UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE VULNERABILIDADES, AMENAZAS Y ATAQUES A LA PÁGINA WEB DE LA UNIVERSIDAD TÉCNICA DE MACHALA.

ROBLES HERRERA RUTH ESTEFANIA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE VULNERABILIDADES, AMENAZAS Y ATAQUES A LA PÁGINA WEB DE LA UNIVERSIDAD TÉCNICA DE MACHALA.

ROBLES HERRERA RUTH ESTEFANIA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE VULNERABILIDADES, AMENAZAS Y ATAQUES A LA PÁGINA WEB DE LA UNIVERSIDAD TÉCNICA DE MACHALA.

ROBLES HERRERA RUTH ESTEFANIA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 01 DE FEBRERO DE 2019

MACHALA
01 de febrero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Análisis de vulnerabilidades, amenazas y ataques a la página web de la Universidad Técnica de Machala., hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

GONZALEZ SANCHEZ JORGE LUIS
0703333898
TUTOR - ESPECIALISTA 1

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
ESPECIALISTA 2

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 3

Fecha de impresión: viernes 01 de febrero de 2019 - 10:25

URKUND

Urkund Analysis Result

Analysed Document:	ROBLES HERRERA RUTH ESTEFANIA_PT-011018.pdf (D47095982)
Submitted:	1/22/2019 3:50:00 AM
Submitted By:	titulacion_sv1@utmachala.edu.ec
Significance:	0 %

Sources included in the report:

Instances where selected sources appear:

0

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, ROBLES HERRERA RUTH ESTEFANIA, en calidad de autora del siguiente trabajo escrito titulado Análisis de vulnerabilidades, amenazas y ataques a la página web de la Universidad Técnica de Machala., otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 01 de febrero de 2019

ROBLES HERRERA RUTH ESTEFANIA
1104820335

RESUMEN

La presente investigación trata sobre el análisis de las vulnerabilidades de la página web de la Universidad Técnica de Machala y las consecuencias que estás producen, este tipo de instituciones de educación superior requieren que sus plataformas digitales se encuentren a las necesidades de los usuarios; de tal modo que, la información y el desarrollo de las operaciones realizadas a través de este medio vayan encaminadas al cumplimiento de objetivos y metas de la institución, es indispensable identificar de manera constante las vulnerabilidades que presenta una plataforma web, de manera que se evalúe la seguridad de la información y se minimice los riesgos de sufrir ataques, manipulación y alteración de datos, presentando así contenido íntegro, el objetivo de esta investigación es analizar las vulnerabilidades, riesgos y amenazas a las que está expuesta la página web, identificando sus principales debilidades en cuanto a seguridad de la información, para análisis de datos se presentó una matriz de riesgos y una matriz FODA que muestra las vulnerabilidades, riesgos y amenazas relevantes que pueden ser mitigados si se usan las herramientas y técnicas adecuadas.

Palabras clave: "Auditoría Informática" / "Seguridad Informática", Cyber-ataques, "Procesos, Riesgos y amenazas".

ABSTRACT

This research is on the analysis of vulnerabilities de the website of the Technical University of Machala and the consequences that you produce, this type of institutions of higher education require that their digital platforms is meet the needs of the users; in such a way that, the information and the development of the operations carried out through this medium will aimed at the fulfilment of the objectives and goals of the institution, it is essential to identify the vulnerabilities that presents a steadily web platform, in a way that will evaluate the security of the information and to minimize the risk of attacks, manipulation and alteration of data, presenting content so full, the objective of this research is to analyze the vulnerabilities, risks and threats that exposed the website, identifying major weaknesses in terms of information, for data analysis was presented an array of risks and a SWOT matrix showing the vulnerabilities, risks and relevant threats that can be mitigated using tools and proper techniques.

Keywords: "Computer Audit" / "Information Security", Cyber-attacks, "Processes, Risks and threats".

ÍNDICE DE CONTENIDO

Pág.

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE ILUSTRACIONES

Pág.

INTRODUCCIÓN

El uso del internet se ha convertido en una herramienta indispensable en la vida del ser humano, permitiendo grandes cambios en la economía, la educación, la política y lo social. A medida que las personas se vuelven más dependientes de la tecnología y sus avances, surgen también más riesgos, volviendo vulnerable los datos e información alojada en los sitios web. En un contexto global donde cada gobierno, entidad e institución se vuelve más competitiva tecnológicamente, los establecimientos educativos han convertido el uso de las TIC's en su herramienta principal tanto como material principal de aprendizaje, que como recurso de administración, asegurando su capacidad de generar logros efectivos y de calidad.

Para las instituciones educativas es de vital importancia que evalúen constante y regularmente cada uno de los procesos que se lleva a cabo a través de los sitios web, ya que la información se encuentra expuesta a sufrir daños o pérdidas; es por ello que la presente investigación se refiere al estudio de la Auditoría informática en los entornos virtuales de los establecimientos educativos, sobretodo de nivel superior, enfocándonos en el ambiente virtual de la Universidad Técnica de Machala. Representa indispensable identificar las vulnerabilidades, amenazas y riesgos que llega a presentar la plataforma web, con el fin de que el contenido y los servicios prestados a través de esta, sean efectivos y de calidad para el usuario.

