UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE VULNERABILIDADES, AMENAZAS Y RIESGOS AL SISTEMA DE MATRICULACIÓN DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH

AGILA TINOCO VALERIA PATRICIA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE VULNERABILIDADES, AMENAZAS Y RIESGOS AL SISTEMA DE MATRICULACIÓN DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH

AGILA TINOCO VALERIA PATRICIA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE VULNERABILIDADES, AMENAZAS Y RIESGOS AL SISTEMA DE MATRICULACIÓN DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH

AGILA TINOCO VALERIA PATRICIA
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 Análisis de vulnerabilidades, amenazas y riesgos al sistema de matriculación de 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

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

ILLESCAS ESPINOZA WILMER HENRY
0704128776
ESPECIALISTA 3

Fecha de impresión: domingo 25 de agosto de 2019 - 18:04

URKUND

Urkund Analysis Result

Analysed Document:	VALERIA AGILA.docx (D54793355)
Submitted:	8/13/2019 8:08:00 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, AGILA TINOCO VALERIA PATRICIA, en calidad de autora del siguiente trabajo escrito titulado Análisis de vulnerabilidades, amenazas y riesgos al sistema de matriculación de 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, 26 de agosto de 2019

AGILA TINOCO VALERIA PATRICIA
0706447364

RESUMEN

La telemática es un plano donde se gestiona las funciones de la sociedad, permite versatilidad la información, transferir saberes e integrar múltiples disciplinas en sistemas digitales, cuyo propósito es optimizar los procesos cotidianos. El presente trabajo aborda la problemática de los riesgos informáticos en sistemas académicos, en particular el de matriculación en la Unidad Académica de Ciencias Empresariales, perteneciente a la Universidad Técnica de Machala. Se aplica metodología descriptiva, mediante un análisis comparativo al establecer las respectivas medidas de seguridad para responder ante las vulnerabilidades detectadas. En la parte final se exponen los resultados como mecanismos de seguridad, soluciones comerciales, configuraciones o componentes lógicos en tablas o cuadros de variables para garantizar la calidad en la matriculación.

Palabras Clave: auditoria Informática, matriculación, vulnerabilidades, controles.

ABSTRACT

Telematics is a plane where society's functions are managed, it allows information versatility, knowledge transfer and integrating multiple disciplines into digital systems, whose purpose is to optimize everyday processes. This paper addresses the problem of computer risks in academic systems, in particular that of enrollment in the Academic Unit of Business Sciences, belonging to the Technical University of Machala. Descriptive methodology is applied, by means of a comparative analysis when establishing the respective security measures to respond to the detected vulnerabilities. In the final part, the results are presented as security mechanisms, commercial solutions, configurations or logical components in tables or tables of variables to guarantee the quality in the enrollment.

Keywords: Computer audit, enrollment, vulnerabilities, controls.

INDICE DE CONTENIDO

ÌNDICE DE IMAGENES

ÌNDICE DE CUADROS

ÌNDICE DE ANEXOS

1. INTRODUCCIÓN

La información es un recurso universal, siendo la vía en toda gestión e índole sin importar su propósito, esfera social o ámbito de aplicación; la velocidad revoluciona a las ciencias y prestaciones de los servicios informáticos para procesar datos exige criterios dinámicos tanto en la formación profesional como destrezas personales al utilizar en forma idónea dichos activos.

Dentro del contexto local, la Universidad Técnica de Machala como institución educativa tiene la pertinencia de forjar profesionales competentes, capaces de transformar e innovar en soluciones para los problemas en su área de desempeño; una variable clave es la didáctica, pedagogía y distribución de conocimientos que se dan mediante sistemas computacionales; los procesos académicos/administrativos se solventan en plataformas web ostentan múltiples potencialidades a la vez que vulnerabilidades paralelas a sus facilidades, es por ello que el proceso de matriculación al darse en el *Siutmach* es propenso a riesgos no contemplados en las directrices de la dirección de tecnologías de la comunicación e información.

La auditoría de información comprende los procedimientos técnicos para evaluar un sistema, diagnosticar debilidades/fortalezas, elaborar un informe e implementar medidas retroalimentativas, al derogar una filosofía de mejora continua como eje de desarrollo en toda organización.

