UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE VULNERABILIDADES DEL SISTEMA INFORMÁTICO PARA RENDIR EXAMEN COMPLEXIVO EN LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH.

PONTON QUEVEDO GEANELA DEL CISNE
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE VULNERABILIDADES DEL SISTEMA INFORMÁTICO PARA RENDIR EXAMEN COMPLEXIVO EN LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH.

PONTON QUEVEDO GEANELA DEL CISNE
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE VULNERABILIDADES DEL SISTEMA INFORMÁTICO PARA RENDIR EXAMEN COMPLEXIVO EN LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH.

PONTON QUEVEDO GEANELA DEL CISNE
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 del sistema informático para rendir examen complexivo en la Unidad Académica de Ciencias Empresariales de la UTMACH., 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 - 12:40

Urkund Analysis Result

Analysed Document:	PONTON QUEVEDO GEANELA DEL CISNE_PT-011018.pdf (D47096122)
Submitted:	1/22/2019 4:18:00 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, PONTON QUEVEDO GEANELA DEL CISNE, en calidad de autora del siguiente trabajo escrito titulado Análisis de vulnerabilidades del sistema informático para rendir examen complexivo en la Unidad Académica de Ciencias Empresariales de la UTMACH., 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

PONTON QUEVEDO GEANELA DEL CISNE
0706442290

RESUMEN

El desarrollo de la presente investigación cuenta con el propósito de analizar las vulnerabilidades que existen en el actual sistema informático de la Unidad Académica de Ciencias Empresariales para la presentación del examen complexivo dimensión teórico, identificando posibles vulnerabilidades, amenazas y riesgos a los que se encuentra expuesta la información de los estudiantes egresados en proceso de titulación de la Universidad Técnica de Machala; la metodología empleada en este proceso es de carácter descriptiva-bibliográfica, basada en fuentes de información fidedignas con medidas estratégicas que garantizan la veracidad de la información y proporcionan el cumplimiento del objeto de estudio, haciendo uso de habilidades, capacidades y recursos que posee el sistema de información de la unidad educativa, además de proporcionar la identificación de amenazas y debilidades que atentan la seguridad de la plataforma que permiten proporcionar sugerencias de mejora para próximos procesos de titulación.

Palabras claves: auditoría informática, procesos de auditoría, vulnerabilidades, amenazas y riesgos, ataques cibernéticos.

ABSTRACT:

The development of the present investigation has the purpose of analyzing the vulnerabilities that exist in the current computer system of the Academic Unit of Business Sciences for the presentation of the complex theoretical dimension, identifying possible vulnerabilities, responses and risks to which it is exposed the information of the students graduated in the process of qualification of the Technical University of Machala; The methodology used in this process is descriptive-bibliographic in nature, based on reliable sources of information with strategic measures that allow the veracity of the information and the study service, the use of skills, capacities and resources that the information system of the educational unit, in addition to providing the identification of the answers and weaknesses that threaten the security of the platform that the results of the improvement for the next titling processes.

Key words: computer audit, audit processes, vulnerabilities, threats and risks, cyber-attacks.

ÍNDICE.

ÍNDICE DE TABLAS.

ÍNDICE DE GRÁFICOS.

INTRODUCCIÓN.

A nivel mundial la humanidad se encuentra en firme contacto con la tecnología a través de teléfonos móvil u ordenadores, además, estos medios de comunicación están expuestos a cualquier tipo de acceso en su sistema informático, en las últimas décadas los archivos o datos que aparentemente se encuentran protegidos se pueden llegar a usurpar o desfalcar de su información real, este método técnico carece de la seguridad que permitirá cifrar la información de extremo a extremo, por tal razón, las entidades de carácter público o privado buscan masificar estrategias tecnológicas de tal manera que permitirá simplificar el trabajo y por ende disminuir el riesgo.

Por otra parte, la era tecnológica ha creado un sinnúmero de políticas de seguridad y resguardo en los sistemas de información y comunicación a nivel mundial, sin embargo, dichos procesos aplicados en los diferentes programas digitales no garantizan su calidad, eficacia y eficiencia al momento de realizar trabajos informáticos que comprometan datos personales o laborales. Según el autor Rodríguez (2016) indica que; "se pueden limitar o reducir la inseguridad que afectan a los seres humanos mas no eliminarlas por completo" (pág. 394). Los procedimientos empleados al momento de ingresar a un ciberespacio son muy relevantes, cada técnica permitirá minimizar el riesgo de un posible fraude, pero no impedirá que el exceso de confianza del usuario sobre su información personal sea expuesto ante la sociedad a través de una red informática, con ello provocará una malversación a su integridad.