A través de la Auditoría informática, se pretende preservar la seguridad de la información, ya que esta representa el todo de una institución, y por consiguiente debe ser resguardada, protegida del riesgo y de posibles pérdidas, alteración, daños, etc.; cabe indicar que la información está en un peligro constante, ya sea interno o externo, es por ello que la importancia de aplicar una auditoría informática en el desempeño y funcionalidad de una página web, radica en que permite determinar las fortalezas y debilidades de su configuración virtual y automatizada.

La metodología empleada para el desarrollo de la investigación es descriptiva, mediante la cual determinaremos las principales vulnerabilidades que posee la plataforma web de la Universidad Técnica de Machala, a través de su identificación se emitirán

recomendaciones acerca de las políticas que no se están considerando en salvaguardar los datos y toda la información alojada en ella, de tal manera que se dé cumplimiento al objetivo planteado en esta investigación; además, se aplica una metodología cualitativa, para la obtención de resultados, haciendo uso de la técnica de la entrevista dirigida al encargado/a de la funcionalidad y mantenimiento de la página web.

1. FUNDAMENTACIÓN TEÓRICA

1.1. Análisis Preliminar

Hoy en día en un entorno donde todo se mueve a través del mundo digital, la auditoría informática se considera como aquella herramienta básica, que permite determinar la correcta funcionalidad de los equipos tecnológicos y de los servicios que se prestan a través de ellos, como la publicidad en plataformas de una empresa o institución donde se dan a conocer sus productos o servicios. La Auditoría Informática según Martínez, Blanco Alfonso, & Loy Marichal (2013) citando a Zavaro Babani, León, Martínez García, & Caferino (1999) es el "conjunto de procedimientos y técnicas que permiten a una entidad: evaluar, total o parcialmente, el grado en que se cumple la observancia de los controles internos asociados al Sistema Informático" (pág. 2); su aplicación permite un resguardo eficiente de la información.

Evaluar la integridad de la información debe estar a cargo de especialistas, y al momento de hablar de auditoría informática, mencionamos que esta debe estar conformada por profesionales, con peritos en informática; de tal modo que se evalúen cada uno de los riesgos a los que se exponen los datos alojados en la web. La información es el bien o activo más valioso que posee una empresa o institución, por lo que debe ser respaldada, cada actividad u operación que se realiza a lo largo del tiempo.

El avance tecnológico, en las últimas décadas va en constante crecimiento y sus cambios han influenciado en varios aspectos, siendo el más destacado el crecimiento económico. Según Porcile, Holland, Cimoli, & Rosas (2006) "la brecha tecnológica afecta el patrón de especialización y el crecimiento relativo de los países en la economía internacional" (pág. 484); es por ello que la tecnología es una herramienta fundamental para el desarrollo social y económico de cualquier país.

Si bien el internet facilita a cualquier entidad o institución llegar al usuario de una forma más interactiva, ahorrando recursos como: el tiempo, dinero, etc., además de que facilita realizar trámites en la mayor brevedad posible, permaneciendo al día con las noticias y cambios que realice la institución. La educación al igual que la economía, ha ido en

constante evolución, por lo que actualmente los servicios que brindan lo realizan a través de plataformas virtuales facilitando las operaciones tanto al usuario como al administrador; por lo que se puede decir que los estudiantes están en contacto directo con docentes o autoridades.

Al ofrecer los sistemas de información grandes beneficios, también representan mayores niveles de riesgo requiriendo cada vez un mayor incremento en la seguridad de la información (Yasser & et al, 2014).

1.2. Riesgos, amenazas y vulnerabilidades en las páginas web

Los sitios web están expuestos a miles de riesgos y vulnerabilidades, puesto que el internet a más de ser una herramienta esencial también es alojamiento de virus y amenazas, que buscar afectar y manipular la información. En abril y agosto del 2008 según Yasser et al., (2014) "aproximadamente 500.000 páginas web que usaban como servidor el Microsoft IIS y el servidor de SQL, fueron atacadas usando inyección de SQL" (pág. 53); cabe indicar que el número de ataques y vulnerabilidades reportadas a través del Instituto Nacional de Vulnerabilidades de Estados Unidos han ido en aumento en los últimos años.

Para mantener un buen seguro de información se precisa de controles de seguridad a los sistemas informáticos, de tal manera que se minimice la pérdida de recursos, el impacto del fracaso de la seguridad en datos confiables, la posibilidad de perder confianza en un servidor o sitio web y la vulnerabilidad del uso de una computadora o cualquier dispositivo electrónico sin autorización (Yasser & et al, 2014); y se menciona *minimizar* debido a que el riesgo siempre está presente.

