, que genera malestar en los socios de la cooperativa.

DESARROLLO

La Cooperativa de Taxis "San Fernando" de la ciudad de Babahoyo inició sus actividades el 22 de septiembre de 1990, cuya figura legal fue como una sociedad. La cooperativa se encuentra situada en la ciudadela Barrio Lindo, Av. Camilo Ponce y primera peatonal, adyacente al Terminal Terrestre de Babahoyo. Los servicios ofrecidos son de transporte de taxis a la colectividad babahoyense; la nómina de personal está conformada por 125 personas, las mismas que se encuentran distribuidas de la siguiente forma:

COOPERATIVA "SAN FERNANDO"	
CARGOS	**SOCIOS**
Presidencia	1
Gerencia	1
Secretaria	1
Comité de Vigilancia	3
Socios	119
TOTAL:	**125**

Tabla 1. Socios y Autoridades

Fuente: Los autores

El sistema de gestión de procesos de la Cooperativa de taxi San Fernando de la ciudad de Babahoyo admite a los socios a tener un perfil de usuario, el cual permite la sistematización de las actividades correspondientes para el registro en línea de los socios y la administración de actividades por parte del personal delegado de la coordinación.

La aplicación informática de la Cooperativa de taxi fue desarrollada en el año 2019, la ejecución de este software (elaborado en PHP) realiza diferentes procesos con lo cual se puede lograr una interacción de la información, obteniendo reportes de las unidades, fallas mecánicas, ventas de puestos y demás actividades de la cooperativa de una manera ágil y eficaz.

El inconveniente informático de la cooperativa de taxis San Fernando de la ciudad de Babahoyo, es falta de establecimiento de las amenazas y vulnerabilidades a las que se diariamente se encuentran expuestas en su sitio web. Actualmente dicho Sistema Web no

posees una persona encargada del mismo, que verifique o realice el mantenimiento y mejoras del mismo, originando lentitud en los procesos administrativos de la cooperativa.

La información que publican puede estar en peligro de no ser confidencial, por cuanto la persona encargada de esta actividad no forma parte de la cooperativa de taxi San Fernando y se realiza esporádicamente. Viéndose afectados de esta manera el personal de la Cooperativa por la demora y dificulta en el acceso a la información, riesgo de robo o corrupción de datos personales, Interceptación de datos confidenciales, entre otros.

En los últimos años, el lenguaje de programación PHP aparece en los primeros puestos de software confiables, siendo uno de los más usados. PHP es un lenguaje multiplataforma cómodo, flexible, potente y fácilmente extensible, ideal tanto para programar pequeñas soluciones como para acometer grandes proyectos informáticos. Estas características han hecho que se emplee tanto en informática doméstica como en ambientes científicos o entornos empresariales. (Gutiérrez, 2019)

Según ((Advisors., 2019) afirma que "Nessus es el estándar mundial para la prevención de ataques de red, identificación de vulnerabilidades y detección de problemas de configuración que utilizan los hackers para entrar en la red. Nessus se ha utilizado por más de 1 millón los usuarios en todo el mundo, por lo que es el líder mundial de evaluación de la vulnerabilidad, configuración de seguridad y cumplimiento de las normas de seguridad.", Nessus es un software de los más utilizados actualmente en la realización de pruebas de vulnerabilidades y amenazas en las organizaciones, nos ayuda a determinar e identificar los errores que poseen los sistemas con el fin de prevenir posibles ataques cibernéticos.

Según. (Urbina, 2016), Las empresas constantemente están amenazadas con sufrir daños en sus sistemas informáticos, estos daños pueden incitar a la perdida de datos (información de socios, contables, financieros). Las amenazas son mayores cuando en el sistema existen ciertas brechas de seguridad llamados vulnerabilidades que pueden perjudicar de gran manera a las organizaciones.

Actualmente la sociedad se está volviendo cada vez más un consumidor virtual por motivo de la demanda del uso de los softwares por parte de empresas o usuarios finales. Esto ha ocasionado un gran crecimiento de forma exponencial debido a la importancia de la implementación de la tecnología, la misma que ayuda a optimizar los procesos de gestión en la administración de información.

