UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

MEDIDAS DE SEGURIDAD INFORMÁTICA EN LA PLATAFORMA VIRTUAL DE LA UTMACH ENTORNO A PHISHING, MALVERTISING, PHARMING E INYECCIÓN SQL

FALCONI CABRERA ANDREA ELIZABETH
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

MEDIDAS DE SEGURIDAD INFORMÁTICA EN LA PLATAFORMA VIRTUAL DE LA UTMACH ENTORNO A PHISHING, MALVERTISING, PHARMING E INYECCIÓN SQL

FALCONI CABRERA ANDREA ELIZABETH
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

MEDIDAS DE SEGURIDAD INFORMÁTICA EN LA PLATAFORMA VIRTUAL DE LA UTMACH ENTORNO A PHISHING, MALVERTISING, PHARMING E INYECCIÓN SQL

FALCONI CABRERA ANDREA ELIZABETH
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 26 DE AGOSTO DE 2019

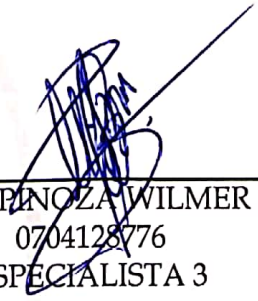
MACHALA
26 de agosto de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado MEDIDAS DE SEGURIDAD INFORMÁTICA EN LA PLATAFORMA VIRTUAL DE LA UTMACH ENTORNO A PHISHING, MALVERTISING, PHARMING E INYECCIÓN SQL, 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

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2



ILLESCAS ESPINOZA WILMER HENRY
0704128776
ESPECIALISTA 3

Fecha de impresión: lunes 26 de agosto de 2019 - 13:55

URKUND

Urkund Analysis Result

Analysed Document:	ANDREA FALCONI.docx (D54792040)
Submitted:	8/13/2019 3:35:00 AM
Submitted By:	jgonzalez@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, FALCONI CABRERA ANDREA ELIZABETH, en calidad de autora del siguiente trabajo escrito titulado MEDIDAS DE SEGURIDAD INFORMÁTICA EN LA PLATAFORMA VIRTUAL DE LA UTMACH ENTORNO A PHISHING, MALVERTISING, PHARMING E INYECCIÓN SQL, 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, 26 de agosto de 2019

FALCONI CABRERA ANDREA ELIZABETH
0704398106

DEDICATORIA

A Dios, primeramente por ser el inspirador y darme fuerza para continuar en este proceso de obtener uno de los anhelos más deseados, el cual me permitió culminar con éxito esta etapa de mi vida.

A mis padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes hemos logrado llegar hasta aquí y convertirme en lo que soy. Ha sido el orgullo y el privilegio de ser su hija, son los mejores padres.

A mis hermanas (os) por estar siempre presentes, acompañándome y por el apoyo moral, que me brindaron a lo largo de este camino.

A mi hija por ser el motor fundamental de mi vida, la razón de levantarme cada día y esforzarme por el presente y el mañana, eres mi principal motivación.

Y amigas que gracias a su apoyo, y conocimientos hicieron de esta experiencia una de las más especiales en esta etapa.

Autora: Andrea Elizabeth Falconí Cabrera

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presentes.

Mi profundo agradecimiento a todas las autoridades y personal que hacen la Universidad Técnica de Machala, por confiar en mí, abrirme las puertas y permitirme realizar todo el proceso investigativo dentro de su establecimiento educativo.

De igual manera mis agradecimientos a mis profesores quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada una de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Finalmente quiero expresar mi más grande y sincero agradecimiento al Ing. Jorge Luis González Sánchez, principal colaborador durante todo este proceso, quien con su dirección, conocimiento, enseñanza y colaboración permitió el desarrollo de este trabajo.

Autora: Andrea Elizabeth Falconí Cabrera

RESUMEN

Actualmente la era tecnológica se ha posesionado de manera imperiosa, al sector productor, comercial, educativo, los que principalmente han acogido las nuevas tecnologías y acoplado a su sistema de trabajo, esto se debe a las grandes ventajas que tales tecnologías ofrecen. En el sector de producción utilizan maquinarias que facilitan el trabajo, el sector comercial se ve influenciado por tecnologías que se encargan de manejar el proceso de publicidad, compra y venta de artículos, entre otros. Por otro lado, el sector educativo con el fin de mejorar las técnicas de enseñanza y ampliar los campos que proporcionen información a los estudiantes han hecho uso de las TIC's para satisfacer esta necesidad. Tal es el caso que han implementado plataformas virtuales mediante las cuales el proceso de enseñanza – aprendizaje ha tenido cambios considerables, mostrando mejoras en el sistema, volviéndolo más versátil además de proporcionarle al cuerpo estudiantil más y mejores fuentes de información. No obstante, existen ciertos peligros que rodean a las plataformas virtuales, para los cuales existen medidas de prevención y/o mitigación; se pretende explicar algunas medidas llevadas dentro de la plataforma virtual de la UTMACH a fin de protegerla ante peligros como el Phishing, Malvertising, Pharming e Inyección SQL.