Se aplica una metodología exploratoria, de carácter descriptivo al caracterizar los fundamentos teóricos, analizar el estado de seguridad en el sistema de matriculación por medio de la normativa ISO/IEC 27001 e investigación de campo para proponer actividades de control en respuesta a las vulnerabilidades evaluadas.

El objetivo del proyecto es: Analizar las vulnerabilidades, amenazas y riesgos al sistema de matriculación de la unidad Académica de Ciencias Empresariales de la Utmach.

Los objetivos particulares son: Caracterizar la fundamentación teórica por medio de una revisión literaria; diagnosticar las amenazas y vulnerabilidades mediante observación/entrevista y analizar los riesgos informáticos en el proceso de matriculación para proponer mecanismos de control factibles.

2. DESARROLLO´

Delinea el proceso para solucionar el caso práctico, desde la caracterización cognitiva hasta el análisis e inferencia de resultados.

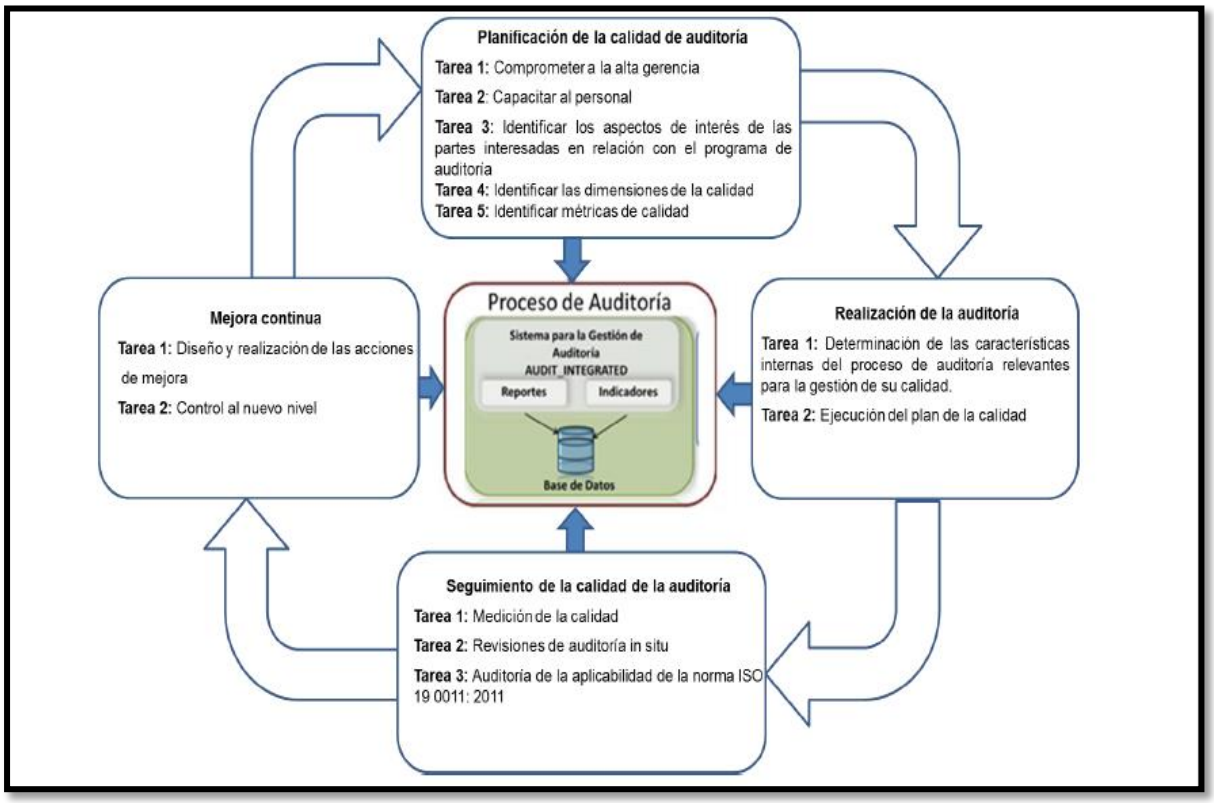
2.1 FUNDAMENTACIÓN TEÓRICA

Son el conjunto de términos relacionados a la temática, para compilar los conocimientos necesarios en el desarrollo del proyecto.