Información

La información es el activo más valioso de las organizaciones y es por eso que debe ser protegida de una manera adecuada, ya sea que se encuentre en forma digital o física, porque no importa en la forma que se encuentre la información o el medio por el cual esta se almacenada o compartida esta debe siempre estar salvaguardada apropiadamente. (Velthuis, 2018)

Seguridad Informática

Esta disciplina se orienta a las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo. (Cano, 2018)

La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. (Luan, 2019)

Gestión de Riesgos

Según Obando, T.(2007) manifiesta que: "La gestión del riesgo es un programa de trabajo y estrategias para disminuir la vulnerabilidad y promover acciones de conservación, desarrollo, mitigación y prevención frente a desastres naturales y antrópicos". (Obando, 2019)

Amenazas informáticas

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

considerar el riesgo como la probabilidad de que una amenaza concreta aproveche una determinada vulnerabilidad. (Romero, 2018)

Por lo tanto, podemos describir una amenaza informática aquella operación que aprovecha una vulnerabilidad para lograr sacar provecho para ataques o irrumpir un sistema informático.

Vulnerabilidades informáticas

Son fallos o debilidades de un sistema informático. Se trata de agujeros que puede ser producido por un error de configuración, o por una persona malintencionada para comprometer su seguridad.

Según (Panths, 2019), afirma que "En la actualidad estamos expuestos a sufrir ataques cada vez más sofisticados y frecuentes que ponen en peligro nuestro negocio, reputación, privacidad y confianza. Por eso, necesitamos ser cada vez más receptivos a las medidas de ciberseguridad y redefinir nuestra estrategia hacia la ciber-resiliencia.", Ningún sistema es completamente seguro ya que existe un alto crecimiento del espionaje informático y cada vez más personas alejadas a las buenas prácticas de la seguridad en los sistemas están en busca de brechas que permitan vulnerar los sistemas produciendo así la filtración de información sensible de la organización.

Magerit

El método MAGERIT, son las iniciales de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, este método abarca la fase AGR (Análisis y Gestión de Riesgos). Si lo describimos desde el punto de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el centro de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico. (welivesecurity, 2018)

En la actualidad tenemos una gran calidad en la tecnología, alta transferencia de datos en nuestras redes con una velocidad muy rápida. Pero el problema es la cantidad de usuarios que utiliza la red, al ser tantos es difícil tener una calidad óptima y nos encontramos con multitud de redes en el entorno en especial de la señal WIFI, esto es la que se denomina Saturación, la degradación del servicio por el número de usuarios accediendo de forma simultánea, solicitando algún servicio a la red. (Martín, M. et..all, 2014).

METODOLOGÍA

La técnica de investigación es aplicada en la mayoría de los casos para el análisis de gestión de riesgos dentro de los sistemas informáticos es la metodología MAGERIT. La misma que fue creada e implementada por el Consejo Superior de Administración Electrónica con el afán de reducir los riesgos en el manejo de información dentro de una organización con el afán de optimar el uso de los recursos tecnológicos, esta metodología tiene 5 fases:

- **Fase 1 Activos:** Establecer los activos relevantes para la organización.
- **Fase 2 Amenazas:** Determinar a qué amenazas están expuestos dichos activos.
- **Fase 3 Salvaguardas:** Fijar que salvaguardas hay dispuestas y cuan eficaces son frente al riesgo.
- **Fase 4 Impacto residual:** Evaluar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- **Fase 5 riesgo residual:** Valorar el riesgo definido como el impacto ponderado con la tasa de ocurrencia de la amenaza. (Molina-Miranda, 2017)

Adicionalmente, se encuesto a los socios de la Cooperativa que son en la actualidad 125, para tener una mayor exactitud se encuesto a todos. Donde se pudo obtener información verídica de la situación actual de la Cooperativa San Fernando.