PALABRAS CLAVES: Plataforma virtual, Phishing, Malvertising, Pharming, Inyección SQL.

ABSTRACT

At the moment the technological era has been imperatively possessed, to the producer, commercial, educational sector, those that have mainly welcomed the new technologies and coupled to their work system, this is due to the great advantages that tales available technologies. In the production sector we use machines that facilitate work, the commercial sector is influenced by technologies that handle the process of advertising, buying and selling items, among others. On the other hand, the education sector in order to improve teaching techniques and expand the fields that provide information to students who have used ICT to meet this need. Such is the case that they have implemented virtual platforms through any teaching-learning process has had considerable changes, showing improvements in the system, making it more versatile as well as providing the student body with more and better sources of information. However, there are certain dangers surrounding virtual platforms, for which there are prevention and / or mitigation measures; It is intended to explain some measures carried out within the UTMACH virtual platform in order to protect it against dangers such as Phishing, Malvertising, Pharming and SQL Injection.

KEYWRDS: Virtual Platform, Phishing, Malvertising, Pharming, SQL Injection.

ÍNDICE GENERAL DE CONTENIDOS

Pág.

ÍNDICE DE GRÁFICOS

Pág.

ÍNDICE DE CUADROS

Pág.

1. INTRODUCCIÓN

Es importante destacar que, para cada organización sea cual sea la función que desempeña, necesita ejecutar procesos que regulen el funcionamiento de sus operaciones y actividades.

Actualmente en la mayoría de establecimientos es muy común encontrar Tecnologías inmersas en el sector de la producción, logística de la empresa y en el manejo de información, estas TIC's brindan muchas posibilidades y beneficios a la empresa, puesto que con el uso de maquinaria sofisticada, el número de empleados se reduce considerablemente, por ende se reduce también el pago de salarios, además se ha demostrado que el uso de tecnologías optimiza el desarrollo de actividades, ejecutándolas en menor tiempo y de manera más eficiente.

El uso de Tecnologías de Información y Comunicación hace que el mundo se mueva a un paso acelerado logrando avances nunca antes vistos, lamentablemente todo este beneficio se ve opacado por ciertos riesgos a los que se exponen los sistemas informáticos, servidores o plataformas web. Para controlar que estas amenazas no causen daños irreparables a los sistemas o a la información que estos manejan, se ha creado una serie de procesos que llevados a cabo son capaces de intervenir y mejorar la situación; estos procesos se denominan auditorías informáticas, cuyo objetivo se basa en la identificación y posterior mitigación de amenazas informáticas.

La incorporación de TIC's a los ámbitos educativos es muy común, tanto así que no solamente son herramientas de ayuda, sino más bien esenciales en el proceso de enseñanza – aprendizaje (Santiso, Koller, & Bisaro, 2016).

Como derivación de esto, las plataformas educativas se enfrentan a nuevos riesgos informáticos que pueden afectar la seguridad de los sistemas informáticos. Entonces, se dice que cada auditoría ejecutada responde a la necesidad de proteger la información contenida dentro de estas plataformas.

En la UTMACH para el desarrollo de las actividades académicas virtuales, se trabaja con algunas plataformas virtuales que facilitan la interacción entre alumno y profesor, el aula virtual es una de ellas, pues permite subir información al estudiante además de participar en foros o enviar mensajes y responderlos en tiempo real, otra plataforma muy utilizada es el llamado SIUTMACH, que contiene información de la vida académica del alumno como calificaciones, registro de matrícula.

Estas plataformas cuentan con su propio sistema de control y vigilancia, mediante el cual se puede tomar medidas preventivas y de seguridad ante amenazas latentes en el medio (Romero, 2010).

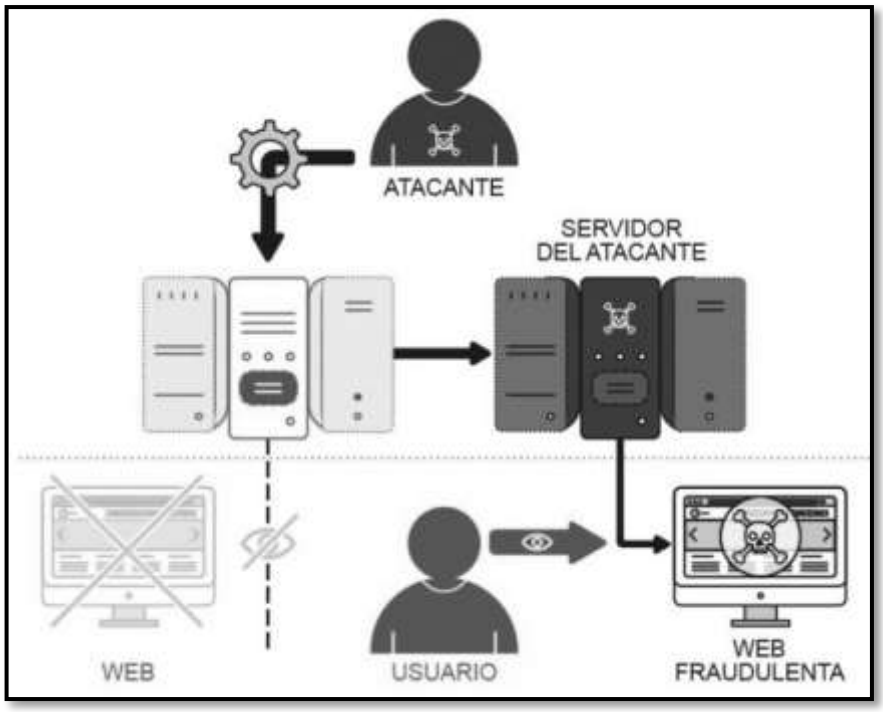
Cuadro 1. Categorización de las amenazas informáticas