2.1.1 AUDITORÍA

Es un sistema de evaluación, control e implementación de medias para optimizar los estados financieros, equipos, departamentos y toda actividad externa e interna (Rodriguez Cordova, 2016); facilitan tomar decisiones oportunas analizando el su entorno en tiempo real.

Imagen 1. **Diseño para la gestión de calidad en el proceso de auditoría**



Fuente: (Escobar Rivera, Moreno Pino, & Cuevas Rodriguez, 2016)

2.1.2 AUDITORÍA INFORMÁTICA

Es el proceso para examinar e interpretar los estados en los sistemas informáticos con la meta de garantizar la solvencia, eficiencia e integridad de sus recursos tanto humanos como materiales y lógicos (Martinez, Blanco Alfonso, & Loy Marichal, 2013).

2.1.3 SISTEMA INFORMÁTICO

Es un conjunto de mecanismos que funciona en forma holsitica, permite gestionar datos e informaciòn de cualquier indole, con el proposito de emular procesos en forma digital facilitando las labores o automatizndo tareas secuenciales (Vega Perez, Grajales Lombana, & Montoya Restrepo, 2017).

2.1.4 SEGURIDAD INFORMÁTICA

Comprende los criterios para proteger los activos virtuales a un costo rentable para la institución, examina punto por punto todos los aspectos y ámbitos corporativos al evaluar las posibles vulnerabilidades al minimizar problemas (Baca Urbina, 2016).Sus características más relevantes son:

Efectividad. – Se encarga de proporcionar información oportuna para el desarrollo de las actividades de la empresa.

Eficiencia. - Capacidad para brindar información oportuna y adecuada con el óptimo uso de los recursos empresariales.

Confidencialidad. - Es importante para las organizaciones que la información sea protegida ante amenazas o robo de información**.**

Integridad. – La información debe ser coherente en su contenido para el proceso de validez de datos en la compañía**.**

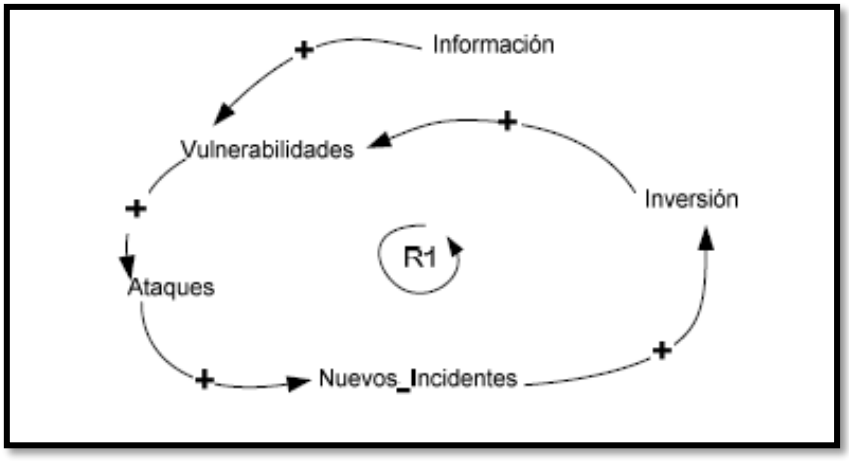
Disponibilidad. - La información debe presentarse a tiempo, cuando sea requerida por los departamentos de la organización,

Apego a estándares. – El desarrollo de la información organizacional debe estar sujeto a las leyes de acuerdo a los reglamentos expuestos por la institución.

Confiabilidad. – Se refiere que la información no haya sido modificada sin autorización de los encargados.

Las variables contempladas durante un ciber ataque se resumen en la imagen 2.

Imagen 2.Empresa sin medida de seguridad



***Fuente**: (Gil Vera & Gil Vera, 2017)*

2.1.5 VULNERABILIDADES EN SISTEMAS INFORMÁTICOS

Son las debilidades o errores en seguridad que son aprovechados para concretar un ataque; es decir al descuidar las contraseñas cualquiera puede ingresar, pero si se cuenta con verificación biometría aun con datos no podrá acceder (Quiroz-Zambrano & Macías-Valencia, 2017) Las más comunes son:

- Inyección SQL
- No respaldar archivos
- Configuración de seguridad incorrecta
- Carencia de certificados
- Virus o códigos maliciosos
- Puntos de acceso inalámbricos
- Hackeo (Quiroz-Zambrano & Macías-Valencia, 2017).