Es esencial aceptar el riesgo, ya que siempre existe un grado de incertidumbre y lograr el éxito depende de asumir riesgos, y saber cómo gestionar controles que los combatan y nos conduzcan hacia el cumplimiento de objetivos y metas. Cuando hablamos de riesgo siempre asumimos que nos irá mal, sin embargo junto al riesgo se presentan nuevas oportunidades, que son claves para el crecimiento de un emprendedor. "Establecer

controles significa la generación de políticas, normas y procedimientos que conlleven a la mitigación del riesgo" (Gómez, Pérez, Donoso, & Herrera, 2010, pág. 110).

Las tecnologías de Información y Comunicación se están convirtiendo en herramientas indispensables para las instituciones de educación superior, porque a través de ellas se puede compartir ideas, enviar tareas, mantener clases virtuales, noticias en páginas web, bibliotecas virtuales y se puede mencionar muchos más beneficios que otorgan. "Hoy en día cualquier computadora conectada a internet está expuesta a diversas amenazas" (Hernández Saucedo & Mejia Miranda, 2015). La mejor manera de prevenir los ataques informáticos es actuar de manera anticipada, detectando las vulnerabilidades presentes en la web, los fallos en la seguridad y de esta manera reducir la probabilidad de que exista un ataque.

1.3. Cyberataques

Cualquier dispositivos electrónico está propenso a sufrir un hacker o ataque cibernético, ninguno resulta hoy en día lo suficientemente seguro para estar libres de riesgo. Cabe indicar que el riesgo cibernético se encuentra en tercer lugar, dentro de las preocupaciones de las empresas según lo menciona (Sobrino, 2017, pág. 144). Muchas de las veces una pérdida de información no solo afecta al propietario del sistema sino que se genera un daño a terceros como pueden ser los clientes, mencionando como ejemplo a las tiendas virtuales, donde los clientes ingresan información financiera y se producen cuantiosas pérdidas económicas, los bancos son otro elemento que tiende a sufrir mayores ataques cibernéticos.

Según menciona Vicente Pons (2017) "El surgimiento de internet y su expansión ha demostrado ser una de las revoluciones tecnológicas más importantes de la historia contemporánea" (pág. 81); este rápido y acelerado crecimiento de las tecnologías de información abrió espacios para el delito, poniendo a disposición de las delincuentes y terroristas un arma poderosa. Los aspectos ilícitos cometidos en el ciberespacio poseen cuatro características según Subijana Zunzunegui (2008) citado por Vicente Pons (2017) "se cometen fácilmente; requieren escasos recursos en relación del perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio; y se

benefician de debilidades que pueden existir en determinados espacios u áreas" (pág. 82), estas lagunas han sido denominados paraísos cibernéticos.

En Ecuador los delitos informáticos cometidos a través de dispositivos electrónicos y que se penalizan con prisión preventiva son los siguientes: pornografía infantil, violación del derecho a la intimidad, revelación ilegal de información de bases de datos, interceptación de comunicaciones, pharming y phishing, fraude informático, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente y acceso no permitido a un sistema informático, telemático o de telecomunicaciones (Código Orgánico Integral Penal COIP, 2014).

1.4. Cyberseguridad

Antes de hablar de la seguridad informática, definiremos lo que es defensa para Vargas Borbúa , Recalde Herrera, & Reyes (2017) "son aquellas medidas que permiten mantener un resguardo de los riesgos, amenazas, peligros y daños" (pág. 32), a los que está expuesta la información sean estos físicos o lógicos. Al representar la información el activo más preciado de toda organización e institución, se requiere de un seguro que permita resguardarla, es decir que las acciones de defensa deben estar estrechamente ligadas a los riesgos y amenazas que surgen en el tiempo, de tal forma que brinden confianza y certeza de desarrollar actividades en el mundo virtual.

Con los avances tecnológicos y el aumento de dispositivos, la necesidad de mitigar el riesgo y mejorar la asignación de recursos para combatir las amenazas, requiere de un análisis en busca de soluciones a problemas, de tal forma que se evite pérdidas de información y dinero (Parada, Flórez, & Gómez, 2018, pág. 28). Es por ello que actualmente existen empresas que brindan seguros a la información, por ejemplo si llegase a ocurrir un daño a la información financiera de un cliente en una entidad bancaria y esta cuenta con un seguro, las probabilidades de recuperarla y evitar daños es alta, brindando una mayor confianza a los clientes según lo menciona (Sobrino, 2017).

La seguridad cibernética es el conjunto de prácticas, herramientas y técnicas que se incorporan en la seguridad de las TIC's para minimizar las vulnerabilidades, mantener la

integridad del sistema, permitir acceso solo a usuarios aprobados y defensa de activos; apoya los objetivos de aseguramiento de la información dentro de un contexto digital pero no se extiende a lo analógico (Darko, Darko, & Boris, 2017, pág. 274). Sin embargo para mantener una buena seguridad informática es imprescindible mantener una buena seguridad física, empezando por el acceso limitado del personal, seguridad física de los dispositivos electrónicos y del área en donde se encuentren ubicados.

