UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN:

MAYO – SEPTIEMBRE 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:

PLAN DE GESTIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN PARA EL MANEJO DE VULNERABILIDADES DE LOS SISTEMAS DE LA UTB, TOMANDO LOS REQUISITOS DESCRITOS EN LA NORMA ISO 27005

ESTUDIANTE:

JAMES WALTHER BRAVO BUSTAMANTE

TUTOR:

ERICK MAGNO RICAURTE ZAMBRANO

2022

RESUMEN

A lo largo del tiempo los sistemas informáticos han sido vulnerados, permitiendo que elementos y/o personal no autorizado obtenga acceso a información que debería ser confidencial, causando una serie de inconvenientes en las organizaciones e instituciones del país. Actualmente, la seguridad de los sistemas de un aspecto de vital importancia, por lo que constantemente se destina una gran cantidad de recursos para poder neutralizar los posibles ataques y amenazas a las cuales se encuentran expuestos.

El problema de la Universidad Técnica de Babahoyo (UTB), radica en que no determinadas las amenazas y vulnerabilidades a las que se encuentran expuestas sus sistemas informáticos, por lo que usuarios no autorizados podrían acceder a dicha información y por lo tanto visualizarla, modificarla e incluso robar información sensible y confidencial para la institución. Arriesgando así la triada CID (Confidencialidad, Integridad, Disponibilidad) de la información al no realizar un análisis frecuente de los sistemas para determinar problemas de seguridad y poder tratarlos de manera adecuada y a tiempo antes de que produzcan un daño mayor.

Basado en este hecho se delimitó el caso de estudio que permitió estudiar los sistemas informáticos y poder analizar las falencias de seguridad que estos presentan, al igual que poder realizar un diagnóstico sobre su estado actual de los mismos y poder valorar sus mecanismos de ciberseguridad. Cabe recalcar que el presente trabajo fue realizado en base a las técnicas de investigación de campo y deductivo, al igual la técnica de investigación relacionada al análisis de gestión de riesgos presentes en los sistemas informáticos, el cual se refiere a la norma ISO 27005.

Palabras claves: Amenaza, vulnerabilidad, información, riesgo, gestión.

ÍNDICE

PLANTEAMIENTO DEL PROBLEMA

Un análisis de riesgos se refiere al estudio de las vulnerabilidades y amenazas que pueden existir en un sistema informático, además de los posibles daños que estos pudieran causar.

Vulnerabilidades que se han podido identificar en los sistemas de la Universidad Técnica de Babahoyo (UTB) mediante el uso de diversas herramientas tecnológicas, como el sistema operativo Kali Linux, famoso por ser uno de los mejores y más completos entornos con decenas de herramientas para la realización de hacking ético y/o pentesting para comprobar su nivel la seguridad y vulnerabilidades de un sistema. Como Nmap, herramienta que nos permite comprobar los puertos que se encuentran abierto en una página y a veces mostrar a que servicio está conectado ese puerto; o Jack The Ripper, un famoso crackeador de contraseñas.

Entre las vulnerabilidades que se han encontrado, hay algunas que realmente ponen en total peligro sus datos e información, por ejemplo, mediante el uso de la herramienta Nmap de Kali Linux para el mapeo de los puertos, se detectó que el Sistema Académico Integral (SAI), en ocasiones suele tener abierto el puerto 3306 correspondiente a la base de datos; creando la posibilidad de que se pueda realizar un ataque de inyección SQL que consiste en la creación de scripts o líneas de código SQL que al momento de ser ejecutados o enviados, generalmente en un formulario, confunda al sistema y pueda retornar información directamente desde la base de datos o realizar cambios en la misma.

La raíz del problema radica en que la Universidad Técnica de Babahoyo no es consciente ni tiene determinada las amenazas y vulnerabilidades a las que se encuentran

expuestas, poniendo en riesgo la triada CID (Confidencialidad, Integridad y Disponibilidad) de la información que utilizan.

La información que manejan corre el riesgo de perder su confidencialidad y que por lo tanto pueda ser filtrada, alterada, corrompida o incluso sufrir de robos o secuestro de información, entre otros.

La seguridad es un aspecto primordial para el ser humano, en todo momento debe ser tomada muy enserio, así como (Uriona, 2002) describe que "La seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella"

Los avances tecnológicos que vivimos constantemente y su evolución, han convertido a los sistemas de información y las telecomunicaciones en una herramienta fundamental para la realización de diversas actividades, pero esta misma evolución y crecimiento de la tecnología se ha encargado de brindarnos vulnerabilidades de las mismas, poniendo en riesgo los datos e información que constantemente estamos generando y manipulando.

Durante los últimos años las vulnerabilidades en los sistemas han permitido que elementos no autorizados consigan acceso a la información confidencial, lo cual conlleva una serie de problemas para cualquier organización y/o institución que los presente. Actualmente, la seguridad de la información es de vital importancia, por lo que se debería invertir y prestar toda la atención necesaria para prevenir y/o neutralizar cualquier tipo de ataque ante el cual se encuentren expuestos.

JUSTIFICACIÓN

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.

Actualmente el impedir la ejecución de operaciones no autorizadas sobre un sistema informático, sin importar la naturaleza de este, se lo considera como un proceso de vital importancia, puesto que los efectos que dañinos que estos podrían ocasionar sobre los datos, su integridad y confidencialidad son muy altos, y deberían ser tratados de la manera más meticulosa posible.

Una planificación acorde a los estándares de ciberseguridad referente a la información que se maneja en la institución es necesaria para ayudar a prevenir el crecimiento de amenazas y vulnerabilidades ya presentes en un sistema informático.

La norma ISO 27005 ofrece un estándar de calidad en respecto al tratamiento de la seguridad de información, también conocidos como “Sistema de Gestión de Seguridad de la Información”, la cual establece una serie de lineamientos a seguir en cuanto a la seguridad de la información, así como acciones oportunas a tomar en caso un incidente, además, brindar un plan adecuado para el tratamiento de los riesgos que corre la información y dar soluciones a los posibles incidentes.

OBJETIVOS

OBJETIVO GENERAL

Elaborar un plan que permita gestionar de manera correcta el riesgo en la seguridad de la información basado en la normativa ISO 27005 ante una posible explotación de vulnerabilidades de seguridad

OBJETIVOS ESPECÍFICOS

1. Identificar los requisitos de la ISO 27005 adecuados para el caso de estudio
2. Analizar vulnerabilidades de seguridad identificadas en los sistemas informáticos de la Universidad Técnica de Babahoyo
3. Especificar las vulnerabilidades encontradas y el riesgo que representan

LÍNEA DE INVESTIGACIÓN

El caso de estudio se centra en la línea de investigación sistemas de información y comunicación, emprendimiento e innovación, la misma que se encuentra respaldada por la sublínea de investigación de redes y tecnologías inteligentes de software y hardware. También se determinó incorporar el método de investigación cualitativo, considerando a su vez el método deductivo, el cual permitió obtener información actualizada y así determinar cuáles son las situaciones que afectan la UTB; mediante la aplicación de encuestas y entrevistas se pudo obtener más de datos para el desarrollo del caso de estudio.