2.1.6 RIESGOS EN MEDIOS COMPUTACIONALES

Son la convergencia de la debilidad y la amenazada, dando paso a un ataque o efectuar un daño evidente al sistema, comúnmente son las desatenciones, falta de un plan de gestión de riesgos, recursos monetarios o falencias humanas que vulneran los sistemas.

2.1.7 MÉTODOS PARA DETECTAR DEBILIDADES

Permiten encontrar fallos en la seguridad, los más relevantes son:

- White/Black-box: Descubre vulnerabilidades desde la perspectiva de la organización y del atacante.
- Análisis de líneas de código: Revisa posibles fallos en la seguridad

- Análisis Dinámico: En tiempo real evalúa la seguridad al intentar violar la seguridad
- Pruebas de penetración: Realiza ataques mediante ingeniería de software para medir el grado de seguridad e inseguridad en los sitios analizados.
- Monitoreo del tráfico de datos: Escanear puertos, direcciones IP y revisar posibles ingresos no autorizados (Hernández Saucedo & Mejia Miranda, 2015).

2.1.8 METODOLOGÍA ISO/IEC 27001

Las consideraciones de mayor importancia se sintetizan en el cuadro 1.

Cuadro 1. Metodología ISO 27001 para gestión de seguridad Informática

FASES	DESCRIPCIÒN
Definir alcance y políticas del SGSI	Responsabilidades Políticas Recursos Identificar necesidades y objetivos
Análisis de requerimientos en seguridad	Valorar riesgos y activos Diagnosticar vulnerabilidades Identificar riesgos
Diseño del SGSI	Auditoria Planificación y gobierno de TIC`s Controles a implementar Medición, análisis y evaluación

Fuente: (Valencia-Duque & Orozco-Alzate, 2017)

2.1.9 CONTROL INTERNO

Es un proceso llevado a cabo por las personas de una organización, diseñado con el fin de proporcionar un grado de seguridad “razonable” para la consecución de objetivos.

Vega de la Cruz y Nieves manifiestan que “es una herramienta encargada de hacer cumplir los objetivos de las organizaciones mediante la toma de decisiones correctas haciendo uso de los recursos óptimos y necesarios para lograr veracidad y exactitud de la información”.

2.1.10 UX (USER EXPERIENCE)

Es la metodología que estudia el sistema-usuario desde la funcionabilidad, usabilidad y consistencia con la finalidad de ofrecer una sistema eficaz, amigable, fiable al uso humano mejorando la productividad en los sistemas informáticos (Molero Castillo, Benitez Guerrero , & Mezura Godoy , 2017).

2.2 CASO PRÀCTICO

El sistema de matriculación de la Unidad Académica de Ciencias Empresariales de la UTMACH, brinda al estudiante el acceso a la plataforma para su respectivo registro previo al inicio del periodo de clases; es fundamental desarrollar dentro de cualquier institución una Auditoria Informática, gracias a que se evalúan las vulnerabilidades, amenazas y riesgos potenciales, para mejorar la calidad, eficacia y eficiencia constantemente.

2.2.1 PLANEACION DE AUDITORIA

Se realiza una visita técnica, entrevista y concatenación con los criterios de la auditoria informática para responder adecuadamente al reactivo práctico.

2.2.2 VISITA PRELIMINAR AL ÁREA AUDITADA

Se procedió con la visita al departamento de las TIC'S para poder obtener la información necesaria a través de una entrevista al encargado del área sobre la seguridad lógica para detectar los pro y contras del software informático dentro de la plataforma de matriculación.