AMENAZAS INFORMÁTICAS	
Errores humanos	Mal uso de equipos, mal manejo de software
Fallos en el sistema informático	Programas obsoletos, desactualización del sistema
Factores ambientales (desastres)	Tormentas, huracanes, nevadas fuertes, olas de calor
Actuación maliciosa	Robo de información, fraude, malversación

Fuente: (Figueroa, Rodríguez, Bone, & Saltos, 2017)

Sin embargo, estas plataformas pueden estar amenazadas por muchos problemas tecnológicos como: virus informáticos, phishing, malvertising, pharming e inyección SQL; que de no ser atendidos a tiempo y de manera adecuada, podrían ser los causantes, en el peor de los casos, de la destrucción de la información (Roque & Juárez, 2018).

Gráfico 1. Esquematización del Pharming.



Fuente: (Corchado, 2017)

2. DESARROLLO

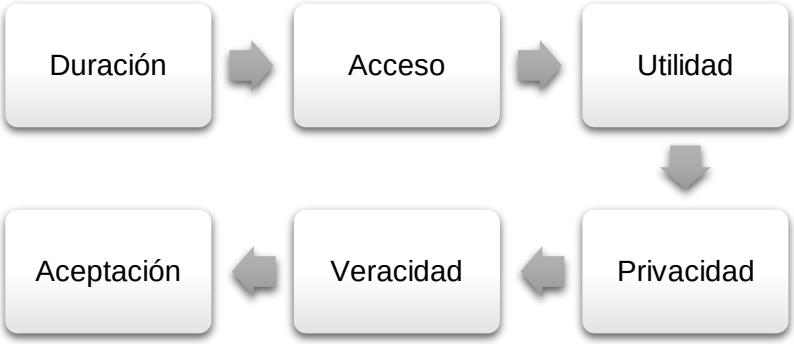
2.1 FUNDAMENTACIÓN TEÓRICA

En este apartado se describe la terminología que explica el desarrollo de la temática planteada, toda la información contenida en esta sección ha sido tomada de artículos de revistas científicas y en algunos casos se ha tomado la información de tesis desarrolladas con temas similares.

2.1.1 *Seguridad informática* Se refiere al estado de control de la información que se maneja, el objetivo de la seguridad informática es minimizar cualquier amenaza o riesgo a la que posiblemente podrían exponerse los recursos informáticos de la organización. Lo que busca con esto, es asegurar la continuidad de los procesos operacionales de la entidad, aun cuando se estén ejecutando medidas de mitigación de riegos o ataques informáticos (Quiroz & Macías, 2017).

Además, se pretende mantener la privacidad de la información, cuidando que no exista filtración o mal manejo de ella, pues en el medio digital existe gran variedad de piratas informáticos que con sus conocimientos son capaces de acceder a sistemas privados para robar información a cambio de dinero o de adquirir poder mediante la sustracción de dicha información.

Gráfico 2. Características de la confidencialidad.



Fuente: (Quiroz & Macías, 2017)

La seguridad informática agrupa una serie de técnicas empleadas para protección de la información y los sistemas informáticos de una determinada entidad, se busca esta protección ante posibles ataques que pudieran ocurrir, sean originados por alguien o simplemente al ser productos de un accidente. La seguridad informática puede dividirse o clasificarse en las siguientes unidades:

Cuadro 2. Clasificación de la seguridad informática

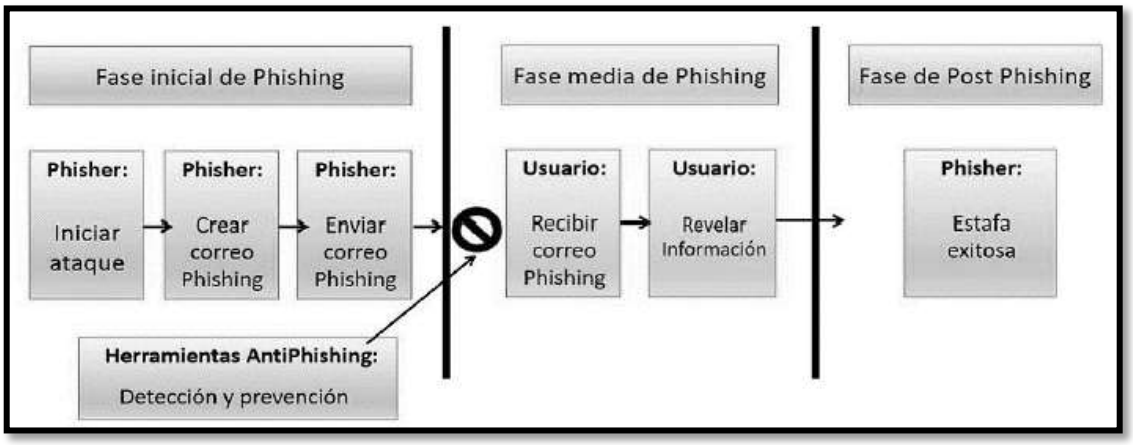
CLASIFICACIÓN DE LA SEGURIDAD INFORMÁTICA	
Seguridad Física	Cuida que el manejan el ordenador o los equipos informáticos sean manejados por personal autorizado y con suficiente conocimiento para hacerlo.
Seguridad lógica	Controla el libre acceso a la información o a las plataformas virtuales, protege la integridad de los datos.
Recuperación de datos	Brinda los parámetros necesarios para manejar sistemas de recuperación de datos. Admite la recuperación de información perdida o alterada.
Disposición de recursos	Cuida que los recursos o datos informáticos contenidos en sus servidores estén disponibles para su utilización en cualquier momento que se requiera.
Políticas de Seguridad	Normas, leyes y preceptos que regulan el uso de los recursos informáticos dependiendo de las necesidades de la entidad.
Análisis forense	Consecuencia del estudio de incidentes originados en las entidades por causa de la seguridad informática. Busca proveer los datos de quien originó tal ataque.

Fuente: (Acurio Del Pino, 2015)

2.1.2 ***Phishing*** Es una forma empleada por piratas informáticos para robar o malversar información, utilizando como medio una dirección de correo electrónico que a simple vista parece ser legal. Dicho correo contiene un link que lleva al usuario a un sitio inexistente pero que tiene similitud con el real, una vez ahí, es posible para el ciber atacante robar información confidencial, como: contraseñas, información privada, números de cédula, tarjetas de crédito, etc.

El phishing pertenece a un grupo de amenazas informáticas, que, al igual que las TIC's han tenido un avance en cuanto a su concepción, pues en tiempos anteriores se dice que la identificación de estos correos maliciosos era más sencilla a la que se puede dar ahora, debido a que ha mejorado la calidad en la falsificación, su diseño y presentación supera por mucho la calidad que antes presentaban (Roque & Juárez, 2018).

Gráfico 3. Proceso de ataque de Phishing



Fuente: (Hernández Dominguez & Storchak, 2018)

Para atenuar los ataques informáticos de Phishing se ha ideado algunos instrumentos útiles en la detección de la amenaza, se los puede subdividir en tres grupos. El primero incluye la parte educativa y legal, en donde se establecen las normativas concebidas dentro de un marco legal, ya sea de la empresa o del circuito al que pertenezca, en este mismo estado se puede establecer si existe alguna condena por tráfico y robo de información privada. Se establecen también agrupaciones especializadas en detectar problemas o riesgos informáticos, en base a conocimientos previos (Hernández & Storchak, 2018).

El segundo grupo es el desarrollo computacional que aplica técnicas semi – automáticas: en la actualidad existen medidas que empresas privadas como Outlook o Gmail (más conocidas) emplean para clasificar correos que consideran “peligrosos” para el usuario, ya sea por su procedencia o su contenido; toman la medida preventiva de clasificarlos en la lista de “Correos no deseados” o “Spam”. No está de más mencionar que esta medida no siempre funciona como debería, pues, ocasionalmente suele atrapar correos no peligrosos y colocarlos dentro del grupo.

La tercera agrupación se trata sobre los métodos de Machine Learning o aprendizaje automático empleados en la detección de amenazas de Phishing, mediante las características que se observan en el correo electrónico que origina el ataque (Hernández Dominguez & Storchak, 2018).

2.1.3 *Malvertising* El Malvertising representa la publicidad que contiene códigos maliciosos, los cuales están ocultos detrás de anuncios en línea, que en determinado

momento son entregados a los usuarios, quienes confiados de que ingresan a un sitio web seguro, están adquiriendo elementos maliciosos para su seguridad informática.

Para controlar las amenazas informáticas presentes en el medio, se debe tener la precaución de no ingresar a sitios con apariencia sospechosa o a correos electrónicos cuya procedencia sea dudosa o desconocida.

Por ello, es conveniente acceder solamente a sitios genuinos y legales que pueden ser identificados de manera independiente (Dwyer & Kanguri, 2016).

El malvertising es la unión de dos palabras “malware” y “advertising”, que traducidos significan “anuncio o publicidad maliciosa”. Se inserta en anuncios publicitarios de manera secreta e infecta los servidores aun sin la necesidad de que el usuario de clic sobre el anuncio.