MARCO CONCEPTUAL

SISTEMAS DE INFORMACIÓN

(Chen, 2019) define al sistema de información como: Un conjunto de datos que interactúan entre sí con un fin común.

En informática, los sistemas de información ayudan a administrar, recopilar, recuperar, procesar, almacenar y difundir información relacionada con los procesos básicos y únicos de cada organización.

Con el advenimiento de las tecnologías de la información y la comunicación TIC, las organizaciones son capaces de generar datos relevantes y relevantes para decisiones estratégicas basadas en evidencia bajo el mapeo de procesos de negocios que están lógicamente coordinados y entendidos como un conjunto de actividades vinculadas. Vi la oportunidad de implementar un sistema de información que permitiera la consulta y el acceso a. Desarrollado por la organización para lograr resultados comerciales oportunos y concretos.

Primero, es necesario aclarar que el término sistema se refiere a "un conjunto de componentes que interactúan para lograr un objetivo común". Hay muchos tipos diferentes de sistemas, la mayoría de los cuales pueden representarse mediante un modelo que consta de cinco bloques básicos: elementos de entrada, elementos de salida, secciones de transformación, mecanismos de control y objetivos.

Figura 1 *Estructura de un Sistema de Información* ***Fuente:*** *Autor*

- **Entrada:** Corresponde a la recolección o registro de datos internos y externos registrados en el sistema de información.
- **Transformar:** La entrada se manipula, analiza y procesa para que el usuario del sistema la entienda.
- **Salida:** Consiste en distribuir información procesada a usuarios que la utilizan en momentos específicos de un determinado proceso o actividad.

COMPONENTES DE LOS SISTEMAS DE INFORMACIÓN

Las entradas del sistema son datos, y cada dato se considera un conjunto de hechos que representan eventos que han ocurrido en su organización o entorno. Sin embargo, se separan sin ordenar ni organizar. Por lo tanto, los humanos no pueden entender que se usan de manera efectiva.

El hardware requerido para el funcionamiento de un sistema de información basado en él puede almacenar, procesar y distribuir a los usuarios la información que una organización quiere incluir en el sistema.

El software, comúnmente conocido como programas informáticos, es un conjunto de instrucciones lógicas que dirigen y controlan el procesamiento de tareas específicas que permiten a SI comprender el problema para el que está diseñado.

INFORMACIÓN

(Velthuis, Rubio, & Muñoz-Reja, 2006) definen a la información como: El activo más valioso de las organizaciones y es por eso que debe ser protegida de una manera adecuada, sin importar la manera en la que se encuentre, ya sea física o digital, porque sin importar como se encuentre la información o el medio por el cual sea almacenada y/o transmitidas, siempre debe estar protegida de manera adecuada.

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)

(Luan, 2019) señala que 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, También puede incluir otras cualidades como confiabilidad, responsabilidad, confiabilidad y no repudio.

Objetivos de la seguridad informática:

- Minimizar y administrar el riesgo e identificar posibles problemas y amenazas de seguridad.
- Garantizar el uso adecuado de los recursos del sistema y las aplicaciones.
- Limitar las pérdidas y asegurar la recuperación adecuada del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y los requisitos establecidos por el cliente en el contrato.

Para lograr los objetivos mencionados se debe contemplar los siguientes 4 planos de atención:

Plano humano:

- Concienciación y educación
- Funciones, obligaciones y responsabilidades de los empleados
- Gestión y seguimiento de empleados

Plano técnico:

- Selección, instalación, configuración y actualizaciones de soluciones de hardware y software
- Criptografía
- Estandarización de productos
- Desarrollo seguro de aplicaciones

Plano Organizacional:

- Políticas, reglas y procedimientos
- Plan de respuesta a emergencias y respuesta a incidentes
- Relaciones con terceros (clientes, proveedores)

Plano Legislativo:

- Cumplimiento y adaptación a la legalidad vigente

SEGURIDAD DE LA INFORMACIÓN

Se puede definir como un conjunto de medidas que ayudan a proteger y resguardar la información, mismas medidas que pueden ser preventivas o reactivas, es decir, se pueden aplicar antes, durante o después de que se dé un hecho que afecte los sistemas

tecnológicos de una organización y que atente contra la triada CID de la información (Confidencialidad, Integridad y Disponibilidad).

Según el tipo de información manejada y los procesos que requiere su organización, en la seguridad de la información puede ser más importante que garantizar la confidencialidad, integridad o disponibilidad de sus activos de información.

Figura 2 *Triada CID* ***Fuente:*** *Norma ISO/IEC 17799*

OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

- Seguir las normas, leyes y requisitos contractuales de la empresa relacionados con el manejo seguro de la información.
- Asegurarse de que sus empleados estén capacitados en seguridad de la información.
- Regularmente identificamos riesgos relacionados con la seguridad de la información y tomamos medidas de protección.
- Manejar adecuadamente los incidentes de seguridad y asegurar la confidencialidad, integridad y disponibilidad de la información.
- Monitorear y mejorar continuamente las regulaciones y los controles internos que permiten controles de seguridad mejorados.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Un evento único o una serie de eventos de seguridad de la información no deseados o inesperados que ponen en peligro las operaciones comerciales y es muy probable que pongan en peligro la seguridad de la información. (ISO/IEC, 2005)

EVENTO DE SEGURIDAD DE LA INFORMACIÓN

Una ocurrencia identificada de una condición de sistema, servicio o red que indica una situación previamente desconocida que puede ser una violación de una política de seguridad de la información o una falla de las medidas de protección, o que puede estar relacionada con la seguridad. (ISO/IEC, 2005)

TRIADA CID

(Rock, 2018) señala que Es un concepto de ciberseguridad que hace referencia a tres principios que deben trabajar en conjunto para garantizar la seguridad de un sistema informático: Confidencialidad, Integridad y Disponibilidad.

- **Confidencialidad:** Facultad que posee un sistema para evitar que personal no autorizado de la organización acceda a la información. (González, 2010)
- **Integridad:** La integridad se refiere a la exactitud e integridad de la información que tenemos.
- **Disponibilidad:** Propiedad de la información que garantiza que se encuentre disponible y accesible en el momento que sea necesario, siempre y cuando posea la debida autorización para acceder a ella. (García, 2017)

ISO 27005

La gestión de riesgos de la seguridad de la información forma parte de la familia ampliada de la serie ISO 27000 de normas ISO/IEC para sistemas de gestión de la seguridad de la información.