RESULTADOS Y DISCUSIÓN

Se efectuó el escaneo de vulnerabilidades con la ayuda de la herramienta Nessus, es una de las más usada a nivel mundial en la realización de hacking ético y verificar vulnerabilidades en una aplicación web.

Fase 1. Activos

En la primera fase del desarrollo de la investigación se identificaron los activos relevancia en la Cooperativa de Taxi San Fernando de la ciudad de Babahoyo dentro de la organización los cuales forman parte del estudio de caso y se los especifican a continuación:

ACTIVOS	
Hardware	Instalaciones

Software	Personal administrativo
Datos	Socios

Tabla 2. Activos tecnológicos de la Cooperativa

Fuente: Los autores

Fase 2. Amenazas

En esta fase se determinan cuáles han sido las amenazas y vulnerabilidades que podrían poner en riesgo los activos tecnológicos de la cooperativa, para lograr esta identificación de amenazas se utilizó la herramienta Nessus que posee una interfaz fácil y sencilla en la búsqueda de brechas de seguridad dentro de sistemas informáticos.

Identificación de amenazas y vulnerabilidades

Realizado la respectiva configuración e instalación procedemos a realizar el escaneo con la herramienta Nessus por cada uno de los hosts listados. Se establece que el sistema informático evaluado muestra vulnerabilidades que permiten a un pirata informático recabar información que luego será usado como insumo para ataques mejor elaborados y el uso de comunicaciones sin cifrar o con cifrado débil nos podrían derivar en una fuga de datos al interrumpir o capturar la información emitida en los formularios.

Se realizó el escaneo del Sistema Informático de la Cooperativa de Taxi San Fernando el día jueves 17 de febrero, a las 14:50 pm y se pudo observar vulnerabilidades las mismas que se dividieron según lo detallado en la tabla 2. Este análisis se centrará en las más importantes y es detallado a continuación.

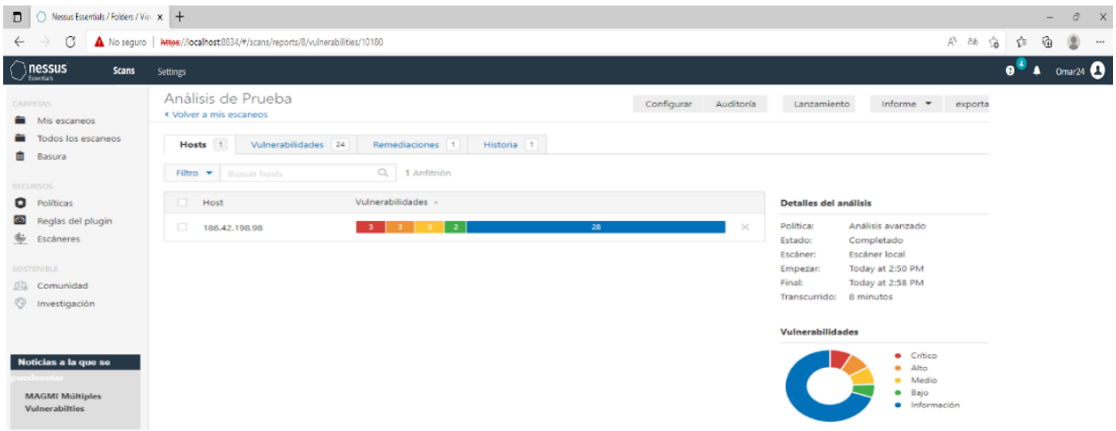

Ilustración 1. Vulnerabilidades en el Sistema Web

A continuación, se detalla una tabla del escaneo realizado usando Nessus, con lo cual podemos establecer el número de vulnerabilidades existentes en la Aplicación Web de la Cooperativa de Taxi San Fernando de la ciudad de Babahoyo.