El malvertising puede estar en cualquier sitio web que contenga anuncios publicitarios, es muy común encontrarlo en sitios donde su funcionamiento es completamente legal como: descarga de música o películas, pero en los últimos tiempos este fenómeno ha empezado a ocurrir en plataformas menos comunes como Spotify, Amazon, YouTube e incluso a ciertos medios de comunicación como MSN, el NYT y la BBC.

Gráfico 4. Categorías de sitios web más utilizadas.

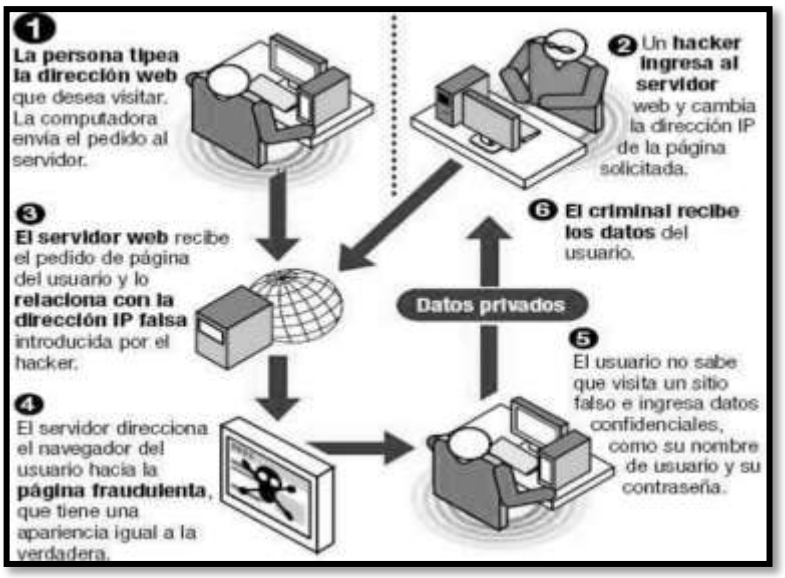
Fuente: (Invitados, 2012)

2.1.4 *Pharming* Este delito informático es una innovación del Phishing, mucho más difícil de detectar y con mejores cualidades para cometer fraude; tiene la característica de conducir al usuario a un sitio fraudulento, aunque siempre se escriba una dirección correcta.

El Pharming ataca los Servidores DNS (Sistema de Resolución de Nombres de Dominio) que es el encargado de traducir a un lenguaje informático, todo lo que externamente se escribe desde una dirección IP determinada, ataca también a los archivos Hosts, cuya característica es bloquear páginas, aumentar la velocidad del equipo en el que está instalada, etc., el ataque de Pharming se da al momento en que el delincuente modifica el archivo Hosts para que redireccione al usuario a un sitio similar al original, pero alterado para obtener datos de interés del atacante.

En resumen, el Pharming es la "modificación de los nombres de usuarios en internet" originado por un código malicioso introducido en el ordenador al momento de realizar una descarga desde un correo no deseado (Callegari, 2016).

Gráfico 5. Proceso de desarrollo del Pharming.



Fuente: (Martínez García, 2009)

Se diferencia del Phishing porque en contraste con éste en donde se necesita que el usuario actúe ingresando a una página dirigido por un link que le proporcionan, en el Pharming el usuario ingresa normalmente a una página web "segura" que puede ser que de uso ocasional, pero cuyo DNS está modificado por algún programa creado por un pirara informático, lo que causa el redireccionamiento de la IP que termina llevándolo a una página fraudulenta con el fin de acceder a información privada (Callegari, 2016).

2.1.5 Inyección SQL Esta afectación de seguridad informática tiene el objetivo de perjudicar las aplicaciones web, ocurre al insertar un código SQL a través de cualquier

entrada proporcionada por el cliente, la cual permite leer la interfaz y realizar modificaciones de la interfaz (Iñiguez, Guaman, Figueroa, & Ajila, 2016).

Un ataque de tipo inyección SQL se dirige a cambiar o modificar el propósito original de la solicitud que se maneje, a través de la inserción de la sentencia SQL dada por el atacante, que afecta directamente a la base de datos.

El ataque SQL puede tener éxito dependiendo de la aplicación en donde se origine y de la rapidez de procesamiento de datos que esta tenga, los alcances pueden ir desde la infección de la aplicación, hasta la verificación que permite propagar información hacia los demás usuarios de la aplicación, que facilite la distribución del código malicioso (De La Quintana Illanes, 2017).

2.2 Metodología

En esta sección se detalla la metodología empleada en la búsqueda y procesamiento de información necesaria para desarrollar la temática planteada, estas técnicas se describen a continuación:

2.2.1 ***Investigación Documentada*** La investigación documental es una doctrina instrumental de carácter metodológico. Su desarrollo proviene de la búsqueda de información teórica que posteriormente debe ser respaldada por la métodos o teorías científicas (Tancara, 2017).

Lo que quiere decir que la búsqueda de información debe ser siempre basada en documentación probada y fundamentada en bases científicas, por lo que es importante verificar la fuente de donde se extrae la información a fin de cumplir con este requerimiento.

