UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2021 – ABRIL 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANALISIS DE AMENAZAS Y VULNERABILIDADES DE LA GESTION DE PROCESOS DEL SISTEMA INFORMÁTICO EN LA COOPERATIVA DE TAXI SAN FERNANDO DE BABAHOYO

ESTUDIANTE:

JASUME NAYELI CRESPO OROZCO

TUTOR:

FABIAN EDUARDO ALCOCER CANTUÑA

AÑO 202

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, 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 es cual se refiere a la metodología MAGERIT.

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

PLANTEAMIENTO DEL PROBLEMA

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 sinnúmero de recursos para poder neutralizar los ataques a los cuales se encuentran expuestos.

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. Para poder establecer el objetivo del caso de estudio, se va a utilizar el método cuantitativo por cuanto la información fue obtenida a través de encuestas y

adicionalmente se utilizó la técnica de investigación relacionada en el análisis de gestión de riesgos aplicados a los sistemas Web la cual es la metodología MAGERIT.

La identificación de vulnerabilidades en las aplicaciones web, busca identificar los riesgos más críticos que puede enfrentar la organización, basándose en la metodología MAGERIT, para analizar, identificar y evaluar los riesgos que se enfrenta una aplicación web y 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.

¿cómo el análisis de amenazas y vulnerabilidades a la gestión de procesos del sistema informático en la cooperativa de taxi San Fernando de Babahoyo, permitirá mermar el impacto y la probabilidad de ocurrencia de las amenazas a que se expuesto el sistema para proponer acciones de mejoramiento de la seguridad en la Cooperativa de taxi San Fernando de Babahoyo?

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 mantenimiento 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 dificulta en el acceso a la información, riesgo de robo o corrupción de datos personales, Interceptación de datos confidenciales, entre otros.

JUSTIFICACION

Los sistemas de información son un notable aporte para realizar acciones de automatización en distintas ramas, localizar los mecanismos ideales para desarrollarlos ha sido una alternativa que permite a las personas poder mejorar en diferentes aspectos del diario vivir. El uso adecuado de la tecnología en las últimas épocas ha ayudado que las PYMES puedan tener la posibilidad de llevar su información de manera correcta y eficaz.

En los tiempos actuales, las empresas sean estas públicas o privadas se encuentran enmarcadas dentro de los sistemas informáticos, los cual conlleva alcanzar una eficiente administración de los datos y gestión de procesos, gran parte de ellos se encuentran vinculados a la red, lo que ocasiona que sean vulnerables a gran cantidad de amenazas informáticas originadas por la mala utilización de los recursos, las cuales nos afectaría y ocasionaría la triada CID de la información 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. El presente caso de estudio **ANALISIS DE AMENAZAS Y VULNERABILIDADES DE LA GESTION DE PROCESOS DEL SISTEMA INFORMÁTICO EN LA COOPERATIVA DE TAXI SAN FERNANDO DE BABAHOYO** se encuentra orientado a la línea de investigación sistemas de información y comunicación, emprendimiento e innovación, sostenida por la sublíneas de investigación de redes y tecnologías inteligentes de software y hardware.

En la organización objeto de análisis, existen inconvenientes relacionados con las **AMENAZAS Y VULNERABILIDADES DE LA GESTION DE PROCESOS DEL SISTEMA INFORMÁTICO EN LA COOPERATIVA**, debido a que 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.

OBJETIVOS

Objetivo general.

- Analizar las amenazas y vulnerabilidades de la gestión de procesos del sistema informático en la cooperativa de taxi San Fernando de Babahoyo

Objetivo Específico

1. Identificar los factores de amenaza y las vulnerabilidades de seguridad que se presentan en el sitio Web, para identificar la causa o el origen de las mismas.
2. Determinar los tipos de vulnerabilidades y/o amenazas, en activos definidos por la organización.
3. Evidenciar los hallazgos mediante los informes ejecutivos, técnicos, y matriz de vulnerabilidades.

LÍNEAS DE INVESTIGACIÒN

Esta indagación está enfocada en la línea de investigación sistemas de información y comunicación, emprendimiento e innovación, sostenida por la sublíneas de investigación de redes y tecnologías inteligentes de software y hardware. Se determinó incorporar la investigación cualitativa, teniendo en cuenta el método investigativo deductivo, mismo que permitió la obtención de información actualizada y de esta manera llegar a los dilemas que afectan a la Cooperativa de taxi San Fernando de Babahoyo, mediante la técnica de encuestas y entrevistas, se obtuvo datos importantes para el logro de este proyecto caso de estudio.