En la provincia de El Oro, la Universidad Técnica de Machala es una institución de educación superior, dicho establecimiento ha desarrollado notablemente en los recursos técnicos para lograr una mejor seguridad en la información y comunicación en toda la cofradía universitaria en general. Es decir que, existe fragilidad al revelar datos privados o indagaciones específicas del área académica. Por tal razón, se plantea el desarrollo de la presente investigación titulada "Análisis de vulnerabilidades del sistema informático para rendir examen complexivo en la Unidad Académica de Ciencias Empresariales de la UTMACH".

El objetivo principal es analizar las vulnerabilidades que existen en el sistema informático en el que se rinde el examen complexivo dimensión teórico en la UACE, mediante la identificación de los posibles riesgos y amenazas a los que se encuentra expuesta la

plataforma para salvaguardar los datos específicos de los estudiantes egresados en proceso de titulación.

Con el análisis respectivo se logrará minimizar las debilidades en el medio virtual utilizado por la UACE para el proceso de acreditación académica, de tal forma se alcanzará disminuir eventualidades inconformes que contenga el sistema informático e impedir la filtración y desfalco de información, es sustancial conocer las políticas de seguridad que permitan salvaguardar los datos procesados de la plataforma, para evitar la ejecución de terceras personas ante la usurpación del contenido a través de la facilidad al acceso web.

Los procedimientos empleados permiten una percepción adecuada sobre el peritaje realizado a través de la entrevista, la cual consta de dos secciones fundamentales: la primera al departamento de sistemas y la segunda al departamento de la UMMOG, con el fin de profundizar los inconvenientes ocasionados a lo largo del régimen estudiantil, posteriormente la elaboración de una matriz FODA la cual admitirá realizar un análisis de mejoras en las próximas metodologías admisibles dentro del desarrollo calificativo titular y evitar que se susciten los mismos inconvenientes.

1. FUNDAMENTACIÓN TEÓRICA.

Auditoría informática. – Este procedimiento permite valorar y establecer sistemas de control y calidad en las organizaciones en especial en sus elementos informáticos, utilizando técnicas dirigidas a la valoración general y parcial de la información real del sistema. Además, un auditor informático posee la capacidad de recolectar, clasificar y estimar evidencias encontradas que garanticen la veracidad real de los resultados auditados, hechos constatados empíricamente con evidencias que manifiestan la certeza y sustento definitivo del mismo (Martínez, Blanco, & Loy, 2013).

Procesos de auditoría. – Según Gallego, Hernández y Clavijo (2016) menciona que; en la auditoría es importante recalcar que la veracidad de sus informes deben llevar un orden específico para complementar su trabajo, para ello se hace énfasis a tres procesos relevantes e indispensables que son:

1. **Planificación**, de puntualizar objetivos relevantes y determinar el nivel de riesgo en los informes de la auditoría.
2. **Ejecución**, la habilidad de crear, procesar y evaluar la información específica y enfatiza hallazgos de mayor relevancia para su trabajo.
3. **Informe,** el auditor realiza la argumentación en base a los hallazgos encontrados en la fase de ejecución para deducir su opinión.

Vulnerabilidad, amenazas y riesgo - El autor Santiso, Koller y Bisaro (2016) indica que: la vulnerabilidad es la debilidad o error del sistema informático que permite la fragilidad de la seguridad de los datos que se almacenan en la base de su sistema electrónico. Mientras que la amenaza es la acción de aprovecharse del peligro eminente que enfrenta la red informática, para poner en riesgo la seguridad del sistema computacional, mediante la propagación de virus, robo o fraude de la información ingresada. Para finalizar el riesgo es la posibilidad de que el perjuicio se cristalice aprovechándose de una vulnerabilidad y con ello afectando la totalidad de los resultados esperados del sistema digital.

Ataques cibernéticos. – Según Santiso, Koller y Bisaro (2016) los ciberataques se expanden por medio de internet mediante la propagación de virus, accesos a la web no

autorizados, o por sistemas creados para hurtar bases de datos de entidades públicas o privadas que pueden resultar muy perjudiciales afectando la confidencialidad del usuario.