2.2.2 ***Método inductivo – deductivo*** Este método se fundamenta en el conocimiento de un tema en particular, mediante el estudio del cual, se obtiene una conclusión global; el uso de este método se basa en el análisis de cada parte que integra un caso general, buscando relacionar cada característica encontrada para explicar dicho fenómeno. Esencialmente se busca encontrar ciertos parecidos o características que relacionen cada elemento dentro del grupo, algo que lleve a la formulación de una conclusión que englobe los aspectos determinantes de dicho grupo (Rodríguez & Pérez , 2017).

2.2.3 ***Método analítico:*** Este método es el encargado de disgregar de manera casi mental un tema global, especificando sus partes propiedades o características, etc.,

realiza este proceso con la intención de poder analizar y conocer las peculiaridades de cada parte por separado. Una vez realizado este proceso, se presenta resultados que expliquen el origen o consecuencia del porqué sucede determinado caso.

2.3 Procesos

En el marco del desarrollo de los procesos administrativos de una empresa, es importante realizar evaluaciones a los sistemas que lo conforman de manera periódica; es así que mediante procesos denominados auditorias informáticas, se espera conocer las falencias de los sistemas que conforman la empresa y de esta forma poder contrarrestarlas para que no afecten a la organización.

2.3.1 ***Plataformas virtuales utilizadas en la UTMACH*** La Universidad Técnica de Machala (UTMACH), en calidad de centro de educación superior, busca siempre implementar tecnologías que de alguna manera ayuden a la mejora de los procesos de enseñanza – aprendizaje, generando mejores resultados como la acreditación y crecimiento a nivel institucional.

La inserción de TIC's en los procesos educativos es una premisa que define la calidad de educación que se pretende otorgar a la sociedad; el uso de plataformas virtuales versátiles y de fácil manejo son el principal recurso con el que cuenta la Universidad.

Gráfico 6. Página de entrada e inicio de sesión del Aula virtual de la UTMACH.

Fuente: (UTMACH, Moodle UTMACH, 2019)

Plataformas como el Aula virtual (Moodle), el Repositorio Digital (DSpace), a más de servicios como el SIUTMACH y la Biblioteca Digital son las principales herramientas

empleadas por la Universidad Técnica de Machala para el desarrollo de sus actividades académicas.

Gráfico 7. Página de inicio del SIUTMACH.

Fuente: (UTMACH, SIUTMACH, 2019)

Gráfico 8. Página de inicio del Repositorio Digital.

Fuente: (UTMACH, Repositorio Digital de la UTMACH, 2019)

2.3.2 ***Medidas de seguridad informática*** Para mantener un correcto control y adecuado manejo de la información se debe desarrollar medidas que regulen el buen funcionamiento de los sistemas informáticos, a continuación, se describen algunos:

2.3.3 Implementación de políticas de seguridad Es importante estableces un conjunto de reglas o políticas de la empresa que anteriormente hayan sido aprobadas por la administración de la entidad a la que pertenecen.

2.3.4 Repartición de responsabilidades en el control de la seguridad Se debe asignar la ejecución de tareas a quienes conforman el equipo de trabajo, para que en caso que ocurra alguna novedad respecto a la seguridad, haya quienes respondan en un área en específico.

2.3.4 Auditorias de seguridad informática Deben planificarse previamente, para que su ejecución sea óptima y pueda detectar amenazas latentes en el medio, proporcionando observaciones eficientes que permitan tomar mejores decisiones en cuanto a la mitigación de ataques informáticos.

2.3.5 Capacitación al personal Ninguna medida de prevención funciona totalmente si el personal que la ejecuta no tiene noción de su funcionamiento, por ello es importante la capacitación.

2.3.6 Reporte de incidentes En toda organización debe existir un lugar en donde pueda reportar algún incidente en el desarrollo de los procesos preventivos y de seguridad informática.

2.3.7 Recuperación Se debe ejecutar algún plan que permita recuperar la información q ya no está disponible.

2.3.8 Acatamiento de leyes Revisar la normativa y leyes que se asocien al desempeño de actividades relacionadas a la funcionalidad de la organización (Santiso, Koller, & Bisaro, 2016).

2.4 Control de Phishing en las plataformas virtuales

El Phishing es una amenaza importante a la que se enfrentan las plataformas virtuales y los servidores web, pues con engaños fácilmente se puede filtrar información privada y caer en manos equivocadas.

Este tipo de ataque consiste en la remisión de correos falsos desde direcciones de correo electrónica supuestamente pertenecientes a instituciones legales, pidiéndole a

la víctima, datos personales, generalmente relacionados a términos económicos (García , 2018).

Con el fin de proteger tal información, las plataformas virtuales emplean ciertas medidas de control y autenticación que hacen que el usuario sienta más confianza al utilizar determinada plataforma o sitio web. El inicio de sesión utilizando un usuario y contraseña, elaboración de un sistema especializado en diferenciar las características de un correo real que permita determinar cuándo es un correo dañino de phishing, un algoritmo que utilice técnicas anti – phishing, detección de phishing basándose en la clasificación de enlaces, entre otros.