1.5. Control Informático y seguridad

La seguridad de la información surge en función de los objetivos que se plantea una organización, con el fin de su cumplimiento, se convierten en prioridad mucho más si están ligados al área de telecomunicaciones e informática. Existen dos términos usados en torno a esto: La Seguridad de la Información y Seguridad Informática, que aunque su significado no es lo mismo, persiguen un mismo fin cuando se trata de proteger la Confidencialidad, Integridad y Disponibilidad de la Información (Roba Iviricu, Vento Alvarez, & García Concepción, 2016).

La seguridad de la información para Roba, Vento & García (2016) es la disciplina que nos habla de los riesgos, de las amenazas, de análisis de escenarios, de buenas prácticas y esquemas normativos; y que se crean técnicas para la protección de la información, tales como: antivirus, firewalls, detección de intrusos, atención de incidentes, detección de amenazas, entre otros (pág. 336). La protección de la información debe estar a cargo de profesionales de tal modo que constantes análisis sean eficientes y obtengan una integridad de información cada vez más completa, incrementando la confiabilidad y respaldo de datos en una institución.

La detección oportuna de vulnerabilidades, no se limita en identificar un par de riesgos en la web, sino que evalúa cada uno de los activos más frágiles de una organización y crea una barrera de protección. Roba, Vento & García (2016) mencionan que “se precisa de una buena metodología con el propósito de evaluar los activos relevantes a ser protegidos” (pág. 337), esta metodología permite la eficiencia y eficacia en la detección de vulnerabilidades y mitiga el riesgo de sufrir un ataque informático.

1.6. La seguridad informática en los websites.

Como se mencionó anteriormente la seguridad lógica depende de la seguridad física, debido a que un tercero no podrá hacer uso de un dispositivo electrónico si no tiene permiso de acceso, por lo tanto su amenaza u ataque estará bajo control, esto se debe a que hay sistemas u operaciones que son ejecutadas desde un comando principal y se necesita tener acceso del mismo para llevar a cabo cualquier manipulación de la información. "La seguridad de la información ha cobrado una importancia relevante en las organizaciones, tanto públicas como privadas, ya que representa en un bien en riesgo, que debe ser resguardado y protegido contra posibles daños, pérdidas, manipulación, etc." (Arcentales Fernández & Caycedo Casas, 2017, pág. 159).

La seguridad física es aquella que se encarga de resguardar los dispositivos tecnológicos de las amenazas producidas por el hombre y la naturaleza; mientras que la seguridad lógica restringe el acceso a programas y archivos, evitando el acceso de intrusos en el sistema informático (Martelo , Tovar, & Maza, 2018). Se precisa de los dos tipos de seguridad para mantener un control de información eficiente, puesto que el número de amenazas aumentan conforme crecen los mecanismos de la seguridad informática.

Para determinar las debilidades y fortalezas, en cuanto a funcionalidad del sistema de información automatizada, configuración de la plataforma, calidad y dominio informático, exploración y simulación de vulnerabilidades se precisa de la intervención de la auditoría informática, integrada por profesionales que identifiquen cada riesgo presente en el o los sistemas. "Un conjunto bien definido de políticas y procedimientos de seguridad puede prevenir pérdidas y ahorrar recursos para la organización, es así que la Auditoría de Seguridad Informática es importante como medio de detección de desviaciones" (Arcentales Fernández & Caycedo Casas, 2017, pág. 163); una vez identificadas las irregularidades el auditor emite sugerencias de corrección las mismas que van encaminadas a conseguir el cumplimiento de los objetivos de una organización.

La seguridad informática para Gil Vera & Gil Vera (2017) "representa igual de importante que la seguridad aplicada a otros entornos, ya que trata de minimizar los riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada y en general

malintencionada" (pág. 194). Su único fin es proteger los recursos informáticos valiosos de cualquier organización.

2. RESULTADOS

Con el fin de determinar las vulnerabilidades, riesgos y amenazas a los que está expuesta la plataforma virtual de la Universidad Técnica de Machala, se consideró realizar una entrevista a la Ing. Betty Pachucho encargada del mantenimiento de la página web a través de la Unidad de Sistemas de la Dirección de Tecnologías de Información y Comunicación, partiendo antes de una investigación documental, donde se obtendrá información de libros, revistas, códigos y políticas.

La seguridad de la información que se brinda a través de áreas tecnológicas, presenta políticas de seguridad con el fin de garantizar la confidencialidad, integridad, disponibilidad de la información y uso correcto de los equipos informáticos, las mismas que son emitidas por la Dirección de las TIC, cabe indicar que los lineamientos que contiene será para aplicación de toda la comunidad universitaria: docentes, empleados y estudiantes; además indica que para la protección de los sistemas, la Dirección de TIC debe autorizar el uso de las herramientas y asegurar que el software de seguridad sea actualizado de manera permanente (Dirección de TIC Universidad Técnica de Machala, 2018).