2. METODOLOGÍA

Esta investigación está fundamentada específicamente a la investigación descriptiva-bibliográfica, proceso que permitirá valorar la calidad del sistema informático utilizado por la UACE para el proceso de titulación, misma que surge tras la necesidad de conocer y valorar el nivel de vulnerabilidades riesgos y amenazas constantes que sufre el sistema y por ende emitir recomendaciones tras la realización del análisis de la matriz FODA que permitan evitar o prevenir cualquier atentado contra el sistema logrando de esta manera mayor integridad, confiabilidad y confidencialidad en la información.

3. SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN.

Para el autor Gil y Gil (2017) la seguridad informática **"**Trata de minimizar los riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada y en general malintencionada" (pág. 194). Por otra parte, el autor Roba, Vento y García (2016) menciona que:

> La seguridad informática es la disciplina que nos habla de los riesgos, amenazas, análisis de escenarios, buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos tecnologías para elevar el nivel de confianza en la creación, uso almacenamiento, transmisión, recuperación y disposición final de información. (pág. 336)

La validación de la información es relevante ante una sociedad, es notable que todas las entidades públicas y privadas tratan de garantizar los datos subjetivos y preservar los recursos, procesos o técnicas institucionales, previniendo la variación, disolución, manipulación o circulación de manera prejuiciosa de información o comunicación entre los individuos.

La seguridad informática consiste en identificar y proteger todos los activos o dispositivos físicos que nos permitirán dar una mejor seguridad a los equipos con los que la empresa trabaja; mientras que la seguridad de la información ya no se basa en ¿Que vamos a proteger? sino ¿Cómo lo vamos a proteger? es decir; se resguarda la información almacenada en la base de datos; por ejemplo: el encargado debe saber ¿Qué? ¿Para qué?

y ¿Cómo? se utiliza la información que se está modificando, creando o accediendo en la empresa u organización, de modo que se pueda preservar de cualquier tipo de ataque en las bases de datos los cuales puedan representar un riesgo infalible para ellas (Martelo, Tovar, & Maza, 2018).

Por otra parte, la seguridad de información en la actualidad cuenta con diferentes niveles que permiten que la información ingresada cuente con alertas de seguridad, como pueden ser: claves de acceso, mensajes de texto, correos electrónicos, alerta mediante notificaciones al teléfono móvil de ingresos al sistema mediante dispositivos nuevos, el uso de protección de las cuentas con contraseñas mayores a 8 caracteres que contengan (letras mayúsculas y minúsculas, números, símbolos) entre otros (Monsalve, Aponte, & Chaves, 2014).

Un sistema informático según el autor Corda, Viñas y Coria (2017) puede definirse como confiable cuando cuenta con las siguientes particularidades:

- **Integridad:** significa que toda transformación en la información se debe conservar en el sistema de base de datos sin modificaciones no autorizadas en la información que esta almacene. Las medidas de protección pueden ser: otorgar solo acceso necesario, procedimientos de control de cambio, comprobadores de integridad y separación y rotación de deberes.
- **Confidencialidad:** es el pacto o acuerdo de confidencialidad de las personas físicas o morales de una entidad u organización la cual garantiza que prohíbe a los empleados de dicha empresa a la divulgación de la información que se indica en el contrato. Es decir; la información solo puede accedida por personal autorizado de manera autorizada.
- **Disponibilidad:** el contenido de la información debe estar disponible para el personal autorizado con libre acceso del usuario en el momento que consideré necesario. Las amenazas a la disponibilidad pueden ser: la negación al servicio, desastres naturales y acciones intencionales.
- **Irrefutabilidad:** la información no debe contener réplicas, es una forma estricta de automatización, por ende, debe portar contenido fidedigno e incuestionable.

El uso de las Tecnología de la Información y Comunicación (TIC) según indica el autor Bareño, Cárdenas, Navarro, Sarmiento y Forero (2017) “hace fácil, sencillo y seguro la implementación de un sistema electrónico” (pág. 73). Es decir, las TIC agilita los procesos de transferencia y almacenamiento de información; las entidades públicas o privadas e instituciones académicas: escuelas, colegios, universidades lo usan, estos sistemas permiten almacenar gran cantidad de información y evitar posibles pérdidas aun cuando no se garantiza seguridad al cien por ciento.