La norma ISO 27005 se compone de diversas etapas para poder realizar una correcta gestión del riesgo, dichas etapas van desde la identificación de los posibles riesgos, hasta un monitoreo de los mimos posterior a un tratamiento para darle solución, dichas etapas son:

1. Establecimiento del contexto
2. Identificación del riesgo
3. Estimación del riesgo
4. Evaluación del riesgo
5. Tratamiento del riesgo
6. Aceptación del riesgo
7. Comunicación del riesgo

ANÁLISIS DEL RIESGO

Uso sistemático para la identificación de fuentes y la evaluación de riesgos. (ISO/IEC, 2005)

Una técnica de análisis de riesgos es una técnica que ayuda evaluar el riesgo presente en un proyecto o proceso. Estos métodos nos ayudan a mejorar la toma de decisiones que nos permiten tomar medidas de precaución para evitar peligros potenciales y por lo tanto mitigar sus efectos. (Calle, 2020)

(Sordo, 2020) Un análisis de riesgos normalmente consta de 5 pasos, que se encargan de identificar, clasificar y dar seguimiento a los riesgos encontrados, pasos que son:

1. Considerar los riesgos que amenazan un proyecto o producto
2. Clasificar cada riesgo
3. Calificar cada riesgo
4. Pensar soluciones para cada riesgo
5. Calificar de nuevo cada riesgo

EVALUACIÓN DEL RIESGO

Proceso de comparar un riesgo estimado con un criterio de riesgo específico para poder determinar la importancia del riesgo. (ISO/IEC, 2005)

GESTIÓN DE RIESGOS

Según (Obando, 2019) 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.

TRATAMIENTO DEL RIESGO

Proceso de manejo de la selección e implementación de medidas para cambiar el riesgo. (ISO/IEC, 2005)

AMENAZAS INFORMÁTICAS

Las amenazas son eventos que pueden dañar procesos o recursos, pero las vulnerabilidades son fallas en el sistema de seguridad o en sí mismo y se utilizan para realizar actividades que permiten a los usuarios crear problemas con éxito. El trabajo

principal del gerente. La seguridad es una evaluación de riesgos mediante la identificación de vulnerabilidades y amenazas y, con base en esa información, la evaluación de los riesgos para las actividades y los activos. El riesgo debe verse como la posibilidad de que una amenaza particular explote una vulnerabilidad particular. (Romero, 2018)

La amenaza informática se refiere a la posibilidad de que ocurra un evento que cause un daño significativo o no grave a los recursos de su computadora o al sistema de información en cualquier momento. Se consideran amenazas los ataques de personas internas o externas que pueden dañar la infraestructura técnica, los sistemas de información o la misma información que se distribuye dentro de la organización.

Por lo tanto, Las amenazas informáticas se pueden describir como operaciones que explotan vulnerabilidades para explotar ataques o penetrar en los sistemas informáticos.

VULNERABILIDADES INFORMÁTICAS

Son fallas o debilidades del sistema informático. Estas son lagunas que pueden ser causadas por malas configuraciones o personas malintencionadas que violan la seguridad.

(Paths, 2019) establece que "Hoy en día, las empresas están expuestas a ataques informáticos que las ponen en peligro. Por lo tanto, debemos ser más aceptados por las políticas de seguridad informática y redefinir nuestra estrategia para la resiliencia cibernética."

DELITOS INFORMÁTICOS

Se refiere a todas las acciones realizadas por medios informáticos para sustraer, dañar o modificar información que afecte a una empresa o persona.

HACKERS

Es alguien que tiene un alto nivel de conocimiento sobre tecnología y puede usarlo para descubrir posibles vulnerabilidades en los sistemas informáticos.

CRACKERS

Es alguien con un alto grado de conocimiento técnico, pero a diferencia de los hackers, los crackers usan su conocimiento para comprometer los sistemas informáticos y, a menudo, beneficiarse. Y así lograr robar información sensible de la empresa.

VIRUS INFORMÁTICO

Estos son programas maliciosos que pueden cambiar el comportamiento de su computadora y destruir y eliminar información valiosa.

KALI LINUX

Kali Linux se basa en un sistema operativo especialmente diseñado para realizar funciones de seguridad como análisis de red, ataques a redes inalámbricas, análisis forense y otras funciones de seguridad.

Puede usar muchas herramientas para realizar pruebas de seguridad y actividades de análisis. Para ello tiene a disposición algunas herramientas como:

- Foremost
- Kismet
- Aircrack
- Nmap, etc.

NESSUS

Nessus es un programa de escaneo de vulnerabilidades para varios sistemas operativos. Consta del daemon nessusd, que ejecuta el análisis en el sistema de destino, y el cliente nessus, que muestra el progreso e informa sobre el estado del análisis.

Los beneficios más relevantes con los que cuenta son:

- Con la base de instalación más grande de la industria y la mejor experiencia, Nessus ayuda a los clientes a identificar las mayores amenazas y responder rápidamente.
- **Detalles:** paneles detallados para ayudar a los clientes a proteger sus redes de las ciberamenazas
- **Rentable:** Nessus reduce el tiempo y el costo de los análisis de seguridad y garantiza el cumplimiento de las normas de seguridad.

NMAP

Nmap es actualmente la mejor herramienta de escaneo de puertos y detección de host. Puede usar Nmap para obtener mucha información sobre las computadoras en su red. También puede buscar hosts activos y ver si hay algún puerto abierto si está filtrando puertos (firewall habilitado). E incluso puede conocer el sistema operativo utilizado por un objetivo en particular.

OPENVAS

Un servicio de escaneo (scanner) encargado de realizar análisis de vulnerabilidades. Un servicio de cliente utilizado como interfaz gráfica (web) necesaria para configurar OpenVAS, mostrar los resultados capturados y ejecutar informes.

MARCO METODOLÓGICO

La norma ISO 27005 se compone de 7 etapas, en las cuales se identificará, analizará, clasificará y tratará las vulnerabilidades encontradas durante el proceso de búsqueda de amenazas y vulnerabilidades, dichas etapas son:

1. Establecimiento del contexto
2. Identificación del riesgo
3. Estimación del riesgo
4. Evaluación del riesgo
5. Tratamiento del riesgo
6. Aceptación del riesgo
7. Comunicación del riesgo

INVESTIGACIÓN DE CAMPO

Es el proceso que nos permite tomar datos de la realidad y estudiarlos exactamente como se presentan, sin manipular variables. Por ello, es imprescindible realizarlo fuera del laboratorio, donde se produce el fenómeno. Permitirá tener una mejor percepción sobre el objeto de estudio al estudiarlo de cerca y poder recabar más información que ayude a tener un mejor resultado y apoye la toma de decisiones.

RECOLECCIÓN DE DATOS

Para lograr la obtención de los datos e información necesarias para el desarrollo de la investigación, se realizó una encuesta dirigida hacia la población estudiantil de la institución, al igual que ciertos integrantes del personal administrativo de la misma.