MARCO CONCEPTUAL

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	
Socios	Cargos
1	Presidencia
1	Gerencia
1	Secretaria
3	Comité de Vigilancia
119	Socios

Tabla 1Nomina y Cargos del Personal de la Cooperativa San Fernando

Fuente: La Autora

El sistema de gestión de procesos de la Cooperativa de taxi San Fernando de la ciudad de Babahoyo permite a cada uno de los socios poseer un perfil, a través del cual se sistematiza 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) asevera que “Nessus pertenece al estándar mundial, relacionada a la prevención de ataques informáticos, establecimiento de vulnerabilidades y localización de inconvenientes de configuración que son usados por intrusos informáticos. Nessus es una aplicación que ha sido 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 organizaciones a menudo se encuentran amenazadas con la destrucción o alteración de la información existentes en los sistemas informáticos, estos daños pueden incitar a la perdida de datos (información de socios, contables, financieros). Las amenazas son de mayor riesgo cuando en aplicación Web poseen agujeros de seguridad los cuales se denominan vulnerabilidades que ocasionan un enorme daño a las organizaciones.

Actualmente la sociedad se ha convertido en un consumidor tecnológico por la gran demanda de software ya sean estas 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 utilización de técnicas para la defensa de la información, el auge de los recursos tecnológicos; antivirus, firewalls, detección de intrusos, detección de anomalías, que relacionados con reglas definidas por el gobierno, las tecnologías de la información determinan la forma en que se actúa y asegura los escenarios de posibles fallas. (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), establece que "actualmente nos encontramos expuestos a soportar ataques informáticos, que colocan en situación peligrosa a las organizaciones. Por lo cual, debemos ser más receptivos a las políticas de seguridad informática y redelimitar la estrategia hacia la ciber-resiliencia."

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)

MARCO METODOLÓGICO

La técnica de investigación es aplicada en la mayoría de los casos, el análisis de gestión de riesgos en los Sistemas Web es la llamada 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 los recursos tecnológicos, la metodología está compuesta por 5 etapas:

- **Etapa 1**

  Toma el nombre de Etapa de revisión de activos, que permite establecer los activos selectos para la organización.

- **Etapa 2**

  Se encuentra relacionada a las amenazas, las cuales determina a qué amenazas sen encuentran expuestos dichos activos.

- **Etapa 3**

  Llamada Etapa de Salvaguardas, sirve para fijar las salvaguardas existentes y cuan eficientes son al riesgo.

- **Etapa 4**

  El impacto residual permite Valorar el impacto, definido como el daño sobre el activo de la amenaza.

- **Etapa 5**

  El riesgo residual, establece el valor el riesgo y el impacto ponderado con la tasa de ocurrencia de la amenaza. (Molina-Miranda, 2017)

RESULTADOS

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.

Etapa 1. Activos

En este primer análisis se establecieron cuales son los activos más relevantes en la Cooperativa de Taxi San Fernando de la ciudad de Babahoyo, las cuales se definen a continuación:

Activos	
Hardware	Instalaciones
Software	Personal administrativo
Datos	Socios

Tabla 2 Activos Tecnológicos de la Cooperativa de taxi San Fernando

Fuente: La Autora

Etapa 2. Amenazas

En esta etapa 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 en la Ilustración 2. 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.

Ilustración 1 Análisis de vulnerabilidades con la herramienta Nessus

Fuente: La Autora

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.