La administración de la información en las instituciones mediante el uso de las TIC puede aportar según el autor González, Zayas y Lopéz (2015) en “diseñar e implementar sistemas que recopilen, clasifiquen, analicen, evalúen, y distribuyan aquella información precisa, oportuna y necesaria a los procesos productivos y de servicio en las organizaciones” (pág. 35). Estos métodos al ser utilizados de manera adecuada permitirán disminuir gastos innecesarios en peritos y personas capacitadas en el manejo de sistemas de información y sobresalir en la exploración y atracción de mejores técnicas de captación de mercado.

Las entidades dependen de la información y la tecnología que las soporta, mismos que transfieren una serie de vulnerabilidades o contextos de debilidad en los recursos que administra y que pueden aparecer en cualquier parte de los elementos que conforman el hardware del sistema operativo, como también en el software. Por otra parte, los activos de una organización se encuentran expuestos a extenuaciones físicas, naturales, fraudes informáticos, hardware, software, medios de almacenamiento maliciosos, errores humanos, entre otros que pueden ocasionar daños irreversibles (Quiroz & Macías, 2017).

Los ataques cibernéticos son muy comunes en unidades educativas, empresa u organizaciones con el objetivo de reproducir la información, misma que puede ser utilizada con fines prejuiciosos para afectar a terceros o en caso de temas educativos variar datos y notas de los estudiantes. Por ello, se deben implementar constantemente adaptaciones mejoradas y sólidas que permitan garantizar la excelencia y calidad de los recursos, avalando la seguridad de la información compartida entre clientes y servidores y haciendo frente de forma efectiva a los ataques en los que se puede ver expuesta la información (Muñoz & Rivas, 2015).

Ahora bien, según Parada, Flórez, y Gómez (2018) indica que la seguridad de información es un recurso que tiene valor para la empresa y por consiguiente debe ser protegida correctamente, se debe implementar estrategias claras, que sirvan de apoyo respecto a la seguridad, disponibilidad, legalidad y confiabilidad de la información, frente a un conjunto de amenazas que pueden perjudicar el contenido almacenado, es importante que las medidas tomadas sean debidamente documentadas, evaluadas, revisadas y actualizadas de ser necesario; el autor Azán, y otros (2014) menciona que para minimizar la divulgación de datos se requiere de la constante revisión y control de los sistemas para que el personal encargado actúe en el momento exacto, identificando y corrigiendo a tiempo las partes del sistema que se consideran más vulnerables.

4. PROCESO DE MATRICULACIÓN AL EXAMEN COMPLEXIVO.

El examen de grado de carácter complexivo dimensión teórica, tiene como finalidad que el estudiante demuestre sus dominios en los ejes curriculares durante el proceso de formación académica, es por ello que la UTMACH cuenta con un sistema informático que permite a las/los estudiantes egresados facilitar y agilizar el proceso, al mismo tiempo almacenar la información de cada uno de los estudiantes en una base de datos.

Gráfico 1. Inicio de sesión SIUTMACH Fuente: https://app.utmachala.edu.ec

Durante el periodo académico y hasta la matriculación del proceso de titulación la información es almacenada en el SIUTMACH con el siguiente proceso de matriculación:

Gráfico 2. Matriculación proceso de titulación. Fuente: https://app.utmachala.edu.ec

Una vez ingresado al sistema el estudiante debe dirigirse a **titulación, matrícula, registrarme.**

El usuario tendrá que llenar los datos y requerimientos solicitados y por ende seleccionar la opción de titulación (trabajo práctico o examen complexivo), una vez llenados los formularios, si se registró satisfactoriamente se habilitará el botón imprimir, con el cual se procederá a validar la matrícula en el departamento de la UMMOG de cada unidad académica.

4.1. PROCESO PREVIO AL EXAMEN COMPLEXIVO PARTE TEÓRICA.

Previo a la rendición del examen los estudiantes que hayan legalizado la matrícula y se encuentren aptos para rendir el examen deberán.

- Descargar y resolver el banco de preguntas correspondiente a la carrera.
- El estudiante será notificado vía correo electrónico institucional, la fecha, hora y lugar donde deberá rendir el examen complexivo.
- Para la presentación del examen deberá ingresar a un sistema informático específicamente creado para este proceso.