Todas estas medidas de control han sido planificadas con el objetivo de detectar y mitigar los ataques informáticos por phishing (Sastoque & Botero, 2015).

Cuadro 3. Métodos para detectar el Phishing

TÉCNICAS PARA DETECTAR PHISHING	
Inicio de sesión	Contenido relacionado al anti – phishing
Sistema basado en páginas web reales, para detectar sitios de phishing	Definir los ataques de phishing identificando dos fases
Categorización de enlaces	Detección de páginas contaminadas relacionadas con paginas existentes
Prevención de ataques basándose en propiedades similares	Utilización de algoritmos de minería de datos.

Fuente: **(Sastoque Mesa & Botero Tabares, 2015)**

2.5 Medidas de control de Malvertising y Pharming

La publicidad maliciosa o Malvertising es un tipo de ataque informático que está conformado por códigos maliciosos escondidos dentro de anuncios que a simple vista parecen inofensivos y completamente legales, pero que internamente son capaces de afectar un sistema completo.

Para controlar esta amenaza, se puede instalar un antivirus potente o realizar la actualización de uno que se tenga vigente, también resulta útil la instalación de un

bloqueador de publicidad que ayudará a ocultar la publicidad justo antes de que pueda ser visualizada en pantalla.

Es conveniente tener actualizado el navegador, porque un problema suele ser que se dan ataques por fallos en la respuesta del navegador, lo que origina la publicación de anuncios que más tarde resultan maliciosos.

Mantener actualización de complementos es otra forma de combatir el malvertising, pues éstos podrían mostrar si existe alguna alteración en el sistema de seguridad, pero para ello es necesario contar con versiones actualizadas que certifiquen su eficacia.

El Pharming es una evolución del Phishing, más sofisticado y con más usabilidad; se trata de un peligro informático difícil de detectar debido a la casi imperceptible forma de actuar, modifica archivos Hosts con el fin de enviar al usuario a un sitio fraudulento que le sustraiga la información personal que posteriormente puede ser utilizada con fines maliciosos.

Si se recibe links de acceso a través de algún correo electrónico, es preferible que se ingrese a este de manera directa digitando la dirección electrónica manualmente e ingresando por el sitio principal.

Si se tiene dudas sobre la procedencia de la publicidad mostrada, no dar clic en anuncios (Kovacs, 2015).

Gráfico 9. Consejo de Norton Comunity acerca del Malvertising.

Fuente: (Kovacs, 2015)

Las medidas preventivas que podrían tomarse para controlar este tipo de situaciones son:

- Si se recibe correos de dudosa procedencia se los debe denunciar a algún organismo de control informático.
- No abrir correos desconocidos, sin remitente o sospechosos.
- Instalar antivirus, softwares de protección y detección de espías informáticos.
- No responder enviado información privada de ningún tipo, a correos desconocidos.
- No realizar descargas de archivos desde correos o direcciones web sospechosos.
- Además, si se cree que el equipo está en riesgo, es conveniente realizar verificaciones de Hosts, limpieza de registros, pasar antivirus, entre otros.
    - Se puede instalar una aplicación para Windows llamada DNSHostMonitor, este script de Visual Basic brinda la posibilidad de rastrear archivos Hosts a tiempo real para detectar cualquier cambio que pudiera ocurrirle, no pesa demasiado ni consume demasiados recursos del ordenado y da la opción de iniciar Windows con o sin ella (Martínez, 2009).
    - Otra opción es la instalación de un software especialista en el tema, Green Armor es un software que detecta y notifica si el sitio en donde se está navegando es un sitio legal o si es una modificación de este. Es de fácil funcionamiento y se integra de manera fácil para trabajar con perfil bajo verificando la legitimidad del usuario y de la página en donde se está navegando (Callegari, 2016).

Gráfico 10. Green Armor.

Fuente: (Callegari, 2016)

2.6 Incidencia de la Inyección SQL en los entornos educativos

Las plataformas virtuales empleadas en el proceso de enseñanza – aprendizaje tanto en institutos como en universidades, tienes muchas ventajas que generan gran aceptación en ese ámbito, pero existe a menudo una serie de riesgos informáticos que, de no ser prevenidos o mitigados a tiempo, estas plataformas pueden sufrir graves altercados.

La información contenida en las plataformas web institucionales, generalmente está a disposición de los usuarios con solo identificarse y proporcionar una contraseña; en este artículo se ha visto algunos de los posibles ataques informáticos que podrían sufrir, entre ellos la inyección SQL que ocurre cuando se envían datos no codificados a un intérprete en forma de consulta, y éste al ejecutar ciertos comandos o abrir accesos no autorizados, podría sufrir el ataque.

Las bases de datos son fáciles de fácil rastreo por lo que se dice que los ataques de inyección SQL son fáciles de administrar; los ataques pueden darse en diferentes formas, por ejemplo:

Acceso a la plataforma mediante brechas en la entrada de usuarios: que sucede cuando el usuario va a identificarse e ingresa un usuario y una contraseña; existen ciertos scripts que verifican la autenticidad de la información, mismos que pueden ser vulnerados por ciber atacantes (De La Quintana Illanes, 2017).