ESCANEO USANDO NESSUS	
Vulnerabilidades encontradas:	11
Información adicional:	13
Total	24
Tipo de Análisis:	Análisis Avanzado
Tiempo de inicio:	14:50 Pm
Tiempo final:	14:58 Pm
Duración Total	8 minutos
Vulnerabilidades Criticas	3
Vulnerabilidades Altas	3
Vulnerabilidades Medias	3
Vulnerabilidades Bajas	2

Tabla 3. Resultado de escaneo con nessus

Fuente: Los autores

Detalle de las Vulnerabilidades encontradas

Detalle de Vulnerabilidades	
Fecha de Publicación:	25/06/2015
Fecha de Modificación:	17/02/2022
Nombre:	CVE-2015-2275 - CVE-2015-2416 - CVE-2015-3378 - CVE-
Importancia:	Critica
Recursos Afectados:	Apache HTTP Server, versiones 5.4 – 5.4.42

Detalle:	Un intruso remoto puede fructificar estas condiciones para ocasionar un desbordamiento de búfer, lo que nos lleva a tener una condición de denegación de servicios. Existe una vulnerabilidad de DDs en el componente SQL incluido ocasionada por el manejo erróneo en los nombres de cadena de intercalación. Vulnerabilidad de inyección de comandos arbitraria ocasionando una falla en la función php_escape_shell_arg() en exec.c.
Recomendación:	Actualizar PHP versión 5.4.42 o posterior.

Detalle de Vulnerabilidades	
Fecha de Publicación:	04/05/2012
Fecha de Modificación:	23/03/2022
Importancia:	Critica
Recursos Afectados:	Apache HTTP Server, versiones 5.4 – 5.4.42
Detalle:	De acuerdo a la versión, la instalación de PHP en el host remoto ya no es compatible. La no continuidad del soporte implica que ya no existirán nuevos parches de seguridad para el software.
Recomendación:	Actualizar a una versión de PHP que sea compatible actualmente.

Tabla 4. Vulnerabilidad Crítica

Fuente: Los autores

Fecha de Publicación:	11/08/2015
Fecha de Modificación:	17/02/2022
Nombre:	CVE-2015-6822 - CVE-2015-6812 - CVE-2015-6823 - CVE-2015-8364
Importancia:	Alta
Recursos Afectados:	Apache HTTP Server,
Detalle:	Apareció una vulnerabilidad de uso después de la liberación en ext./spl/spl_array.c debido al manejo incorrecto de un dato serializado especialmente diseñado. Existe una vulnerabilidad de recorrido de directorio en la clase Pardita, debido incorrecta implementación de la función extracto. Un intruso remoto no autenticado puede explotar esto a través de una entrada de archivo ZIP diseñada para escribir en archivos arbitrarios.
Recomendación:	Actualice a PHP versión 5.4.44 o posterior.

Tabla 5. Vulnerabilidad Crítica 2

Fuente: Los autores

Detalle de Vulnerabilidades	
Fecha de Publicación:	23/01/2003
Fecha de Modificación:	17/03/2022
Nombre:	CVE-2008-2119
Importancia:	Media
Recursos Afectados:	HTTP TRACE / TRACK Methods Allowed

Detalle:	Las funciones de depuración están habilitadas en el servidor web remote El servidor web remoto acepta los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que utilizados para depuración de conexiones de servidor web.
Recomendación:	Deshabilitar los métodos HTTP. Consultar la salida del plugin para mayor información.

Tabla 6. Vulnerabilidad Alta

Fuente: Los autores

Detalle de Vulnerabilidades	
Fecha de Publicación:	22/11/2013
Fecha de Modificación:	17/02/2022
Nombre:	SSH Débiles algoritmos MAC habilitados
Importancia:	Baja
Recursos Afectados:	SSH -MAC

Detalle:	El servidor SSH remoto se encuentra configurado para admitir algoritmos MD5 y MAC de 96 bits. El servidor SSH remoto se configura para consentir los algoritmos MD5 o MAC de 96 bits, los cuales se creen débiles

Tabla 7. Vulnerabilidad Media

Fuente: Los autores

Fase 3. Salvaguardas

Luego de haber reconocido las amenazas y vulnerabilidades dentro del sistema Web de la Cooperativa de taxi San Fernando se registra la información más relevante recopilados por el sistema. Se recalca la importancia de salvaguardar la información aminorando las amenazas con el propósito de atenuar los riesgos de la empresa.