2.1. Plataforma virtual de la Universidad Técnica de Machala

A pesar de ser una plataforma virtual utilizada como medio público, con el fin de poner a disposición de clientes, usuarios, estudiantes, docentes y terceros, resulta indispensable analizar las vulnerabilidades a las que puede estar sujeta y ofrecer posibles sugerencias que conlleven a incrementar el nivel de seguridad de tal manera que la información que se brinde sea de calidad, íntegra y confiable. El análisis de la seguridad informática de la plataforma virtual de la Universidad Técnica de Machala se realizará a partir de una matriz de riesgos y una matriz FODA, estructurada a partir de los datos obtenidos en la entrevista.

Al ser la UTMACH una institución de educación superior debe hacer uso de excelentes sistemas de información, con una seguridad imprescindible, que se mantenga alerta a los posibles ataques y riesgos que puede sufrir. La plataforma virtual de la UTMACH brinda varios servicios a la sociedad y comunidad universitaria tales como: acceso a la biblioteca virtual, noticias académicas (capacitaciones, talleres, seminarios, etc.), información de autoridades, publicaciones de banco de preguntas para egresados con su respectivo enlace al proceso de titulación, entre otros.

Es importante mencionar que el diseño y estructura de la página web ha sido una adquisición externa gestionada por la Dirección de la Tecnología de Información y Comunicación, la misma que se encarga de gestionar el mantenimiento y actualización de manera semestral. Posee el protocolo HTTPS denominado así por sus siglas en Inglés (Hypertext Transfer Protocol Secure), el cual se encarga de "proveer protección y garantía en el envío de información a través de internet, de manera que el usuario que envía tendrá la confianza de que su información no podrá ser interceptada" (García, Cervigón Hurtado, & Alegre Ramos, 2012, pág. 1128).

Además del protocolo HTTPS la plataforma web cuenta con un certificado SSL y está al día con las actualizaciones brindadas por WORDPRESS. Para García, Cervigón Hurtado, & Alegre Ramos (2012) SSL "también certifica una comunicación segura a través de internet, proporcionando seguridad en la identificación del servidor y del cliente; cifra la integridad de la información en ambas partes de la comunicación" (pág. 129), de esta manera la información viaja a través de internet de una manera segura.

El certificado SSL está incorporado a muchos navegadores web como es: Navigator de Netscape y el Internet Explorer de Microsoft; constituye la solución principal en el comercio electrónico, debido a que está basada en la aplicación conjunta de criptografía simétrica y criptografía asimétrica, que certifican un medio seguro de comunicación a través de internet (Ortega & Canino, 2015, pág. 58), es así que la información proporcionada en la plataforma universitaria es confiable y segura para el cliente.

El análisis de la seguridad informática de la plataforma web de la Universidad Técnica de Machala se realizará a partir de una matriz de riesgos, los mismos que fueron

identificados en base a los datos obtenidos en la entrevista, y se pone de manifiesto que la UTMACH es una institución que hace uso de grandes innovaciones en seguridad informática, y con mantenimientos constantes que evalúan el grado de seguridad de la información expuesta en su plataforma virtual pública. La investigación bibliográfica complementará el desarrollo de la matriz de riesgos, la misma que permitirá determinar de manera objetiva los riesgos que resultan relevantes en cuanto a la seguridad informática de la información alojada en la página web.

Tabla 1 Matriz de Riesgos de la Página web de la UTMACH

Factor de Riesgo	Probabilidad			Impacto			Nivel de Riesgo	Recomendaciones	Responsable
	B	M	A	B	M	A			
Falta de mantenimiento de Plataforma virtual		X				X	Alto	Mantener la actualización y mantenimiento de manera constante, de forma que se minimice la probabilidad de sufrir ataques informáticos, además se puede realizar inspecciones sorpresas.	Unidad de Sistemas de la Dirección de TIC
Inadecuada Exploración de Vulnerabilidades			X			X	Alto	Realizar la exploración de vulnerabilidades, tomando en cuenta las precauciones respectivas de tal forma que la información no se vea afectada al momento de quedar el sistema vulnerable.	Dirección de TIC
Inspección inadecuada del mantenimiento brindado a la plataforma	X					X	Bajo	Auditar el desempeño de la persona y de la dirección a cargo de la plataforma.	Empresa externa
Falta de verificación de la información publicada	X					X	Bajo	Verificar diariamente el contenido y calidad de la información alojada en la plataforma, para evitar inconformidades en los usuarios.	Unidad de Sistemas de la Dirección de TIC
Escasa evaluación de los protocolos de seguridad usados en la plataforma.		X			X		Medio	Evaluar constantemente el protocolo HTTPS y el certificado SSL para determinar el nivel de seguridad que brindan a la página web.	Unidad de Sistemas de la Dirección de TIC

La matriz de riesgos como se puede observar, muestra los riesgos, amenazas y vulnerabilidades más relevantes a los que está expuesta la plataforma virtual de la Universidad, representando estás un riesgo de que la plataforma pueda ser afectada; es importante indicar que cuando se realizan exploración de vulnerabilidades, la página web queda expuesta y propensa a sufrir ataques y amenazas virtuales pero tomando las precauciones y seguridad correcta se puede llevar cabo sin que el sistema informático se vea afectado.