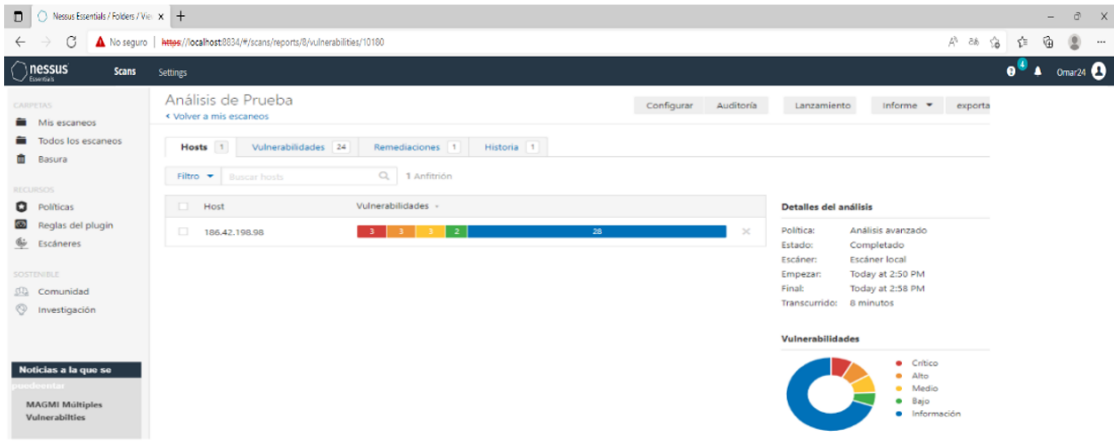


Ilustración 2 Vulnerabilidades en el Sistema Web
Fuente: La Autora

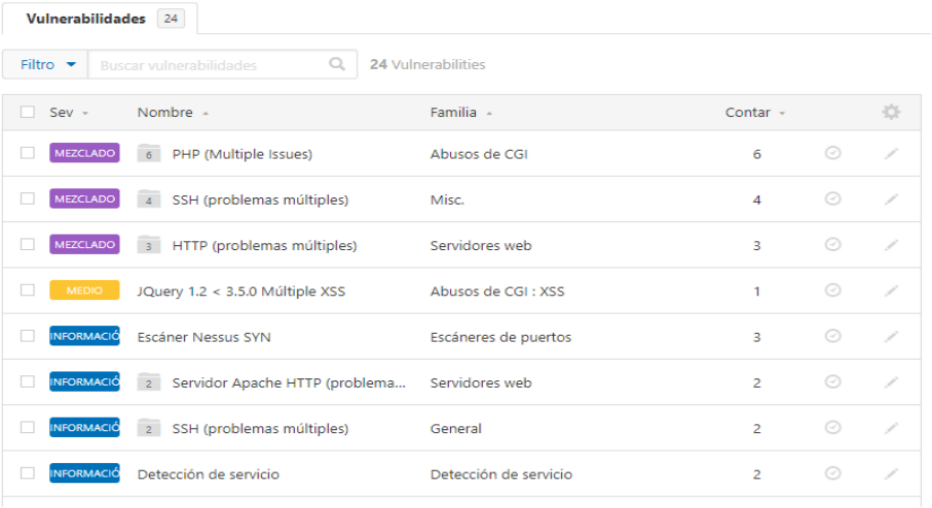


Ilustración 3 Vulnerabilidades encontradas

Fuente: La Autora

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 empleando Nessus	
Vulnerabilidades encontradas:	11
Información extra:	13
Total de vulnerabilidades	24
Tipo de Análisis:	Avanzado
Duración inicial:	14:50 Pm
Duración final:	14:58 Pm
Duración Total	9 mts
Vulnerabilidades	
Criticas	3
Altas	3
Medias	3
Bajas	2

Tabla 3 Resultado de Escaneo con Nessus

Fuente: La Autora

Detalle de las Vulnerabilidades encontradas

Detalle de Vulnerabilidades	
Fecha de Publicación:	**25/06/2015**
Fecha de Modificación:	**17/02/2022**
Nivel:	**Critica**
Recursos Comprometidos:	**Apache HTTP Server, versiones 5.4 – 5.4.42**
Detalle:	Un atacante de forma remota podría aprovechar estas oportunidades para producir un desbordamiento de búfer, lo cual produciría una condición de denegación de servicios. Se estableció una vulnerabilidad de DDs en el componente SQL incluido originada en manejos erróneos de los nombres de cadena de intercalación. Se determino la vulnerabilidad de inyección de comandos arbitraria produciendo una error en la función php_escape_shell_arg() en exec.c.
Recomendación:	**Actualización de la versión 5.4.42 o posterior del software**

Tabla 4 Vulnerabilidad Crítica
Fuente: La Autora

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:	El análisis de 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. Se pudo determinar, que es posible que existan vulnerabilidades de seguridad.
Recomendación:	Actualizar a una versión de PHP que sea compatible actualmente.

Tabla 5 Vulnerabilidad Crítica 2

Fuente: La Autora

Detalle de Vulnerabilidades	
Fecha de Publicación:	11/08/2015
Fecha de Modificación:	17/02/2022
Importancia:	Alta
Recursos Afectados:	Apache HTTP Server, versiones 5.4
Detalle:	Surgió una vulnerabilidad en el uso posteriormente de la liberación en ext./spl/spl_array.c por el manejo incorrecto de un dato serializado. Se determino una vulnerabilidad en el recorrido de directorio de la clase Pardita, por la incorrecta ejecución de la función extracto. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad a través de una entrada de archivo ZIP diseñada para escribir en archivos arbitrarios.
Recomendación:	Actualizar a una versión de PHP que sea compatible

Tabla 6 Vulnerabilidad Alta

Fuente: La Autora

Detalle de Vulnerabilidades	
Fecha de Publicación:	23/01/2003
Fecha de Modificación:	17/03/2022
Importancia:	Media
Recursos Afectados:	HTTP TRACE / TRACK Methods Allowed
Detalle:	Las funciones de depuración se encuentran activadas en el servidor web remote. El servidor web remoto acepta los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP los cuales son usados en la depuración de conexiones de servidor web.
Recomendación:	Deshabilitar los métodos HTTP. Determinar la salida del plugin para obtener una mejor información.