RESULTADOS

Tras la realización de un escaneo de vulnerabilidades con ayuda de herramientas como Nessus, una de las herramientas de seguridad informática para la realización de hacking ético y análisis de vulnerabilidades más usadas a nivel mundial, se pudo determinar ciertos problemas de seguridad.

ACTIVOS

En esta etapa se establece cuáles son los activos más importantes que tiene la UTB y serán considerados para estudio de caso, los cuales son:

ACTIVOS	
Hardware	Personal administrativo
Software	Datos
Instalaciones	Servidores

Tabla 1 *Activos* ***Fuente:*** *Autor*

IDENTIFICACIÓN DE RIESGOS

En esta etapa se realiza la determinación de amenazas y vulnerabilidades que fueron encontradas y que podrían poner en riesgos los activos tecnológicos de la UTB, para lograr esta identificación se hizo uso de la herramienta Nessus.

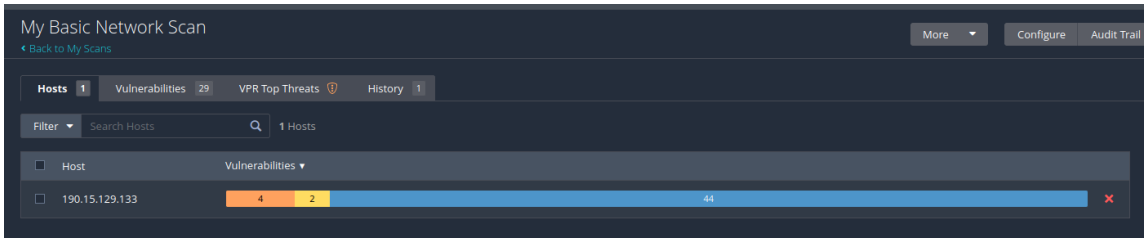


Figura 3 *Proceso de Escaneo con Nessus* ***Fuente:*** *Autor*

Tras la realización del análisis al sistema informático se pudo determinar que existen ciertas fallas de seguridad que ponen en riesgo la información que aquí se maneja.

Figura 4 *Resultados de Nessus* ***Fuente:*** *Autor*

A continuación, se detalla en una tabla los resultados arrojados del escaneo del sistema SAI de la UTB, con lo cual se puede determinar cuáles han sido las vulnerabilidades encontradas.

ESCANEO CON NESSUS		**VULNERABILIDADES**	
Vulnerabilidades:	6	**Criticas**	0
Información extra:	18	**Altas**	0
Total:	24	**Medias**	4
Tipo de Análisis:	Avanzado	**Bajas**	2
Hora Inicio:	8:50 PM		
Hora Fin:	9:10 PM		
Duración:	20 Min		

Tabla 2 *Resultados de Escaneo con Nessus* ***Fuente:*** *Autor*

ESTIMACIÓN Y TRATAMIENTO DEL RIESGO

En esta etapa se procede a realizar una estimación del riesgo que representan las vulnerabilidades que fueron encontradas en el escaneo y las acciones a tomar para poder solucionar el mismo.

Vulnerabilidad	JQuery 1.2 < 3.5.0 Multiple XSS		**Amenaza**	Robo de credenciales	
PROBABILIDAD		**Probable**	Media	Alta	Alta
		Posible	Baja	Media	Alta
		Improbable	Baja	Baja	Media
			Menor	**Moderado**	**Critico**
			IMPACTO		
Evaluación de Riesgo	Evitar el riesgo	**Tratamiento**	Actualizar la versión de JQuery mínimo a 3.5.0 o superior, para así poder evitar que el servidor pueda ser infectado mediante Scripts maliciosos que modifiquen su funcionamiento y/o comportamiento.		

Tabla 3 *Tabla de Vulnerabilidad 1* ***Fuente:*** *Autor*

Vulnerabilidad	SSL Certificate Cannot Be Trusted		**Amenaza**	Fallas certificado SSL	
PROBABILIDAD	**Probable**	Media		Alta	Alta
	Posible	Baja		Media	Alta
	Improbable	Baja		Baja	Media
		Menor		**Moderado**	**Critico**
		IMPACTO			
Evaluación de Riesgo	Modificar el riesgo	**Tratamiento**	Buscar otras opciones de certificados SSL que se adecuen a la naturaleza del sistema y por lo tanto se pueda brindar una mejor protección para una navegación e intercambio de información segura.		

Tabla 4 *Tabla de Vulnerabilidad 2* ***Fuente:*** *Autor*

Vulnerabilidad	TLS Version 1.0 Protocol Detection		**Amenaza**	Falla comunicación y criptografía	
PROBABILIDAD	**Probable**	Media		Alta	Alta
	Posible	Baja		Media	Alta
	Improbable	Baja		Baja	Media
		Menor		**Moderado**	**Critico**
		IMPACTO			
Evaluación de Riesgo	Modificar el riesgo	**Tratamiento**	Modificar las opciones de compatibilidad de la capa de seguridad de transporte con versión mínima de 1.2, de preferencia 1.3 y deshabilitar la 1.0 para evitar la ejecución de exploits no deseados.		

Tabla 5 *Tabla de Vulnerabilidad 3* ***Fuente:*** *Autor*

Vulnerabilidad	TLS Version 1.1 Protocol Deprecated		**Amenaza**	Falla comunicación y criptografía	
PROBABILIDAD	**Probable**	Media		Alta	Alta
	Posible	Baja		Media	Alta
	Improbable	Baja		Baja	Media
		Menor		**Moderado**	**Critico**
		IMPACTO			
Evaluación de Riesgo	Modificar el riesgo	**Tratamiento**	Modificar compatibilidad de la capa de seguridad de transporte con versión mínima de 1.2 para evitar la ejecución de exploits no deseados y mal funcionamiento y/o incompatibilidad con algunos navegadores.		

Tabla 6 *Tabla de Vulnerabilidad 4* ***Fuente:*** *Autor*

Vulnerabilidad	SSH Weak Key Exchange Algorithms Enabled		**Amenaza**	Algoritmos de intercambio débiles	
PROBABILIDAD	**Probable**	Media		Alta	Alta
	Posible	Baja		Media	Alta
	Improbable	Baja		Baja	Media
		Menor		**Moderado**	**Critico**
		IMPACTO			
Evaluación de Riesgo	Modificar el riesgo	**Tratamiento**	Comunicarse con el proveedor del servicio y/o revisar la documentación y opciones del producto para deshabilitar la opción de ejecutar algoritmos de intercambio débiles, provocando intercepciones de comunicación y sufrir robos de información.		