2.2.3 OBJETIVOS A LA AUDITORIA INFORMÁTICA DEL SISTEMA DE MATRICULACIÓN DE LA UACE

Objetivo General

Evaluar las posibles vulnerabilidades, amenazas y riesgos que se puedan presentar al sistema de matriculación de la UACE mediante una auditoria para proponer medidas que garanticen las actividades respectivas en la plataforma

Objetivos Específicos

- Verificar que el departamento de informática cumpla con los protocolos y estándares de seguridad para el acceso a la plataforma de matriculación
- Identificar posibles amenazas y sus vulnerabilidades correspondientes a través de una entrevista para determinar las necesidades en seguridad
- Desarrollar medidas de seguridad preventivas con la finalidad de reducir los riesgos que pudiesen presentarse en el sistema informático al matricularse.

2.2.4 GUIA DE LA AUDITORIA

Los puntos a evaluarse en el Sistema Informático de Matriculación de la Unidad Académica de Ciencias Empresariales de la UTMACH son:

- Revisar la existencia de un protocolo de seguridad para el acceso a la plataforma.
- Verificar si el sistema informático de matriculación es vulnerable a riesgos o amenazas.
- Verificar si el sistema informático de matriculación ha sido expuesto a una amenaza de hackeo.
- Verificar la protección de datos, procesos y programas a través de un software en caso de pérdida.
- Revisar si la plataforma es actualizada constantemente según el requerimiento de los usuarios.

Se evaluar la seguridad lógica del Sistema de Matriculación de la Unidad Académica de Ciencias Empresariales de la UTMACH por medio de una guía de auditoria que mostrara las herramientas utilizadas en el proceso y las actividades a ejecutarse **(VER ANEXO N°1. GUÍA DE AUDITORÍA).**

2.2.5 EJECUCION DE LA AUDITORIA

La técnica utilizada es: Entrevista de Seguridad lógica al departamento de las TIC'S. **(VER ANEXO N°2)**

La entrevista se realiza al personal técnico, en el departamento de Informática aplicando un análisis comparativo para apreciar las necesidades o eventualidades relacionadas al proceso de matrícula en el *Siutmach*

2.2.6 ENTREVISTA

Existen protocolos de seguridad para acceso a la plataforma. – En cuanto a la respuesta de la primera pregunta realizada manifestó el entrevistado que los protocolos de seguridad son ejecutados diariamente al momento que el personal administrativo, docente y estudiantes quieren acceder al sistema en lo cual el usuario debe proporcionar mediante su cedula y contraseña correspondiente; además recalco que es posible renovar los accesos al mismo una vez se desvincule la persona con la institución.

El sistema informático de matriculación es vulnerable a riesgos o amenazas. – El entrevistado recalcó que la vulnerabilidad de una aplicación no se puede encasillar en un sí o un no por las implicaciones que conlleva; sin embargo, detalló que para asegurar el SIUTMACH de donde forma parte el módulo de matriculación han tomado las medidas

necesarias que garanticen la integridad y disponibilidad de la misma, y su vez argumenta que la plataforma es sometida a pruebas periódicamente.

El sistema informático de matriculación ha sido expuesto a amenazas de hackeo. – En contestación a la tercera pregunta el entrevistado señalo que hasta el momento no tienen registro de incidentes que puedan ubicarse en esta categoría.

La protección de datos, procesos y programas es fiable para un software en caso de pérdida. – El entrevistado fue especifico al recalcar que le sistema informático de matriculación obtiene dos respaldos de su información diariamente.

La plataforma es actualizada constantemente según los requerimientos de los usuarios. – detalla el entrevistado que previo a la actualización del servidor de prueba, proceden con las mismas en el servidor de producción, siempre y cuando los primeros hayan sido aplicados exitosamente.

Al haber concluido con la Auditoria informática a la seguridad lógica del sistema de matriculación, dentro del contexto se ha visto la necesidad de obtener opiniones de los estudiantes en cuanto a la plataforma de matriculación, por lo cual se ha aplicado la metodología **USER EXPERIENCE (UX)** que permite emitir criterios en cuanto a la usabilidad, funcionabilidad entre el sistema-usuarios, y la norma ISO/IEC 9126 la cual evalúa la calidad del software y características para el respectivo análisis, para ello se aplicó una entrevista.

Por medio de esta metodología se analizará desde varios aspectos el desenvolvimiento de la plataforma, los cuales se verán reflejadas en las preguntas realizadas siendo el instrumento de eje principal para establecer un criterio fundamentado en cuanto a las experiencias de los usuarios, logrando de esta manera conocer fortalezas, oportunidades, debilidades y amenazas que el mismo presente.