Tabla 7 Vulnerabilidad Media

Fuente: La Autora

Detalle de Vulnerabilidad Baja

Detalle de Vulnerabilidades	
Fecha de Publicación:	22/11/2013
Fecha de Modificación:	17/02/2022
Nombre:	SSH Débiles algoritmos MAC habilitados
Importancia:	Bajo
Recursos Afectados:	SSH -MAC
Detalle:	El servidor SSH remoto está configurado para permitir algoritmos MD5 y MAC de 96 bits.

Tabla 8 Vulnerabilidad Baja

Fuente: La Autora

Etapa 3. Salvaguardas

Determinadas las vulnerabilidades dentro del sistema Web de la Cooperativa de taxi San Fernando se registra la información más relevante en el sistema. Se estableció la importancia de esta etapa reduciendo las amenazas minimizando los riesgos de la cooperativa.

Etapa 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: La Autora

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: La Autora

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 usanmacros 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 11Resultados del Análisis de Aplicaciones.

Fuente: La Autora

CONCLUSIONES

- Los ataques informáticos tanto a equipos como sistemas de información son inevitables. En este estudio de caso 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.

- Con el desarrollo de este estudio de caso 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

RECOMENDACIONES

- Implementar, controlar y monitorear las actividades realizadas en el sistema informático, con el afán de eliminar las amenazas y vulnerabilidades encontradas (DDs a Apache, SSL Versión Detección 2 y 3 del Protocolo, Apache HTTP Métodos HTTP TRACE / TRACK permitidos, Certificado SSL no confiables) y a su vez reducir disminuir el rango de los riesgos a futuro.

- Implementar metodologías de hacking éticos en varios escenarios, esto ayudará a conocer aún más las brechas de seguridad informáticas que pueden comprometer la integridad de la información.

- Establecer capacitaciones técnicas e informativas para el personal de la organización, en temas referentes a la seguridad de la información. Esto permitirá concientizar al personal sobre la importancia del buen uso a los recursos informáticos que posee la cooperativa de taxi San Fernando.

- Inspeccionar habitualmente las políticas y procedimientos, por cuanto la tecnología tiene avances vertiginosos y por tal motivo surgen riesgos que deben ser minimizados para evitar problemas más adelante. Lo que significa una capacitación constante al equipo o al técnico informático de la cooperativa de taxi San Fernando.

REFERENCIAS

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/

ANEXOS

ANEXO 1

UNIVERSIDAD TECNICA DE BABAHOYO

FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA

CUESTIONARIO

INTRUCIONES

SELECCIÓNE LA OPCION QUE USTED CONSIDERE CONVENIENTE.

1. La cooperativa de taxis San Fernando de la ciudad de Babahoyo, conoce las amenazas y vulnerabilidades a las que se encuentran expuestas diariamente en su sitio web.

   Si () no () tal vez ()

2. ¿Usted sabe que es una amenaza informática?

   Si () no () tal vez ()

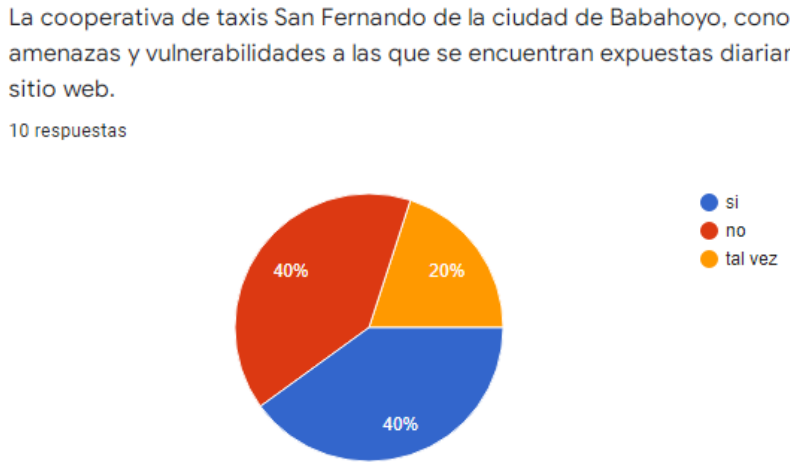
3. Le gustaría a usted, que hubiese una herramienta que le permita evaluar y determinar el impacto de las amenazas y vulnerabilidades dentro de los sistemas informáticos de la cooperativa en taxis san Fernando de Babahoyo.