Tabla 7 *Tabla de Vulnerabilidad 5* ***Fuente:*** *Autor*

<table>
<tr><td>Vulnerabilidad</td><td colspan="2">SSH Server CBC Mode Ciphers Enabled</td><td>Amenaza</td><td colspan="2">Robo de información no cifrada</td></tr>
<tr><td rowspan="3">PROBABILIDAD</td><td>Probable</td><td>Media</td><td>Alta</td><td>Alta</td></tr>
<tr><td>Posible</td><td>Baja</td><td>Media</td><td>Alta</td></tr>
<tr><td>Improbable</td><td>Baja</td><td>Baja</td><td>Media</td></tr>
<tr><td colspan="2"></td><td>Menor</td><td>Moderado</td><td>Critico</td></tr>
<tr><td colspan="2"></td><td colspan="3">IMPACTO</td></tr>
<tr><td>Evaluación de Riesgo</td><td>Modificar el riesgo</td><td>Tratamiento</td><td colspan="3">Comunicarse con el proveedor del servicio y/o revisar la documentación para deshabilitar el modo de cifrado CBC y habilitar otros modos como CTR o GCM, dado que el modo de cifrado que utiliza puede causar que en caso de que un atacante intercepte o robe paquetes, y accedan a ellos por no estar cifrados correctamente.</td></tr>
</table>

Tabla 8 *Tabla de Vulnerabilidad 6* ***Fuente:*** *Autor*

MONITOREO DEL RIESGO

Tras la aplicación del plan y los procedimientos recomendados para gestionar el riesgo, amenaza y vulnerabilidades de los sistemas se puede estimar y determinar que el nivel actual de riesgo que representa cada vulnerabilidad ha sido modificado, y estaría representado de la siguiente manera:

VULNERABILIDAD	PROBABILIDAD	IMPACTO	RIESGO
JQuery 1.2 < 3.5.0 Multiple XSS	Baja	Medio	Bajo
SSL Certificate Cannot Be Trusted	Baja	Medio	Bajo
TLS Version 1.0 Protocol Detection	Baja	Bajo	Bajo
TLS Version 1.1 Protocol Deprecated	Baja	Bajo	Bajo
SSH Weak Key Exchange Algorithms Enabled	Baja	Bajo	Bajo
SSH Server CBC Mode Ciphers Enabled	Baja	Bajo	Bajo

DISCUSIÓN DE RESULTADOS

Durante los análisis al Sistema Académico Integral (SAI) de la UTB, considerado el sistema más importante, se pudieron determinar un total de 24 vulnerabilidades, de los cuales en realidad solo 6 representaban un riesgo para la seguridad de la información, mismas que estaba relacionadas a temas de utilización de tecnológicas desactualizadas y/o malas configuraciones en los servicios. Cabe recalcar que los resultados expuestos aquí aplican en otros entornos, dado que algunas de las vulnerabilidades expuestas en el sistema SAI se repiten en otros sistemas de la UTB.

Entre los principales problemas que se pudieron encontrar en los análisis realizados con Nessus, fue una relacionada con una falta de seguridad al utilizar una versión bastante desactualizada de la librería JQuery, la cual se relaciona con el lenguaje de programación JavaScript, utilizado para diversos propósitos, mayormente para facilitar el desarrollo de aplicaciones web. Situación que se puede corregir realizando una actualización a una versión más actualizada de esta librería, además realizar las respectivas configuraciones y/o correcciones de compatibilidad en caso de existir alguna modificación respecto a la versión usada actualmente.

Además, se pudo establecer alertas producidas por la utilización de certificados SSL no confiables o no adecuados para el tipo de servicio, también por malas configuraciones en el protocolo TLS que brinda seguridad en el transporte de información, al igual que el protocolo SSH, el cual se encarga de brindar una protección mayor a la información que se está intercambiando mediante la aplicación de técnicas de encriptación.

Realizada la valoración de riesgo se alcanza los resultados de que hace falta el diseño de un plan orientado específicamente al control de riesgos, amenazas y vulnerabilidades en los sistemas informáticos, pese a que se pudo saber sobre la existencia de un plan de contingencia, al hacer un análisis sobre el mismo, se pudo determinar que no aborda lo suficiente el tema de seguridad informáticas y amenazas, tampoco contempla una programación periódica para la realización de pruebas de hacking ético hacia los sistemas y por lo tanto poder determinar las vulnerabilidades existentes.

Por tanto, se puede determinar que existe una falta de control en ciertos aspectos de los sistemas, como llevar un control de las versiones utilizadas respecto a la versión más reciente, al igual que la apertura de algunos puertos para permitir conexiones remotas, pero, sobre todo, hace falta que se involucren más en la creación de un plan y/o procedimientos para gestionar de manera eficiente riesgos y amenazas informáticas, además de capacitar a todo el personal administrativo para conocimientos sobre las acciones a tomar ante una posible explotación de vulnerabilidades, si bien es cierto, que no podrán detener la amenaza de manera total, si podrían ayudar a reducir el mismo hasta que llegue personal especializado y pueda tomar las acciones necesarias según sea el caso.

CONCLUSIONES

- Los ciberataques a dispositivos informáticos, así como a sistemas de información son inevitables. Durante el desarrollo de este caso de estudio se pudo evidenciar que los sistemas de la UTB sufren de algunas fallas de seguridad informática, mismas que ponen en riesgo la integridad de los datos. Las vulnerabilidades fueron catalogadas como riesgos medios y bajos, además de información adicional que pueden ser consideradas superficiales y que no afectarían la seguridad de la información.
- Con la realización del caso de estudio se pudo determinar que en los sistemas de la UTB existen vulnerabilidades, algunos provocados por la falta de actualización de los servicios que utilizan, otros por falta de control en los puertos para conectarse a los servicios.
- Es necesario realizar una búsqueda frecuente y actualización de los mejores servicios y herramientas tecnológicas que brinda el mercado para poder realizar la detección de amenazas y vulnerabilidades a las que se exponen los sistemas web. Como las encontradas que hacen referencia a la librería JQuery, a certificados SSL no confiables o no adecuados para el tipo de servicio, malas configuraciones en los protocolos de la capa de seguridad de transporte.
- Contar con un plan de mejoras que permita tener un mejor abordaje sobre los problemas que pueden suceder al mejor de existir una amenaza, ya que mediante el uso del mismo se puede ayudar a mitigar el riesgo existente y ayudar a la toma de decisiones para el rápido restablecimiento del servicio.

RECOMENDACIONES

- Controlar y monitorear las actividades realizadas en los sistemas informáticos, al igual que llevar control de las versiones de las herramientas usadas para el desarrollo de los mismos y los puertos, en busca de reducir la amenaza de vulnerabilidades encontradas (Certificado SSL no confiable, mala configuración del protocolo TLS, mala configuración de protocolos de intercambio) y por lo tanto reducir el nivel de riesgo que estos podrían presentar.
- Aplicar diversas técnicas de hacking ético ambientado en distintos escenarios para poder probar la confiabilidad de los sistemas, y poder así obtener una mejor perspectiva sobre las falencias de seguridad y los riesgos que podrían representar.
- Realizar capacitaciones formativas al personal de la institución, respecto al tema de la seguridad informática y seguridad de la información. Esto con el fin de concientizar al personal sobre la importancia de hacer buen uso de los recursos informáticos y protegerlos adecuadamente.
- Realizar inspecciones de manera periódica a los recursos utilizados en los sistemas, dado a la constante progresión de la tecnológica de la misma manera progresa la manera en la que se pueden presentar los riesgos, mismos que deben ser minimizados para evitar problemas a futuro.