Una vez obtenidos los resultados de los entrevistados cabe señalar que los puntos analizados han sido cuestionados desde el criterio propio del estudiante.

2.2.7 USABILIDAD

Responde a la siguiente cuestiòn:

¿Qué componentes analizaría para valorar la usabilidad del sistema de matriculación?

La usabilidad es el mecanismo que permite a los usuarios utilizar las opciones que tiene la plataforma de manera rápida y fácil de tal manera que contribuya al desenvolvimiento de los mismos logrando así el debido cumplimiento de los objetivos planteados por los dueños del software, es importante señalar que esta caracteristica cuenta con subcaracteristicas como lo son la operatividad, comprension, atractividad las cuales permiten analizar exhaustivamente la plataforma.

Imagen 3. Plataforma de matriculación UACE

Fuente: (UNIVERSIDAD TÈCNICA DE MACHALA, 2015)

Dentro de los hallazgos identificados se presenta que la plataforma no dispone de opciones didacticas como enunciados audibles para los estudiantes con capacidades especiales, lo cual afectaria al estudiante la comprensión para hacer uso de la misma.

El sistema de matriculación dentro de la perspectiva es poco atractivo, debido a que no presenta un buscador interno del sitio donde la comuniacion entre el sistema-usuario se facilite en caso de presentarse poco conocimiento del uso de la plataforma.

Dentro de la operatividad se puede denotar que la falta de estructuración en la navegación del sitio, debido a que existen opciones adicionales en cuanto a la edición de datos personales.

2.2.8 FUNCIONABILIDAD

Su mision es responer a la siguiente interrogante:

¿El sistema de matriculación en base a las necesidades de los estudiantes utiliza una metodología de valoración de la funcionabilidad?

Es aquella que garantiza al usuario que la plataforma esta funcionando de forma óptima con los funciones especificas, las subcaracteristicas que engloban son idoneidad, exactitud, interoperabilidad y seguridad. El sistema de matriculación ante está caracteristica presenta un nivel medio de seguridad para prevenir accesos no autorizados en la plataforma ya que no emiten notificaciones al correo o al celular por algún inicio de sesion accidental. Dentro de la idoneidad la plataforma a presentado en varias ocasiones poca capacidad de navegación, es decir lentitud al procesar información cuando varios usuarios se desplazan en el mismo sitio web ademas cuando existe colapso en la página web el sistema no crea respaldo de la informacion que esta siendo gestionada en ese momento.

El sistema de matriculación no presenta actualizaciones tecnologicas constantes en la plataforma, entre ellos hacer accesible el trámite de matriculación desde el lugar donde se encuentren los estudiantes, sin necesidad de presentar documentos en el departamento de matriculación.

SITUACIONES DETECTADAS

Con los resultados obtenidos de la auditoria informática desarrollada en el Sistema de Matriculación de la Unidad Académica de Ciencias Empresariales de la UTMACH, se detallará a continuación lo encontrado:

Mediante la entrevista al personal encargado del área se evidenció en la seguridad lógica que actualmente la Unidad Académica de Ciencias Empresariales de la UTMACH cuenta con los protocolos de seguridad pertinentes para el acceso a la plataforma; lo cual simplifica que los manuales y procedimientos son ejecutados por los encargados de manera correcta para evitar el acceso no autorizado y su vez proteger la integridad de datos de los usuarios. De la misma manera se señala que el SIUTMACH de donde es parte el sistema de matriculación no está exento a vulnerabilidades, sin embargo, el departamento ha tomado las medidas necesarias para evitar cualquier amenaza donde está expuesta información.

En cuanto a amenazas de hackeo que podría haber presentado el sistema, actualmente el departamento no posee registros de incidentes que podrían ubicarse en esta categoría, por otro parte se señala que el sistema cuenta con el respaldo diario de la información por cuanto no existe en la actualidad posibilidades que exista perdida de información, referente a la actualización de la plataforma recalcaron que constantemente realizar la actualización llevando a cabo los protocolos de seguridad que la misma necesita para el correcto desarrollo.