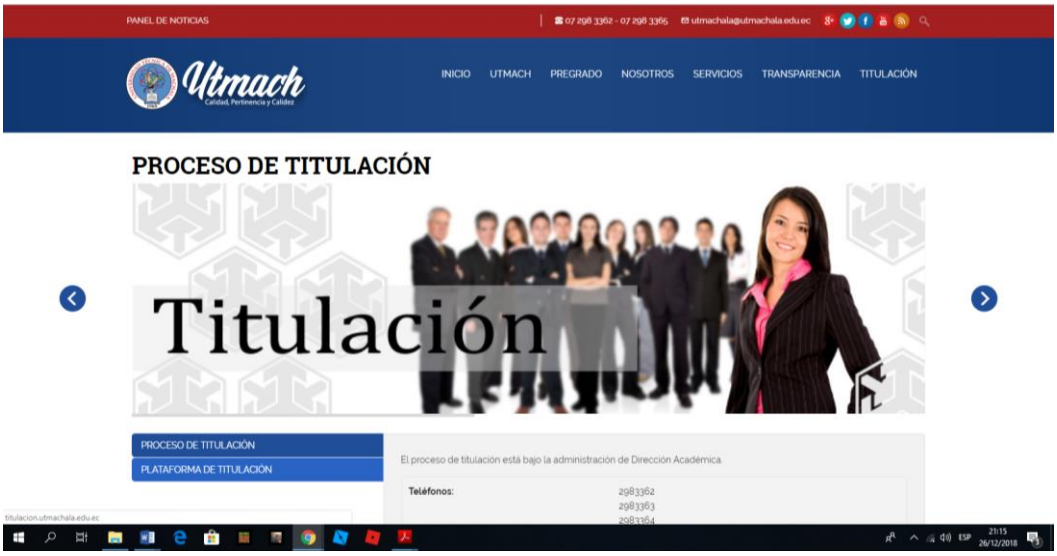

Gráfico 3. Plataforma de titulación. Fuente: https://www.utmachala.edu.ec

Al dar clic en la opción **plataforma de titulación** esta envía directamente a otra pestaña en la se solicita el ingreso del correo electrónico institucional y la contraseña que le permitirá acceder a la evaluación con un tiempo de duración de 120 minutos (2 horas).

Gráfico 4. Inicio de sesión proceso de titulación. Fuente: http://titulacion.utmachala.edu.ec

El puntaje del examen complexivo parte teórica es de 50 puntos la cual consta de 50 preguntas; es decir 1 punto por cada pregunta.

Todo el cuestionario estará sujeto a un sistema informático el cual nos presentará dos opciones:

- No, estoy seguro, pasar a la siguiente pregunta. En caso de que el estudiante no se encuentre seguro de la respuesta correcta, esta opción le permite al usuario volver a visualizar la pregunta al final.
- Sí, estoy seguro, pasar a la siguiente pregunta. En caso de estar seguro con la respuesta correcta, esta opción no permitirá volverla a visualizar.

El examen culminará cuando el estudiante haya respondido las 50 preguntas o cuando el tiempo de 120 minutos haya culminado.

El **Art. 11 Aprobación** de la Guía complementaria para la instrumentalización del sistema de titulación de pregrado de la UTMACH (pág. 2) indica que:

> Se considera aprobada la parte teórica con la obtención de una calificación mínima de 20 puntos en una escala del 1 al 50, con lo que podrá acceder a la parte práctica seleccionando el reactivo práctico de acuerdo a su perfil profesional, en la plataforma informática.

Como se puede notar todo el proceso de titulación del examen complexivo dimensión teórica está sostenido por el departamento de sistemas y departamento de la UMMOG, es por ello que para profundizar la indagación se procederá a la realización de dos entrevistas que permitirán analizar las vulnerabilidades, riesgos y amenazas a las que se encuentra expuesta la información recolectada en estas bases de datos.

5. MATRIZ DE RIESGO

Tabla 1 Matriz de riesgo. Fuente: elaboración propia.