REFERENCIAS

Calle, J. P. (13 de Octubre de 2020). *5 métodos de análisis de riesgos*. Obtenido de Piranirisk: https://www.piranirisk.com/es/blog/5-m%C3%A9todos-de-an%C3%A1lisis-de-riesgos

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

Chen, C. (21 de Mayo de 2019). *Sistema de Información*. Obtenido de Significados: https://www.significados.com/sistema-de-informacion/

García, J. A. (2017). *Auditoría en informática.* Compañia Editorial Continental.

González, J. (2010). *Auditoría en informática.* Madrid.

ISO/IEC. (2005). *Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requerimientos.* Obtenido de ISO/IEC: http://www.cva.itesm.mx/biblioteca/pagina_con_formato_version_oct/apaweb.html

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

Obando. (2019). *Introducción a la Seguridad Informática.*

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

Rock, D. (12 de Marzo de 2018). *¿Qué es la «Tríada CID» o el «Triángulo de la Seguridad»?* Obtenido de Donnierock: https://donnierock.com/2018/03/12/que-es-la-triada-cid-o-el-triangulo-de-la-seguridad/

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

Sordo, A. I. (29 de Diciembre de 2020). *¿Qué es y cómo hacer un Análisis de Riesgos?* Obtenido de HubSpot: https://blog.hubspot.es/marketing/analisis-de-riesgos

Uriona, G. R. (2002). *Estrategias para la seguridad de la información.* La paz Bolivia: Editorial Yanapti.

Velthuis, M. P., Rubio, F. O., & Muñoz-Reja, I. C. (2006). *Calidad de Sistemas Informáticos.* Alfaomega Ra-Ma.

Welivesecurity. (14 de Mayo de 2013). *MAGERIT: metodología práctica para gestionar riesgos*. Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

ANEXOS

ANEXO 1

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

CUESTIONARIO

1. ¿Cree que la Universidad Técnica de Babahoyo conoce las amenazas y vulnerabilidades a las que se encuentran expuestas sus sistemas informáticos?

   Si ( ) No ( ) Tal vez ( )

2. ¿Sabe que es una amenaza informática?

   Si ( ) No ( )

3. ¿Considera que un sistema que utiliza tecnologías desactualizadas es seguro?

   Si ( ) No ( ) Tal vez ( )

4. ¿Cree que es necesario la aplicación de una normativa que ayude a gestionar el riesgo de la seguridad de la información?

   Si ( ) No ( ) Tal vez ( )

5. ¿Conoce sobre la existencia de un plan de gestión ante problemas en los sistemas informáticos?

   Si ( ) No ( )

6. ¿Cuál cree que sería el impacto de positividad de la aplicación de un plan de gestión de riesgos informáticos basado en la norma ISO 27005?

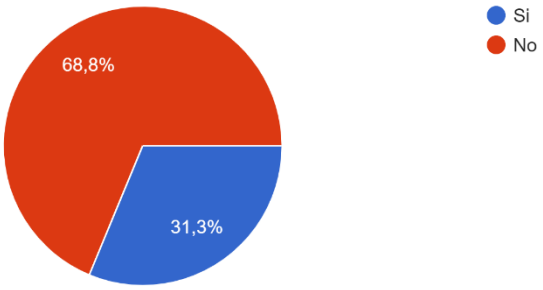
   Ninguno ( ) Bajo ( ) Medio ( ) Alto ( )

ANEXO 2

Tabulación de la información de las encuestas

1. ¿Cree que la Universidad Técnica de Babahoyo conoce las amenazas y vulnerabilidades a las que se encuentran expuestas sus sistemas informáticos?

32 respuestas

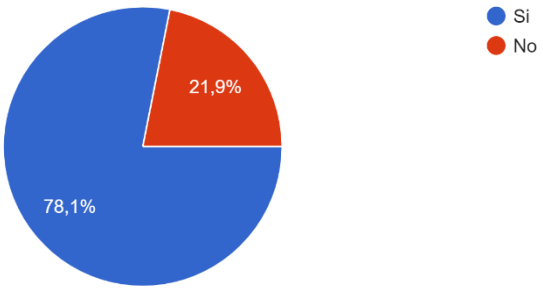


Análisis: De los encuestados se demuestra que un 68.8% indica considerar no creer que la UTB tenga conocimiento sobre las vulnerabilidades de sus sistemas, mientras que el 31.3% restante indica lo contrario, que si tienen el conocimiento.

Interpretación: Se recomienda hace un análisis periódico de los sistemas para dar confianza a ese 68.8% de que su información es segura.

2. ¿Sabe que es una amenaza informática?

32 respuestas

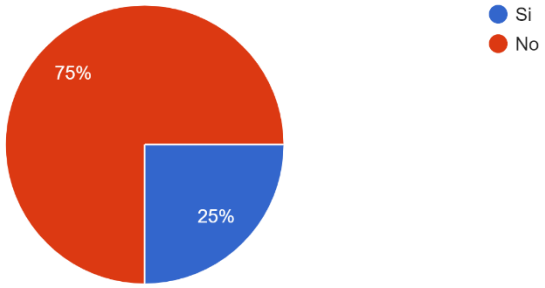


Análisis: El 78.1% de los encuestados manifiesta ser consciente sobre lo que es una amenaza informática y los riesgos que representan, mientras que el 21.9% restante no tiene conocimiento sobre el tema.

Interpretación: Existe un 21.9% de los encuestados que no tienen conocimientos sobre lo que es una amenaza informática.

3. ¿Considera que un sistema que utiliza tecnologías desactualizadas es seguro?

32 respuestas

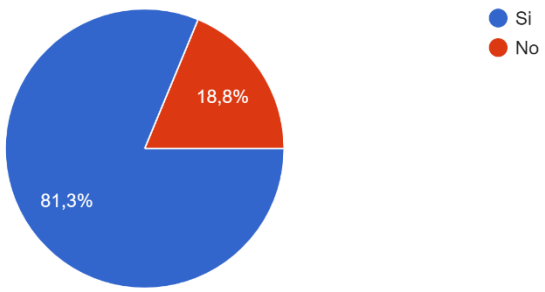


Análisis: El 75% de los encuestados indica que un sistema ya no es seguro si está usando tecnologías desactualizadas, mientras que un 25% considera que sí sigue siendo seguro.

Interpretación: Existe un 75% que indica que se debe trabajar en mantener los sistemas informáticos lo más actualizados posible, para resguardar su información.

4. ¿Cree que es necesario la aplicación de una normativa que ayude a gestionar el riesgo de la seguridad de la información?