La seguridad de la información universitaria, está a cargo de profesionales como se comprobó con el desarrollo de la entrevista. Según Muñoz & Rivas (2015) "Las organizaciones necesitan una estabilidad con un mayor grado de protección enfocada a la seguridad informática para proteger y minimizar las amenazas a su información" (pág. 13); puesto que la desinformación es el principal problema en una organización al momento de tomar decisiones, el establecer una buena seguridad en equipos de seguridad informática es imprescindible ya que de esta depende que se proporcione información eficaz y eficiente.

La importancia de proporcionar una información de calidad en los sitios web y al ser accedidos de forma online por varios usuarios, es lo que obliga a las empresas y organizaciones establecer políticas y herramientas de seguridad, de tal manera que se logre una buena imagen a través de ellos (Vega Oyola, Célleri Pacheco, & Maza Córdova, 2017, pág. 168).

Como ya se mencionó anteriormente la seguridad de la información en los sitios web depende tanto de los factores internos como externos por lo tanto se considera indispensable realizar un análisis FODA, de tal manera que se analice ambos factores y se concluya de esta forma el trabajo de investigación.

La matriz FODA permitirá identificar y analizar los factores internos es decir las fortalezas y las debilidades, y los factores externos oportunidades y amenazas en la plataforma web de la Universidad Técnica de Machala con la finalidad de tomar buenas decisiones en cuanto a la seguridad informática.

Tabla 2 Matriz FODA: Análisis de Resultados

FORTALEZAS	OPORTUNIDADES
• La UTMACH cuenta con protocolos de seguridad HTTPS y SSL, brindando seguridad a la información expuesta en la web. • El mantenimiento de la página web está a cargo de personal capacitado que es la Unidad de Sistemas de la Dirección de TIC. • Cuenta con políticas de seguridad en cuanto al proceso de información y uso correcto de equipos informáticos.	• Brinda confianza a los usuarios, además de que está encaminada al cumplimiento de su visión ser líder del desarrollo educativo. • El diseño, estructura y funcionalidad de la plataforma puede ser modificada por la Dirección de la Tecnología y Comunicación, realizando cambios que considere convenientes. • La seguridad de la página web está guiada a través de políticas que direccionan los procesos y usos correctos del software y hardware.
DEBILIDADES	**AMENAZAS**
• No se toman las medidas cautelares al momento de realizar una exploración de Vulnerabilidades, quedando el sistema expuesto a sufrir ataques. • Los requerimientos para el mantenimiento no llegan de manera directa, sino primero a la Dirección y es el director quien asigna las funciones al área pertinente. • Dentro de las políticas no se definen los controles que a los que está sujeta la plataforma virtual, ni las medidas que se deben considerar al momento de sufrir amenazas.	• Al ser una página pública es propensa a sufrir amenazas y ataques, ya que alguien con experiencia en informática puede fácilmente manipular la información que es publicada en el sitio web. • Sirve como medio de acceso a enlaces importantes que representan ser más vulnerables en comparación a la página web, como es el aula virtual, proceso de titulación, biblioteca y redes sociales. • La seguridad física es deficiente, en comparación a la seguridad lógica.

Como resultados de la matriz FODA tenemos que tanto los aspectos internos como externos, son necesarios e importantes para preservar la seguridad de la información, es así que dentro de lo interno muestra que la funcionalidad se encuentra a cargo de personas expertas en el área de informática, aunque es recomendable estar en constantes capacitaciones, debido a que, conforme avanza la tecnología los riesgos también evolucionan, además es recomendable incluir en sus políticas los controles de seguridad; (Mejia Miranda & Ramirez, 2016) menciona que estos se recomiendan implementar en

un sitio creado por wordpress, con el fin de proteger los tipos de ataques en sitios web, enfocados en memorias Caché, acceso seguro, bases de datos y copias de seguridad (pág. 2); por lo cual deben especificarse dentro de sus políticas y de igual forma ejecutarlos.

Monitorear el desempeño de la plataforma es vital puesto que un buen monitoreo provee la información necesaria para determinar que tanto se está cumpliendo con las políticas que se han implementado para la seguridad de la información en la Universidad Técnica de Machala (Vega de la Cruz, Orlando, Julbe, & Flor , 2016, pág. 15). Este se lleva a cabo mediante una gestión automatizada de un control de seguridad informática que implica la operación, monitorización y revisión del mismo, de forma automática (Miranda, Valdés, Pérez, Portelles, & Sánchez, 2016); sin embargo que su correcta funcionalidad se compruebe de manera física, revisando los informes y reportes que presente el sistema, es necesario y es donde interviene el personal capacitado y profesional con el que cuenta la Unidad de Sistemas de la Dirección de Tecnologías de Información y Comunicación.