No.	FACTOR DE RIESGO	PROBABILIDAD			IMPACTO			CAUSA	RECOMENDACIÓN	RESPONSABLE
		B	M	A	B	M	A			
1	Escasa seguridad en la información almacenada en la base de datos por propenso acceso de terceras personas.	**X**					**X**	Inseguridad del sitio web y divulgación de usuario y contraseña a terceros.	Implementar un enlace de acceso seguro a la plataforma y evitar compartir la información personal.	Departamento de sistemas.
2	No cuenta con alerta de seguridad al acceder a la plataforma de titulación.		**X**				**X**	La plataforma no cuenta los protocolos de seguridad necesarios para proteger la información.	Incorporar el acceso a la plataforma de titulación mediante el modo seguro que utiliza la página pública de la UTMACH, debido a que cuenta con el protocolo HTTPS y certificación SSL y evitar costos adicionales en la utilización de otros sistema de seguridad.	Departamento de sistemas
3	No cuenta con el protocolo HTTPS y certificación SSL.			**X**			**X**	No cuenta con las políticas de seguridad que posee Gmail.	Si la UTMACH tiene un hosting alojado en la cuenta de Gmail o Google, lo ideal sería que el sistema trabaje con toda la seguridad que este proporciona ya que es el único medio seguro que posee la entidad educativa.	Departamento de sistemas.

6. MATRIZ FODA

La sigla FODA forma un acróstico que significa: fortalezas, debilidades, oportunidades y amenazas, que representan una herramienta de estudio la cual permite impulsar al máximo el potencial de cualquier situación, individuo, producto, empresa o en este caso el sistema informático que utiliza la UACE de la UTMACH para la toma del examen complexivo parte teórica, modelo que permite mejorar su funcionamiento de forma estratégica en los próximos procesos de titulación. Esta matriz presenta la habilidad de perfeccionar los factores internos y externos que pueden impactar de forma negativa o positiva creando un plan significativo y fuerte que facilite la toma de decisiones.

Las fortalezas es un factor interno sobre el servicio, es un elemento positivo que le permite poseer una posición privilegiada frente a otros sistemas de información, contando con características tecnológicas que dan mayor realce a la aplicación, facilidad de uso, reducción de costos y gastos, resultados inmediatos y satisfacción al usuario en este caso.

Las oportunidades son aspectos positivos que podemos aprovechar utilizando las fortalezas encontradas, forman parte de las condiciones externas para lograr el objetivo y crear ventaja competitiva, es decir, los hechos que podamos detectar y explotar favorablemente y que puedan ser utilizado en beneficio propio.

Las debilidades son factores interno críticos o negativos que se deben eliminar, que provoca una situación desfavorable, en relación a la capacidad de los sistemas de competencia, es decir representa las carencias, inhabilidades, o actividades negativas que ponen en desventaja el desempeño del sistema informático y por ende se deben mejorar y mantener bajo control.

Las amenazas son aspectos negativos externos que podrían obstaculizar el logro de los objetivos y que no están bajo control, son factores que se encuentran fuera contexto, pueden llegar a atentar negativamente contra el sistema informático y que al momento de ser identificadas a tiempo permitirán crear una estrategia factible que quizá no ayude erradicar el daño, pero si a minimizarlo.

Análisis **FODA**
examen complexivo parte teórica de la UACE

AMENAZAS

- El usuario (estudiante) al compartir la contraseña o permitir el acceso a terceras personas de su cuenta personal.
- Suplantación de identidad o acceso de personas no autorizadas al sistema al momento de rendir la evaluación.
- No posee alerta de seguridad al acceder un usuario desconocido.
- Enlace sin seguridad, propenso a sufrir ataques.

FORTALEZAS

- Aplicación poco compleja con facilidad de uso para cualquier usuario egresado que se encuentre en proceso de titulación en la UACE.
- Reduce costos y gastos incurridos por evaluación a los estudiantes, tanto de personal como de materiales físicos.
- Satisface las necesidades del usuario egresado.
- Calificación inmediata posterior a la evaluación.

DEBILIDADES

- La interfaz y la apariencia del sistema es sencilla y poco llamativa.
- Acceso denegado a la modificación de las preguntas después de ser contestadas.
- Colapso del sistema por exceso de ingresos a la plataforma.
- Acceso rechazado a la visualización de las preguntas al finalizar la evaluación.

OPORTUNIDADES

- Crear un modelo de interfaz más agradable y adaptable a las necesidades del usuario que facilite la comprensión, mejorando la apariencia del sistema informático.
- Implementar un sistema que permite la verificación y modificación de las respuestas si el estudiante aun dispone de tiempo.
- Implementar políticas y aspectos de seguridad para generar confianza en el usuario al usar esta plataforma.
- Incorporar protocolo de seguridad al sistema de titulación de la UTMACH.