Fase final. Impacto y riesgo residual

Los riesgos que se asemejan en el análisis pueden involucrar pérdida de información significativa que pueden colocar en peligro los activos y la infraestructura tecnológica de la cooperativa San Fernando los cuales se deben corregir para aminorar el impacto.

DISCUSIÓN DE RESULTADOS

Se pudo determinar 24 vulnerabilidades de las cuales la gran mayoría de errores estaban relacionadas con el lenguaje de programación del software (PHP) utilizado en la Cooperativa de taxi San Fernando de la ciudad de Babahoyo, el cual no solo poseía vulnerabilidades en la aplicación sino también en su base de datos.

Entre los principales problemas encontrados por la herramienta Nessus podemos darnos cuenta que una de sus vulnerabilidades estaba orientada a detección de versión PHP no

compatible, por cuanto se podría haber corregido con la actualización del lenguaje de programación a una versión de PHP que se soporte actualmente.

Se pudo establecer errores producidos por Denegación de servicio a Apache HTTP, SSL Versión Detección 2 y 3 del Protocolo, Apache HTTP Métodos HTTP TRACE / TRACK permitidos, Certificado SSL no es confiable, los cuales pudieron haber sido evitados o minimizado su riesgo de ataques, si hubiese existido un control o monitoreo de la aplicación web.

Una vez realizada la valoración de riesgos se alcanzan los siguientes resultados:

ÁREAS DE ANÁLISIS	DISTRIBUCIÓN DE DEFENSA DE RIESGOS	MADUREZ DE SEGURIDAD
Infraestructura	•	•
Aplicaciones	•	•
Operaciones y Personal	•	•

Tabla 9. Valoración de riesgos

Fuente: Los autores

Para el área de infraestructura, según Nessus muestran carencias inflexibles de seguridad. En la siguiente tabla se muestra un resumen de los problemas que se consideran más graves dentro de esta área:

Análisis general área infraestructura

Reglas y filtros de cortafuegos	No hay controles de acceso de nivel de red en el perímetro de la misma. Los cortafuegos son la primera línea de defensa, de ahí que resulten imprescindibles para proteger la red de los intrusos. No utiliza software de cortafuegos basados en hosts para proteger los

	servidores.
Acceso Remoto	Existen empleados y/o socios que se conectan remotamente a la red interna, pero no utiliza ninguna tecnología VPN para permitirles un acceso seguro.
Segmentación	La red presenta un sólo segmento.
Sistema de detección de intrusiones (IDS)	No se utiliza ningún hardware, ni software de detección de intrusiones.

Tabla 10. Resultados del análisis de infraestructura

Fuente: Los autores

Análisis general área aplicaciones

En el apartado referente al área de aplicaciones, se muestra la siguiente tabla de resultados:

Aplicación y recuperación de datos	En el sistema informático de la Cooperativa de taxi San Fernando no realizan periódicamente pruebas de recuperación de aplicaciones y datos.
Fabricantes de software independientes (ISV)	En la cooperativa se utilizan aplicaciones que han sido desarrolladas por terceros. Las personas dueñas de software no ofrecen servicios de mantenimiento ni actualizaciones de seguridad.
Desarrollado internamente	Dentro de la Cooperativa no se usan macros personalizadas en aplicaciones ofimáticas.

Vulnerabilidades	No existen procedimientos ni manual de usuarios que aborden los aspectos de las amenazas y vulnerabilidades de la información.

Tabla N°11. Resultado del análisis de aplicaciones

Fuente: Los autores

Al realizar el análisis de la aplicación de las encuestas a los socios de la Cooperativa San Fernando, tenemos los siguientes resultados.