2.2.9 PROPUESTAS DE MEJORA AL SISTEMA DE MATRICULACIÓN DE UACE

Cuadro 2. Resultados de la auditoria Informática al sistema de matriculación

CARACTERISTICAS	HALLAZGOS DESDE LA PERSPECTIVA USER EXPERIENCE	CONTROLES PROPUESTOS
USABILIDAD	No posee enunciados audibles para estudiantes no- vidente No presenta un buscador interno en la plataforma No cuenta con la estructuracion adecuada en los comandos que presenta el sistema.	Incorporar al software la modalidad auditiva . Agregar a la plataforma la opcion de búsqueda Unificar módulos que pertenezcan a un solo contenido
FUNCIONABILIDAD	Lentitud al procesar información. Colapso de la plataforma y no respalda informacion que se gestiona en ese momento. No tiene actualizaciones tecnologicas constantes que optimicen tiempo y recursos	Añadir al sistema un procesador de mayor capacidad. Incorporar la firma electronica.
SEGURIDAD	Su gestion de riesgo es BUENA, no presenta deblidades explotables	Se aplica lo siguiente: Respaldos continuos Pruebas al servidor Protocolos de protecciòn

Fuente: Elaboración Propia

La mayor falencia detectada es la carencia de un plan macro que involucre a todas las dependencias en la UTMACH, no se aplica en forma directa una metodología de riesgos como la ISO u OWASP. Un punto a tratar es la actualización y renovación de equipos que actualmente es una necesidad en toda la infraestructura informática de la universidad, debida en buena parte al recorte presupuestario del estado

Aplica controles diarios y en forma coordinada, como respaldos, pruebas al servidor, verificación de autenticidad, certificados web e integra controles al personal para minimizar errores por la subjetividad humana.

La usabilidad y funcionalidad pueden mejorarse al implementar módulos adicionales e incluir opciones con prestaciones múltiples

El nivel de riesgo es bajo, gracias a que mantiene un control constante y no se han presentado eventualidades que ameriten una fortificación en la seguridad digital

3. CONCLUSIONES

Las amenazas latentes son la carencia de un plan de gestión de riesgos, recursos económicos insuficientes y actualización de equipos e infraestructura virtual; las vulnerabilidades más destacables con la saturación de la red, poca usabilidad y funcionalidad regular que impiden desarrollar con fluidez el proceso de matriculación.

Los controles implementados son respaldo diario de archivos, pruebas de servidor y verificar certificados de seguridad; además no se han evidenciado ni registrados hackers u otros ataques contundentes.

Se aplicó los criterios competentes a la auditoria informática para evaluar la seguridad, obtenido un nivel BUENO, aceptable para garantizar la integridad de los procesos académicos /administrativos y se desarrolló experiencia al redactar informes escritos.

4. REFERENCIAS BIBLIOGRÀFICAS

Baca Urbina, G. (2016). *Introduccion a la SeGuridad Informatica.* Mexico: Grupo Editorial Patria. Obtenido de https://books.google.com.ec/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=auditor%C3%ADa+INFORM%C3%A1tica&ots=0WQw4BAcKu&sig=hUFnxPrx6k9QZBu8yxQOG90LPV8#v=onepage&q=auditor%C3%ADa%20inform%C3%A1tica&f=false

Escobar Rivera, D., Moreno Pino, M. R., & Cuevas Rodriguez, L. (2016). La calidad de la auditoria en Sistemas de gestión. *Ciencias Holguin, 22*(2). Obtenido de http://www.redalyc.org/articulo.oa?id=181545579007

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad Informatica organizacional: un modelo de simulacion basado en dinamica de sistemas. *Scienti Et Technica, 22*(2). Obtenido de http://www.redalyc.org/articulo.oa?id=84953103011

Hernández Saucedo, A. L., & Mejia Miranda, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *ReCIBE. Revista electrónica de Computación, Informática Biomédica y Electrónica*.