   Si () no () tal vez ()

ANEXO 2

Tabulación de la información de las encuestas

PREGUNTA 1



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.

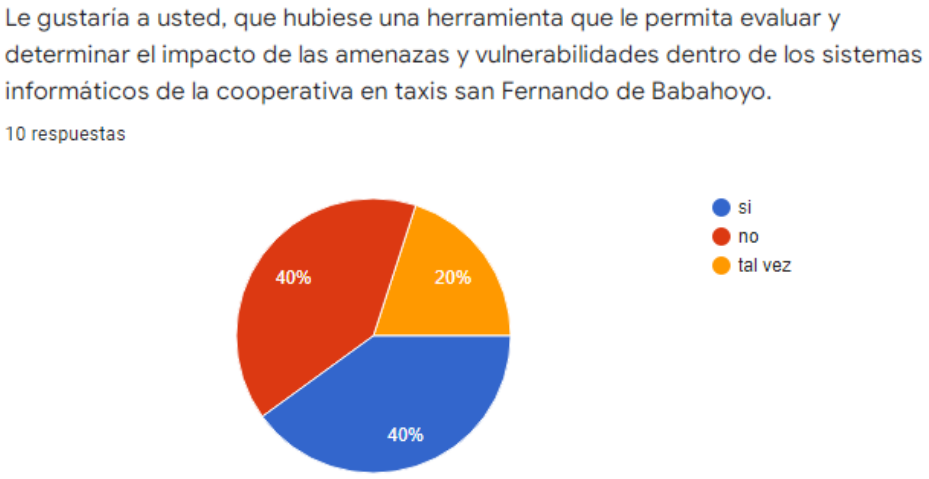
Interpretación: Se recomienda concientizar del problema porque se puede observar un 60% de los encuestados, no tienen el conocimiento amplio sobre el tema.

PREGUNTA 2

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



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 conciencialización de usar una herramienta que permita evaluar y determinar el impacto de amenazas y vulnerabilidades dentro de los sistemas informáticos.

ANEXO 3

Figura 1.

entrevista con la secretaria de la cooperativa en taxis san Fernando de Babahoyo.

Figura 2.

entrevista con el gerente de la cooperativa en taxis san Fernando de Babahoyo.

ANEXO 4

PERMISO RESPECTIVO PARA EL DESARROLLO DEL TRABAJO DE TITULACIÓN MODALIDAD ESTUDIO DE CASO

COOPERATIVA EN TAXIS
"SAN FERNANDO DE BABAHOYO"
RUC: 1290010760001
Fundada el 22 de noviembre de 1990
Mediante Acuerdo Ministerial No 2983
DIRECCION: CDLA. LUZ MARINA 1ª LONGITUDINAL
Telefono: 052023940
Email. coopsanfernandob@yahoo.es

Babahoyo, 18 de marzo del 2022

Sr.

Lcdo. Eduardo Galeas Guijarro, MAE.

DECANO DE LA FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA

En su despacho. –

Reciba un cordial saludo de parte del **LCDO.PEDRO MANUEL BAZAN CASTRO,** portador de la cedula de ciudadanía **No. 120190827-2;** representante legal de la **COOPERATIVA DE TRANSPORTE EN TAXIS "SAN FERNANDO DE BABAHOYO",** el motivo de la presente es para informarle que se le fue otorgado el permiso correspondiente para realizar su caso de estudio con el tema **ANÁLISIS DE AMANEZAS Y VULNERABILIDADES DE LA GESTIÓN DE PROCESOS DEL SISTEMA INFORMÁTICO DE LA COOPERATIVA EN TAXI SAN FERNANDO DE BABAHOYO.** a la señorita **JASUME NAYELI CRESPO OROZCO** con cédula de identidad No. **1207583129,** estudiante de la carrera de Ingeniería en Sistemas de Información, matriculado en el proceso de titulación en el periodo noviembre 2021- abril 2022 para la obtención de su grado académico profesional universitario de tercer nivel como **INGENIERA EN SISTEMAS DE INFORMACION.**

Unidad, Trabajo y Superación
Atentamente

Lcdo. Pedro Bazán Castro
Gerente-Coop.