Pregunta 1:

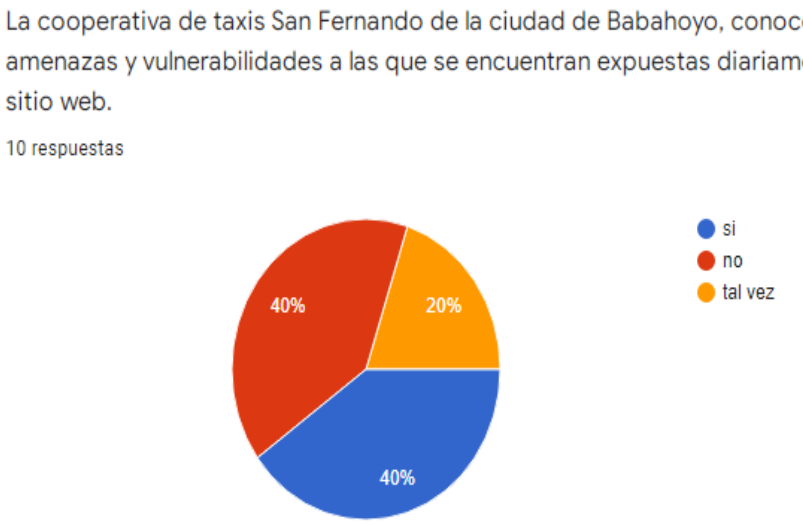

Ilustración 2. Amenazas y Vunerabilidades del Sitio We

Análisis:

De los socios encuestados arroja un 40% indicando que se tiene un amplio conocimiento del tema, mientras que hay otro 40% indicando que no lo hay, finalmente terminamos con un 20% indicando un tal vez.

Interpretación:

Se recomienda concientizar del problema porque se puede observar un 60% de los encuestados, no tienen el conocimiento amplio sobre el tema.

Pregunta 2:

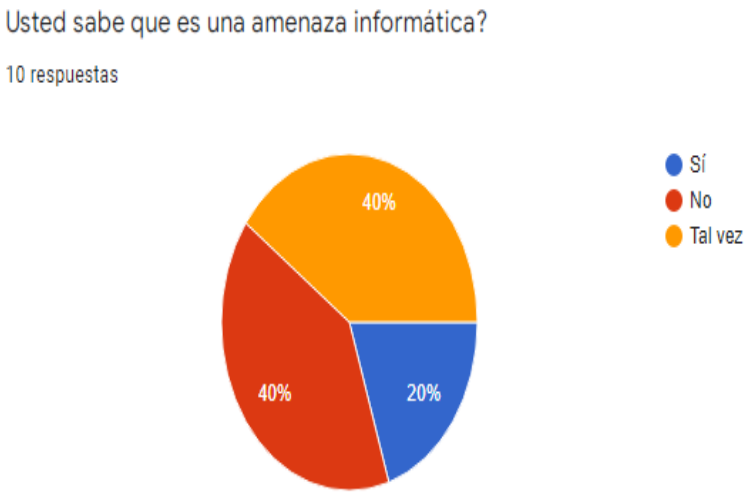

Ilustración 3. Sabe que es una amenaza informática

Análisis:

De los socios encuestados un 20% nos indica que se tiene un amplio conocimiento del tema, mientras que el otro 40% indica que no, finalizando con otro 40% dando como resultado un talvez.

Interpretación:

Existe un 80% de los encuestados que no tienen el conocimiento sobre que es una amenaza informática.

Pregunta 3:

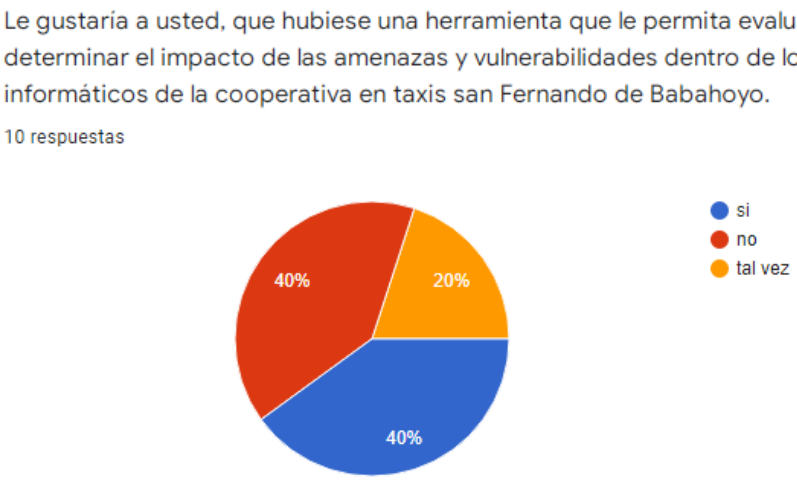

Ilustración 4. Herramienta para evaluar y determinar el impacto

Análisis:

De los socios encuestados un 40% indica que se tiene claro el tema mientas que un 40% indica que no, finalizando con el 20% indicando que el tema no está del todo claro.

Interpretación:

Existe un 60% que indica que se debe trabajar en la concientización de usar una herramienta que permita evaluar y determinar el impacto de amenazas y vulnerabilidades dentro de los sistemas informáticos.

CONCLUSIONES

Los ataques informáticos tanto a equipos como sistemas de información son inevitables. Se observó algunos errores a nivel de seguridad informática, al no contar con políticas de seguridad apropiadas para proteger la integridad de los datos. Las vulnerabilidades encontradas fueron 11 establecidas de la siguiente manera: 3 criticas, 3 altas, 3 medias y 2 de tipo bajas y además se hallaron 13 de información adicional que son consideradas superficiales y que no afectarían la integridad de los datos.

Al realizar el análisis en la Cooperativa de taxis San Fernando de la ciudad de Babahoyo se pudo evidenciar que existen vulnerabilidades, debido a la falta de controles de acceso de nivel de red, además existen empleados y/o socios que se conectan remotamente a la red interna, así como también las personas dueñas del software no ofrecen servicios de mantenimiento ni actualizaciones de seguridad.

Es necesario efectuar una constante actualización y búsqueda de las mejores aplicaciones y herramientas que se encuentren en el mercado tecnológico para la detección de vulnerabilidades y amenazas a las que se exponen los sistemas web. Entre la detección realizada se pudo determinar vulnerabilidades y amenazas referentes a DDs a Apache, SSL Versión Detección 2 y 3 del Protocolo, Apache HTTP Métodos HTTP TRACE / TRACK permitidos, Certificado SSL no confiables.

Contar con un plan de mejoras que permita obtener un mejor enfoque de los problemas que pueda sucederse al momento de la ejecución de una amenaza, ya que con el uso del mismo se puede mitigar los riesgos existentes, además es de ayuda en la toma decisiones para el rápido restitución de los servicios.

REFERENCIAS BIBLIOGRÁFICAS

Advisors., G. (2019). Nessus Escáner de Vulnerabilidad.

Cano, J. J. (2018). Ciberseguridad y ciberdefensa.

Gutiérrez, Á. P. (2019). Python paso a paso . RA-MA S.A. Editorial y Publicaciones.

Hernández, F. &. (2014). Metodología de la Investigación.

Luan, U. N. (2019). Amenazas a la Seguridad de la Información.

Martha Irene Romero Castro, G. L. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. 3Ciencias.

NEOSOFT. (s.f.). NEOSOFT. Obtenido de NEOSOFT.: https://www.neosoft.es/blog/que-es-una-aplicacion-web/

Obando. (2019). INTRODUCCIÓN A LA SEGURIDAD INFORMATICA.

Panths, E. (2019). Redefiniendo la seguridad hacia la ciber-resilencia. Unidad Global de ciberseguridad del grupo telefónica Eleven Panths.

REVIVERSOFT. (2018). REVIVERSOFT. Obtenido de REVIVERSOFT.

Ricardo., M. (2018). Lenguajes de programación:.

Romero, M. F. (2018). Seguridad Informática.

Santos, J. C. (2018). Seguridad Infromática. Grupo Editorial RA-MA.

Velthuis, P. M. (2018). Calidad de sistemas.

welivesecurity. (2018). welivesecurity. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/