Gráfico 5. Matriz FODA Fuente: Elaboración propia

Tras haber analizado los puntos fuertes y débiles, las oportunidades y amenazas del objeto de estudio y la necesidad de emprender una acción en particular que permita obtener éxito, haciendo uso de las habilidades, capacidades y recursos con los que cuenta el sistema informático de la unidad educativa, la cual, permite mencionar las amenazas más relevantes que sufre el sistema que son; no contar con acceso seguro de ingreso a la plataforma de titulación, además del descuido e irresponsabilidad del estudiante al ceder sus usuarios y contraseñas a terceros lo que facilita aún más la usurpación de información, es importante mencionar que la UTMACH utiliza la certificación SSL y el protocolo de seguridad HTTPS, actualización brindada por WordPress, Es por ello, que se debe considerar la oportunidad de implementar este enlace seguro, dentro de la plataforma de la UTMACH, el cual permita hacer uso de la seguridad brindada, además, brindar capacitaciones que permitan concientizar al estudiante sobre la importancia de proteger sus cuentas de usuario. La matriz debe actualizarse constantemente, es decir, no debe mantenerse estática para lo cual se debe aplicar el siguiente proceso:

- Aprovechar las oportunidades
- Minimizar las amenazas
- Eliminar las debilidades y
- Utilizar las fortalezas.

CONCLUSIÓN

En cuanto a lo abordado anteriormente, acerca de la seguridad informática y seguridad de la información, estos dos componentes permitirán la protección de los activos de la entidad como de información almacenada en la base de datos del sistema, motivo por el cual deben estar debidamente protegidos y contar con estrategias tecnológicas que permitan detectar anomalías y minimizar el riesgo de posibles amenazas por filtración o desfalco de información, que puedan perjudicar a la entidad y representar un riesgo infalible para la misma. Un sistema se puede definir como seguro cuando cuentan con las características indispensables tales como: integridad, confidencialidad, disponibilidad e Irrefutabilidad.

Además, en la actualidad las entidades dependen de la información y de las tecnologías que estás lo soportan, es por ello que haciendo énfasis en el tema "análisis de las vulnerabilidades en el sistema informático para rendir el examen complexivo de la UACE de la UTMACH", se concluye que las vulnerabilidades, riesgos y amenazas que reporta el sistema no son representativas, debido a que la información de estas cuentas son privadas, con información competente para cada usuario y es el estudiante quien en muchas ocasiones por exceso de confianza expone información personal a terceras personas y pone en riesgo su integridad, sin embargo la inseguridad siempre está latente en el uso de la plataforma debido a que son seres humanos quienes se encuentran a cargo de dicho proceso.

Cabe recalcar que el sistema de titulación aun teniendo acceso directo desde la página pública de la UTMACH, la cual cuenta con el excelente protocolo y certificado de seguridad, este no cubre a la plataforma de titulación, debido a que al momento de ingresar al enlace la conexión del sitio web no es segura y cuenta con un problema grave de privacidad ya que es posible que otro usuario pueda ver la información ingresada, enviada o recibida a través del sitio. Por otra parte, el análisis FODA realizado permite identificar las vulnerabilidades en el sistema informático y sugerir alternativas de mejora a través del uso de herramientas y técnicas que conlleven a corregir situaciones negativas internas y externas que presenta la plataforma, para evitar inconvenientes que puedan afectar la información almacenada en los próximos procesos encaminado a la calidad, eficiencia y eficacia del sistema.

BIBLIOGRAFÍA

Azán, Bravo, Rosales, Trujillo, García, & Pimentel. (2014). Solución basada en el Razonamiento Basado en Casos para el apoyo a las auditorías informáticas a bases de datos. *Cubana de Ciencias Informáticas, 8*, 52-68.

Bareño, Cárdenas, Navarro, Sarmiento, & Forero. (2017). Sistema de Votación Electrónico con Características de Seguridad SSL/TLS e IPsec en Colombia. *UIS Ingenierías*, 72-81.

Corda, Viñas, & Coria. (octubre de 2017). Gestión de riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra clave, 7*(1), 1-18.

Gallego, Hernández, & Clavijo. (2016). Evaluación de herramientas tecnológicas de uso libre, aplicadas a procesos de auditoría. *Scientia Et Technica, 21*(3), 248-253.

Gil, & Gil. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica, 22*(2), 193-197.