Ilustración 1 Portal web de la UTMACH

3. CONCLUSIONES

- De acuerdo al análisis de la matriz de riesgos y la matriz FODA, en base a los resultados obtenidos de la entrevista, se determinó que la exploración de vulnerabilidades a más de indicar los riesgos a los que está expuesta una plataforma virtual, puede representar una amenaza si se realiza sin considerar las medidas precautelares al momento de ejecutarla; además, que una buena seguridad de información requiere de ambos tipos de seguridad: la física y la lógica, ya que el uso de ambas representan una credibilidad, integridad y confianza para la información.
- Al ser una plataforma virtual pública, debe estar monitoreada de manera constante, debido a que, sirve como portal de acceso al entorno virtual, biblioteca, sistema de titulación, centro de educación continua, entre otros, y los ataques que pueda sufrir afectarían a la información en ella expuesta y los enlaces que contenga.
- La página web de la Universidad Técnica de Machala, cuenta con la seguridad informática adecuada, ya que contiene protocolos HTTPS, certificados SSL y su actualización está a cargo de WORDPRESS, su mantenimiento, evaluación y funcionalidad es supervisada por la Unidad de Sistemas de la Dirección de TIC, la cual está conformada por personal capacitado; por lo cual se puede decir, que la institución no solo cuenta con tecnología idónea, sino que también su seguridad informática es acorde a su nivel y en función a los objetivos que desea alcanzar.

BIBLIOGRAFÍA

Arcentales Fernández, D., & Caycedo Casas, X. (2017). Auditoría Informática: un enfoque efectivo. *Revista Científica: Dominio de las ciencias, 3*, 157-173. doi:http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173

Darko, G., Darko, M., & Boris, G. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika: Journal for Control, Measurement, Electronics, Computing and Comunications (Taylor & Francis), 58*(3), 273-286. doi:DOI:10.1080/00051144.2017.1407022

Dirección de TIC Universidad Técnica de Machala. (2018). *Política General de Seguridad de la Información de la Universidad Técnica de Machala.* Obtenido de Universidad Técnica de Machala: https://www.utmachala.edu.ec/archivos/ley-transparencia-2015/Reglamentos/POLITICA%20GENERAL%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION.pdf

García, A., Cervigón Hurtado, & Alegre Ramos, M. (2012). *Seguridad Informática.* Editorial Paraninfo.

Gil Vera, V., & Gil Vera, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica (Redalyc), 22*(2), 193-197. Obtenido de http://www.redalyc.org/articulo.oa?id=84953103011

Gómez, R., Pérez, H., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería*, 109-118.

Hernández Saucedo, A., & Mejia Miranda, J. (Febrero de 2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *Revista electrónica de Computación, Informática Biomédica y Electrónica (Redalyc)*(1). Obtenido de http://www.redalyc.org/articulo.oa?id=512251501005

Martelo , R., Tovar, L., & Maza, D. (Febrero de 2018). Modelo básico de seguridad lógica. Caso de estudio: el laboratorio de redes de la Universidad de Cartagena en Colombia. *Revista Información tecnológica, 29*(1), 3-10. doi:http://dx.doi.org/10.4067/S0718-07642018000100002

Martínez, Blanco Alfonso, & Loy Marichal. (2013). Propuesta del Sistema de Acciones para la implementación de la Auditoría con Informática. *Revista de Arquitectura e Ingeniería (Redalyc), 7*(2), 1-13. Obtenido de http://www.redalyc.org/articulo.oa?id=193929227003

Mejia Miranda, J., & Ramirez, H. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. *Revista Ibérica de Sistemas y Tecnología de Información*, 1-15. doi:DOI: 10.17013/risti.17.1–15

Miranda, Valdés, Pérez, Portelles, & Sánchez. (2016). Metodología para la implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas*, 14-26. Obtenido de http://rcci.uci.cu

Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *Revista Ibérica de Sistemas y Tecnologías de Información*(222). doi:DOI: 10.17013/risti.e3.1-15

Ortega, S., & Canino, L. (2015). Protocolo de Seguridad SSL. *Revista Ingenieria Industrial (Redalyc), 27*(2-3), 57-62. Obtenido de http://www.redalyc.org/articulo.oa?id=360433561012

Parada, D., Flórez, A., & Gómez, U. (Febrero de 2018). Análisis de los componentes de la seguridad desde una perspectiva sistémica de la dinámica de sistemas. *29*(1), 27-38. doi:http://dx.doi.org/10.4067/S0718-07642018000100005