32 respuestas

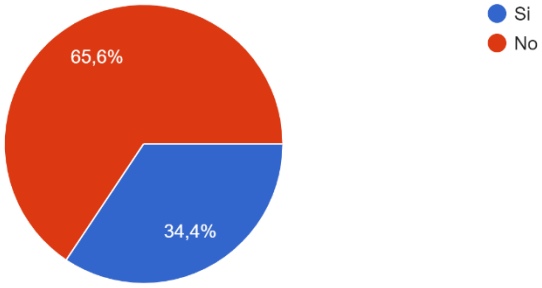


Análisis: De los encuestados un 81.3% considera necesaria la aplicación de una normativa que ayude a gestionar los riesgos informáticos, mientras que un 18.8% considera que no es algo necesario.

Interpretación: El 81.3% de los encuestados considera que es necesario la aplicación de un estándar que ayude a gestionar de manera correcta la gestión de riesgos informáticos.

5. ¿Conoce sobre la existencia de un plan de gestión ante problemas en los sistemas informáticos?

32 respuestas

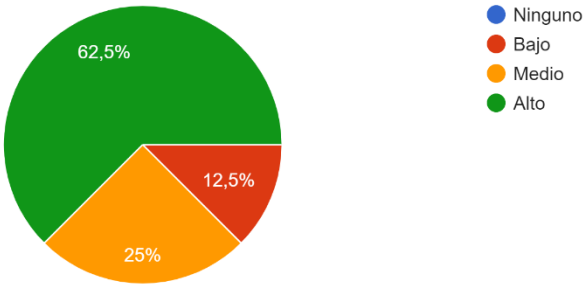


Análisis: De los encuestados un 65.4% de los encuestados manifiesta no tener ningún conocimiento sobre la existencia de un plan de gestión de riesgos informáticos, mientras que un 34.4 manifiesta si tener conocimiento.

Interpretación: Existe un 65.6% que considera necesario la socialización de un plan de gestión en caso de haberlo.

6. ¿Cuál cree que sería el impacto de positividad de la aplicación de un plan de gestión de riesgos informáticos basado en la norma ISO 27005?

32 respuestas



Análisis: El 62.5% de los encuestados considera que un plan de gestión basado en un estándar como la ISO tendría una alta positividad, mientras que el 25% considera que sería un impacto no tan alto y el 12.5% restante cree que sería bajo.

Interpretación: Existe un 62.5% que ve como algo muy positivo un plan desarrollado siguiendo estándares internacionales que permita evaluar y tratar amenazas informáticas correctamente.

ANEXO 3

```
└─$ nmap sai.utb.edu.ec
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-08 11:04 EDT
Nmap scan report for sai.utb.edu.ec (190.15.129.133)
Host is up (0.40s latency).
Not shown: 911 filtered tcp ports (no-response), 79 filtered tcp ports (host-unreach)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
587/tcp  open   submission
2525/tcp closed ms-v-worlds
8008/tcp open   http
9101/tcp closed jetdirect
9102/tcp closed jetdirect
9103/tcp closed jetdirect

Nmap done: 1 IP address (1 host up) scanned in 73.99 seconds
```