Martelo, R., Tovar, L. C., & Maza, D. A. (2018). Modelo Basico de Seguridad Logica. *29*(1). Obtenido de https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100003&lng=en&nrm=iso&tlng=en

Martinez, Y. A., Blanco Alfonso, B., & Loy Marichal, L. (2013). Propuesta del Sistema de Acciones para la implementacion de la Auditoria con Informatica. *Revista de Arquitectura e Ingenieria, 7*(2). Obtenido de http://www.redalyc.org/pdf/1939/193929227003.pdf

Molero Castillo, G. G., Benitez Guerrero , E. I., & Mezura Godoy , C. (2017). Interaccion humano computadora y mineria de datos para la generacion y representacion de conocimiento util. *48*(1), 3-10. Obtenido de http://www.redalyc.org/pdf/1814/181454538001.pdf

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

Rodriguez Cordova, R. G. (2016). Fundamentos básicos para la ejecucion de la auditoria ambiental. *Centro de Informacion y Gestion Tecnologica de Holguin, 22*(1). Obtenido de https://www.redalyc.org/pdf/1815/181543577002.pdf

UNIVERSIDAD TÈCNICA DE MACHALA. (2015). *SIUTMACH*. Obtenido de MATRÌCULA: https://app.utmachala.edu.ec/siutmach/public/seguridades/contenedor/index

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista lbérica de Sistemas y Tecnologías de Información*, 73-88.

Vega de la Cruz, L. O., & Nieves Julbe, A. F. (s.f.). Procedimiento para la gestion de la supervision y monitoreo de control interno. *Centro de Informacion y gestion tecnologica de Holguin, 22*(1), 1-19. Obtenido de https://www.redalyc.org/pdf/1815/181543577007.pdf

Vega Perez, C. A., Grajales Lombana, H. A., & Montoya Restrepo, L. A. (2017). Sistemas de informacion: definiciones, usos y limitantes al caso de la produccion ovina colombiana. *21*(1). Obtenido de http://www.redalyc.org/articulo.oa?id=89653552007

5. ANEXOS

SISTEMA INFORMATICO DE LA UNIVERSIDAD TECNICA DE MACHALA				SIUTMACH FECHA: 13/01/2019 HORA: 9h00
REFERENCIA	**ACTIVIDAD A EVALUAR**	**PROCEDIMIENTOS DE AUDITORIA**	**HERRAMIENTAS UTILIZADAS**	**OBSERVACIONES**
AUD 01	Evaluar la seguridad lógica del sistema	Revisar la existencia de un protocolo de seguridad para el acceso a la plataforma.	Entrevista	
		Revisar si el sistema informatico de matriculacion es vulnerable a riesgos o amenazas.		
		Verificar si el sistema informatico de matriculacion ha sido expuesto a una amenaza de hackeo.		
		Verificar la proteccion de datos, procesos y programas a traves de un software en caso de pérdida.		
		Revisar si la plataforma es actualizada constantemente según el requerimiento de los usuarios.		

ANEXO # 1. Guía de evaluación en la seguridad lógica

ENTREVISTA

1.- ¿Cuáles son los protocolos de seguridad para el acceso al Sistema Informático?

Para poder acceder al sistema el usuario debe proporcionar su cedula o pasaporte y la contraseña correspondiente. Se otorga acceso al sistema al personal administrativo, docente y estudiantes. Es posible revocar los accesos al mismo una vez se desvincule la persona de la institución.

2.- ¿El Sistema Informático de Matriculación es vulnerable a riesgos o amenazas? Si o no

¿Si es si por qué?

La respuesta de la vulnerabilidad de una aplicación no se puede encasillar en un si o un no por las implicaciones que conlleva. Para cuyuna el SIUTMACH de donde forma parte el Modulo de Matriculación se han tomado las medidas necesarias que garanticen la integridad y disponibilidad de la misma, la misma nos sometidas a pruebas periódicas.

3.- ¿Ha sido expuesto la plataforma de matriculación a una amenaza de hackeo?

Hasta la fecha no tenemos registro de incidentes que puedan ubicarse en esta categoría.

4.- ¿El Sistema Informático de Matriculación crea respaldos de información en caso de pérdida? ¿Con que frecuencia?

Se obtienen 2 respaldos diarios.

5.- ¿La plataforma informática de Matriculación es actualizada constantemente?

Para actualización en periodos de pruebas se puede ver las mismas en el servidor de producción siempre y cuando los primeros hayan sido aplicados exitosamente.

ANEXO # 2. Entrevista realiza a personal técnica en el departamento de Informática