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*(20), 80-93. doi:DOI: http://dx.doi.org/10.17141/urvio.20.2017.2563

Porcile, Holland, Cimoli, & Rosas. (Septiembre-Diciembre de 2006). Especialización, tecnología y crecimiento en el modelo Ricardiano. *Nova Economía (Redalyc), 16*(3), 483-506. Obtenido de http://www.redalyc.org/articulo.oa?id=400437543005

República del Ecuador Asamblea General. (03 de Febrero de 2014). Código Orgánico Integral Penal COIP. Quito , Pichincha, Ecuador. Obtenido de http://www.epn.edu.ec/wp-content/uploads/2015/06/COIP1.pdf

Roba Iviricu, Vento Alvarez, & García Concepción. (Octubre-Diciembre de 2016). Metodología para la detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux. *Revista Científica Avances, 18*(4), 334-344.

Sobrino, W. (julio-diciembre de 2017). Los seguros de "Cyber risk" (A propósito del ciberataque mundial de fecha 12 de mayo de 2017). *Revista Ibero-Latinoamericana de seguros, 47*(26), 137-164. doi:doi:10.11144/Javeriana.ris47.lscr

Subijana Zunzunegui, I. (2008). *El ciberterrorismo: Una perspectiva legal y judicial* (Vol. 22). Eguzkilore. Obtenido de http://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf.

Vargas Borbúa , R., Recalde Herrera, L., & Reyes, R. (2017). Ciberdefensa y biberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanzza en ciberdefensa. *URVIO, Revista Latinoamericana de Estudios de seguridad*(20), 31-45. doi:DOI: http://dx.doi.org/10.17141/urvio.20.2017.2571

Vega de la Cruz, Orlando, L., Julbe, N., & Flor , A. (2016). Procedimiento para la Gestión de la Supervisión y Monitoreo del Control Interno. *Revista Ciencias Holguín (Redalyc), 22*(1), 1-19. Obtenido de http://www.redalyc.org/articulo.oa?id=181543577007

Vega Oyola, C., Célleri Pacheco, J., & Maza Córdova, J. (2017). Validación de una metodología de evaluación de calidad de sitios web: Caso de estudio UTMACH. *Revista Cumbres, 3*(1), 167-174.

Yasser , A.-B., & et al. (2014). Solución basada en el razonamiento basado en casos para el apoyo a las auditorías informáticas a bases de datos. *Revista Cubana de Ciencias Informáticas, 8*(2), 52-68. Obtenido de http://rcci.uci.cu

Zavaro Babani, León, Martínez García, & Caferino. (1999). *Auditoría Informática.* Cimex. La Habana: s.n.

ANEXOS

Señor/a entrevistado reciba un cordial saludo y un sincero agradecimiento por su colaboración para el desarrollo de la presente entrevista; su aporte permitirá continuar con el desenlace de mi investigación.

ANEXO 1 - ENTREVISTA

Entrevista realizada al encargado del departamento de Sistemas de la Universidad Técnica de Machala.
Ciudad y Fecha:
DATOS PERSONALES
Nombres y Apellidos:
C.I.:
Edad:
Sexo:
Profesión:
Cargo:
Función que desempeña en la institución de educación superior:

1. ¿El mantenimiento de la plataforma web quién la efectúa?
2. ¿El diseño, estructura y la calidad del contenido por quién fue realizado?
3. ¿A sufrido amenazas o ataques la plataforma, y de qué tipo?
4. ¿Cada que tiempo da mantenimiento y actualiza la página o su actualización es automática?
5. ¿El index de la página web es el correcto para su buen funcionamiento (Velocidad)?
6. ¿La seguridad de la plataforma es la correcta para evitar ataques y amenazas?
7. ¿La página web está alojada en un servidor compartido?
8. ¿Qué tan segura es la página web, como para ingresar datos personales?
9. ¿Hay una conexión o enlace desde la página web hacia las redes sociales?
10. ¿Ha existido alguna vez fuga de información?

ANEXO 2 - PLAN DE TRABAJO

No.	ACTIVIDAD	FECHA
1	Elección del caso práctico	29/11/2018
2	Estructuración del tema	06/12/2018
3	Ingreso preliminar a la página web de la UTMACH	06/12/2018
4	Recopilación de información, acorde al tema	08/12/2018
5	Establecer metodología y herramientas de trabajo	10/12/2018
6	Diseño de Entrevista	17/12/2018
7	Revisión de preguntas para la entrevista	20/12/2018
8	Ejecución de entrevista a la Ing. Betty Pachucho	28/12/2018
9	Identificación de Vulnerabilidades en base a datos obtenidos	02/01/2019
10	Análisis de datos obtenidos	03/01/2019
11	Redactar desarrollo en base a información obtenido de la investigación bibliográfica y entrevista	07/01/2019
12	Socializar informe con tutor	10/01/2019
13	Corrección de Informe	10/01/2019
14	Subir informe al drive compartido en el Sistema de Titulación	19/01/2019