Figura 5 *Analisis de puertos con Nmap* ***Fuente:*** *Autor*

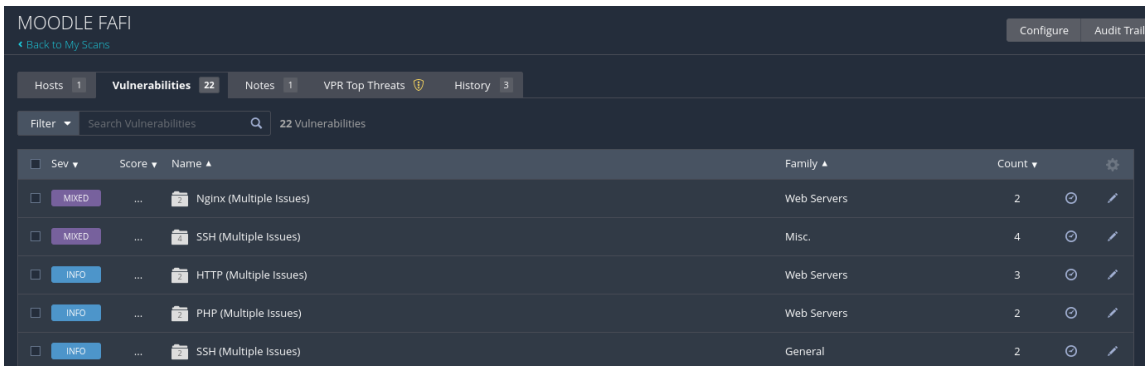


Figura 6 *Resultados de escaneo a Moodle FAFI con Nessus* ***Fuente:*** *Autor*

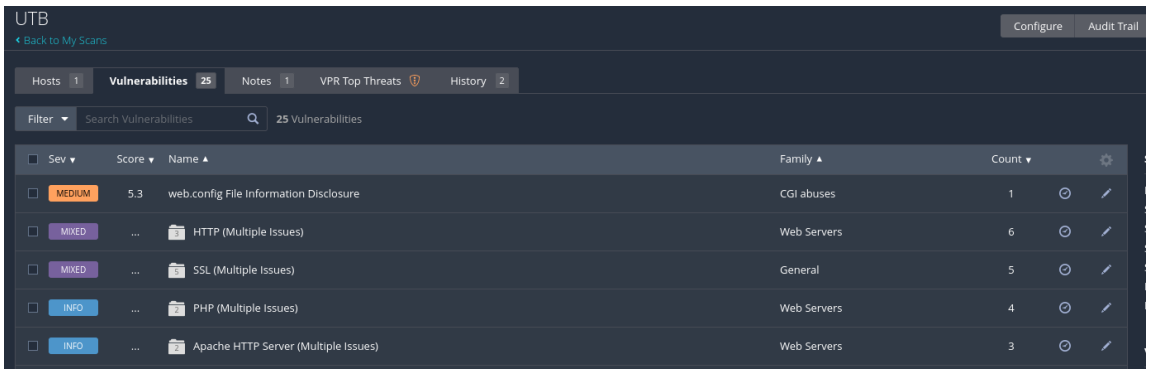
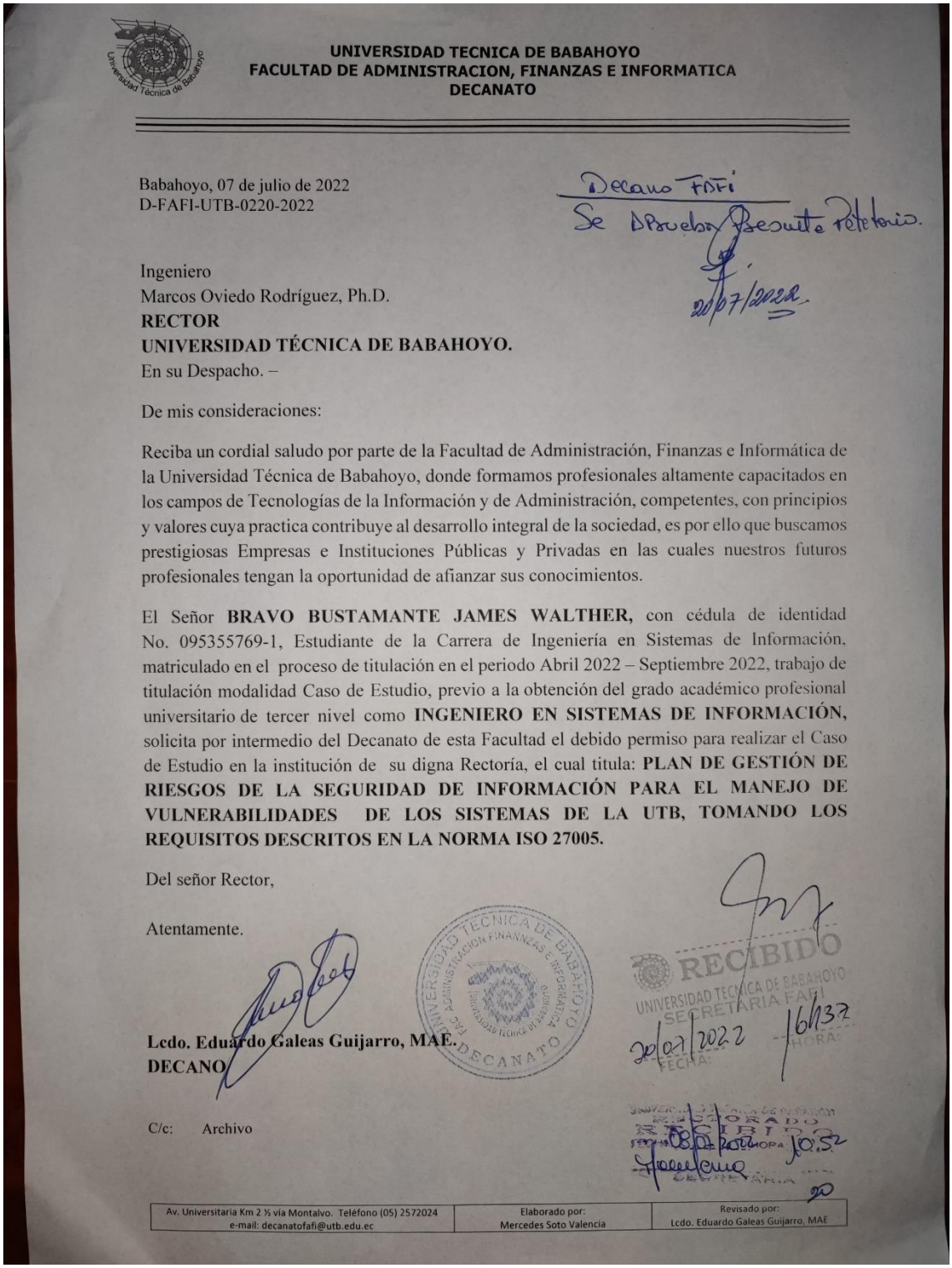


Figura 7 *Resultados de escaneo a la web de la UTB con Nessus* ***Fuente:*** *Autor*

ANEXO 4

AUTORIZACIÓN PARA LA REALIZACIÓN DEL CASO DE ESTUDIO



UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
DECANATO

Babahoyo, 07 de julio de 2022
D-FAFI-UTB-0220-2022

Decano FAFI
Se Aprueba Presente Petición.
20/07/2022

Ingeniero
Marcos Oviedo Rodríguez, Ph.D.
RECTOR
UNIVERSIDAD TÉCNICA DE BABAHOYO.
En su Despacho. –

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El Señor **BRAVO BUSTAMANTE JAMES WALTHER,** con cédula de identidad No. 095355769-1, Estudiante de la Carrera de Ingeniería en Sistemas de Información, matriculado en el proceso de titulación en el periodo Abril 2022 – Septiembre 2022, trabajo de titulación modalidad Caso de Estudio, previo a la obtención del grado académico profesional universitario de tercer nivel como **INGENIERO EN SISTEMAS DE INFORMACIÓN,** solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar el Caso de Estudio en la institución de su digna Rectoría, el cual titula: **PLAN DE GESTIÓN DE RIESGOS DE LA SEGURIDAD DE INFORMACIÓN PARA EL MANEJO DE VULNERABILIDADES DE LOS SISTEMAS DE LA UTB, TOMANDO LOS REQUISITOS DESCRITOS EN LA NORMA ISO 27005.**

Del señor Rector,

Atentamente.

UNIVERSIDAD TÉCNICA DE BABAHOYO
FAC. ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
DECANATO

RECIBIDO
UNIVERSIDAD TÉCNICA DE BABAHOYO
SECRETARÍA FAFI
FECHA: 20/07/2022 HORA: 16h37

Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO

C/c: Archivo

RECIBIDO
FECHA: 08/08/2022 HORA: 10:52
SECRETARÍA

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Mercedes Soto Valencia	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

ANEXO 5

CERTIFICADO DE APROBACIÓN DE ANTIPLAGIO

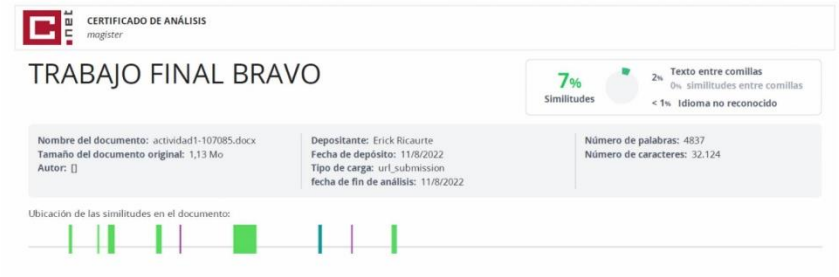
UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE INGENIERIA DE SISTEMAS DE INFORMACIÓN

Babahoyo, 11 de agosto de 2022

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación del Sr.: **Bravo Bustamante James Walther**, cuyo tema es: PLAN DE GESTIÓN DE RIESGOS DE LA SEGURIDAD DE INFORMACIÓN PARA EL MANEJO DE VULNERABILIDADES DE LOS SISTEMAS DE LA UTB, TOMANDO LOS REQUISITOS DESCRITOS EN LA NORMA ISO 27005, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio, obteniendo como porcentaje de similitud de **[7%]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.



Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

Firmado electrónicamente por:
ERICK MAGNO RICAURTE ZAMBRANO

Ing. Erick Ricaurte Zambrano, MSIG,MBA
DOCENTE DE LA FAFI.