González, Zayas, & Lopéz. (2015). Auditoría de información y auditoría de conocimiento: acercamiento a su visualización como dominios científicos. *Revista Cubana de Información en Ciencias de la Salud, 26*(1), 34-52.

Martelo, Tovar, & Maza. (2018). Modelo Básico de Seguridad Lógica. Caso de Estudio: el Labortorio de Redes de la Universidad de Cartagena en Colombia. *Información Tecnológica, 29*, 3-10.

Martínez, Blanco, & Loy. (2013). Propuesta del sistema de acciones para la implementación de la Auditoría con Informática. *Revista de Arquitectura e Ingeniería, 7*(2), 1-13.

Monsalve, Aponte, & Chaves. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). *Facultad de Ingeniería, 23*(37), 65-72.

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

Parada, Flórez, & Gómez. (2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistématica de la Dinamíca de Sistemas. *Información Tecnológica*, 27-38. doi:10.4067/S0718-07642018000100005

Quiroz, & Macías. (2017). Seguridad en informática: consideraciones. *Dominio de las ciencias*, 676-688.

Roba, Vento, & García. (2016). Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux. *Avances*, *18*(4), 334-344.

Rodríguez. (2016). ¿Qué seguridad? Riesgos y Amenzas de Internet en la Seguridad Humana. *Iberoamericana de Filosofía, Política y Humanidades, 18*, 291-415. doi:10.12795/araucaria.2016.i36.17

Santiso, Koller, & Bisaro. (2016). Seguridad en entornos educativos virtuales. *Memoria investigaciones en Ingeniería*, 67-88.

Vicerrectorado Académico de la UTMACH. (s.f.). Guía complementaria para la instrumentalización del sistema de titulación de prograd o de la UTMACH. 1-12. Machala, El Oro, Ecuador: Universidad Técnica de Machala. Obtenido de https://drive.google.com/file/d/1iFCSK9IpZH1qpMEie_gWLNBLBxDLymIj/view

ANEXOS

ENTREVISTA

DEPARTAMENTO DE SISTEMAS

El departamento de sistemas de la UTMACH cumple las funciones de mantenimiento tanto en redes informáticas como en equipos del área tecnológica de la institución y por tanto interviene en el sistema informático mediante el cual se evalúa a los estudiantes egresados, es por ello que se procederá a realizar una entrevista al encargado.

Nombre del entrevistado:

Cargo:

Contacto:

Email:

Fecha:

1. ¿Específicamente cuál es el rol que desempeña el departamento de sistemas en el proceso de titulación parte teórica?
2. ¿Qué amenazas sufre el sistema de titulación comúnmente dentro del proceso?
3. ¿Qué medidas se están tomando para evitar fallos en el sistema utilizado para este proceso?
4. ¿El sistema posee algún tipo de alerta de seguridad en caso de que esté siendo víctima de algún ataque?
5. En caso de que la página sea hackeada. ¿cuál es el nivel de respuesta ante ataque que recibe el departamento de sistemas?
6. ¿Desea aportar con un comentario adicional que ayude a complementar esta investigación?

ENTREVISTA

DEPARTAMENTO DE UMMOG

El departamento de la UMMOG (Unidad de Matriculación, Movilidad y Graduación) de cada Unidad Académica es el encargado de la evaluación del examen complexivo dimensión teoría. Por tanto, se procederá a la entrevista del encargado de dicho departamento para conocer las vulnerabilidades al que se encuentra expuesto el sistema de evaluación a los estudiantes en proceso de titulación.

Nombre del entrevistado:

Cargo:

Contacto:

Email:

Fecha:

1. ¿Específicamente cuál es el rol que desempeña el departamento de UMMOG en el proceso de titulación parte teórica?
2. ¿Cuáles son las amenazas constantes que detecta el sistema de informático en el que se rinde el examen complexivo?
3. ¿Existe algún riesgo de que se filtre información por parte de los docentes, alumnos, encargados o terceras personas?
4. ¿Qué sanciones se toman en caso de que se filtre información por parte de docentes, estudiantes, encargados o terceras personas?
5. ¿Qué tan segura es la plataforma en la que se rinde el examen complexivo parte teórica y cómo podría este departamento responder a un ataque en caso de suscitarse uno?
6. ¿Desea aportar con un comentario adicional que ayude a complementar esta investigación?