Robo de datos a través del manejo de ID: sucede cuando existe espionaje mediante la solicitación de información utilizando un identificador, que generalmente representa la entrada más potencial para recibir un ataque de inyección SQL.

3. CONCLUSIONES

- Actualmente la tecnología está distribuida alrededor de mundo, hay lugares donde su incidencia es mayor que en otros, y también hay sectores en donde su utilización es más requerida. El sector de la educación es un claro ejemplo de ello, implementa su sistema educativo con nuevas tecnologías que le brindan la posibilidad de proporcionar mejor servicio académico; la UTMACH es un ejemplo de ello, porque tras la utilización de importantes plataformas virtuales hace que el proceso de aprendizaje ser más didáctico e interactivo.
- La utilización de servicios web, ocasiona vulnerabilidades en el sistema informático debido a la disponibilidad de la información en la web que causa curiosidad e interés en las personas ajenas a la institución, un factor que ocasiona preocupación al saber que los datos privados están siempre en constante amenaza. Para lo cual se toma medidas preventivas que desarrolladas de manera correcta pueden salvar información valiosa.
- Los ataques informáticos como Phishing, Malvertising, Pharming y la inyección SQL constituyen una potencial amenaza a la información privada de cualquier institución, por lo cual se han revisado una serie de medidas que podrían llevarse a cabo a fin de poder minimizar estas amenazas.

BIBLIOGRAFÍA

Acurio Del Pino, S. (2015). *Delitos Informáticos: Generalidades.* Guayaquil: PUCE.

Callegari, O. (2016). Delitos informáticos: Pharming. *Revista Negocios de Seguridad*, 176-180.

Corchado, B. (25 de enero de 2017). *GoDaddy.* Obtenido de https://es.godaddy.com/blog/que-es-el-phishing-y-que-tipos-existen/

De La Quintana Illanes, M. M. (2017). *SQL Inyection.* La Paz: Universidad Mayor de San Andrés.

Dwyer, C., & Kanguri, A. (2016). Malvertising - A Rising Threat To The Online Ecosystem. *Information Systems & Computing Academic Professionals*, 1-7.

Figueroa Suárez, J. A., Rodríguez Andrade, R. F., Bone Obando, C. C., & Saltos Gómez, J. A. (2017). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*, 145-155.

García García, D. E. (2018). El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de Enero. *Revista Bolivariana de Derecho*, 650-659.

Hernández Dominguez, A., & Storchak, S. (2018). Sistema para la detección de ataques Phishing utilizando correo electrónico. *Revista Telemática*, 60-70.

Invitados, A. (31 de octubre de 2012). *Sociable Blog*. Obtenido de http://www.sociableblog.com/2012/10/31/beware-of-malware-its-everywhere-infographics/

Iñiguez Banegas, J., Guaman Quinche, R., Figueroa Diaz, R., & Ajila Zaquinaula, F. (2016). Revisión Sistemática de Literatura: Inyección SQL en Aplicaciones web. *LATIN AMERICAN JOURNAL OF COMPUTING*, 65-72.

Kovacs, N. (25 de noviembre de 2015). *Norton Comunity*. Obtenido de https://community.norton.com/es/blogs/norton-protection-blog/%C2%BFque-es-malvertising

Martínez García, H. A. (2009). *PHISHING Y PHARMING: Robo de datos y suplantación de identidad en internet.* Yucatán: Instituto Tecnológico Superior Progreso.

Quiroz Zambrano, S. M., & Macías Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Dominio de las ciencias*, 676-688.

Rodríguez Jiménez, A., & Pérez Jacinto, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Escuela de Administracón de Negocios*, 1-26.

Romero Moreno, L. M. (2010). La seguridad informática en el trabajo con la plataforma Moodle. *Revista de Humanidades*, 171-190.

Roque Hernández, R. V., & Juárez Ibarra, C. M. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. *Paakat: Revista de Tecnología y Sociedad*, 1-13.

Santiso, H., Koller, J. M., & Bisaro, M. G. (2016). Seguridad en Entornos de Educación Virtual. *Memoria Investigaciones en Ingeniería*, 67-88.

Sastoque Mesa, D., & Botero Tabares, R. (2015). Técnicas de detección y control de phishing. *Cuaderno Activa*, 75-81.

Tancara, C. (2017). La investigación documental. *Revistas Bolivarianas*, 91-106.

UTMACH. (1 de julio de 2019). *Moodle UTMACH*. Obtenido de https://moodle.utmachala.edu.ec/cursosvirtuales/

UTMACH. (1 de julio de 2019). *Repositorio Digital de la UTMACH*. Obtenido de http://repositorio.utmachala.edu.ec/

UTMACH. (1 de julio de 2019). *SIUTMACH*. Obtenido de https://app.utmachala.edu.ec/siutmach/public/