



UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LOS RIESGOS Y VULNERABILIDADES DEL ENTORNO
VIRTUAL DE APRENDIZAJE DE LA UACE

FLORES BALCAZAR MARIO ANDRE
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019



UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LOS RIESGOS Y VULNERABILIDADES DEL
ENTORNO VIRTUAL DE APRENDIZAJE DE LA UACE

FLORES BALCAZAR MARIO ANDRE
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019



UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE LOS RIESGOS Y VULNERABILIDADES DEL ENTORNO VIRTUAL DE
APRENDIZAJE DE LA UACE

FLORES BALCAZAR MARIO ANDRE
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

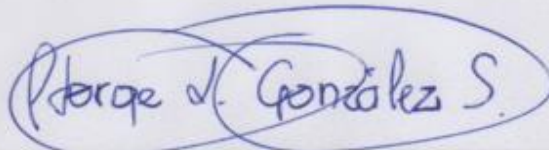
GONZALEZ SANCHEZ JORGE LUIS

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 los riesgos y vulnerabilidades del entorno virtual de aprendizaje de la UACE, 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 BRICENO KARLA FERNANDA
0705031003
ESPECIALISTA 2



CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 3

Fecha de impresión: viernes 01 de febrero de 2019 - 11:43

Urkund Analysis Result

Analysed Document: FLORES BALCAZAR MARIO ANDRE_PT-011018.pdf (D47128588)
Submitted: 1/22/2019 9:47:00 PM
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

El que suscribe, FLORES BALCAZAR MARIO ANDRE, en calidad de autor del siguiente trabajo escrito titulado Análisis de los riesgos y vulnerabilidades del entorno virtual de aprendizaje de la UACE, 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.

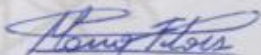
El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las disposiciones definidas por la Universidad Técnica de Machala.

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.

El autor 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



FLORES BALCAZAR MARIO ANDRE
0705274041

RESUMEN

En la Universidad Técnica de Machala (UTMACH), como en otras instituciones de educación superior, se utilizan sistemas informáticos con el fin de automatizar el aprendizaje de los alumnos o bien para reducir el tiempo de ejecución de otros procesos.

En la actualidad a nivel mundial se observa un gran avance tecnológico, lo cual en algunos aspectos favorece al desarrollo social, pero contraen peligros a los que se expone el entorno virtual. Por tales razones, este documento expone contextualmente la explicación concerniente a riesgos y vulnerabilidades en el entorno virtual de aprendizaje (EVA), describiendo cuáles criterios deben considerarse en la seguridad informática.

Con la instalación de antivirus o capacitaciones al usuario, realizando revisiones regulares a los equipos, no se reduce la amenaza al que están propensos, siendo más eficiente contratar a una empresa que tenga experiencia en ataques y seguridad de sistemas, para garantizar la integridad de datos o evitar el robo de información. Mediante la investigación bibliográfica y el análisis deductivo, se propone los controles físicos/lógicos más eficientes, para responder a las amenazas/vulnerabilidades latentes en el EVA, además de un cuadro comparativo con las medidas que podrían tomarse para evitar ataques potenciales en los sistemas computacionales.

Palabras Clave: Entorno virtual, riesgos, vulnerabilidades

ABSTRACT

In the Universidad Técnica de Machala UTMACH), as in other institutions of higher education, computer systems are used in order to automate the learning of students or to reduce the execution time of other processes. At the present time worldwide, a great technological advance is observed, which in some aspects favors social development, but they contract dangers to which the virtual environment is exposed. For these reasons, this document provides a contextual explanation of the risks and vulnerabilities in the virtual learning environment (EVA), describing which criteria should be considered in computer security. With the installation of antivirus or user training, making regular revisions to the equipment, the threat to which they are prone is not reduced, it being more efficient to hire a company that has experience in attacks and system security, to guarantee the integrity of data or avoid information theft. Through bibliographic research and deductive analysis, the most efficient physical / logical controls are proposed to respond to the latent threats / vulnerabilities in the EVA, as well as a comparative table with the measures that could be taken to avoid potential attacks on computer systems.

Keywords: Virtual environment, risks, vulnerabilities

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES	3
ÍNDICE DE CUADROS	3
INTRODUCCIÓN	4
2. DESARROLLO	6
2.1. FUNDAMENTACIÓN TEÓRICA	6
2.2. MARCO CONTEXTUAL	7
2.2.1 MACRO	8
2.2.2 MESO	9
2.2.3 MICRO	9
2.3. METODOLOGÍA	11
2.3.1 Investigación documentada:	11
2.3.2 Análisis deductivo:	11
2.3.3 Observación:	11
2.4. DESARROLLO	11
2.4.1 Gestión de roles	12
2.4.2 Cambio periódico de contraseña	12
2.4.3 NMAP	12
2.4.4 Metasploit	12
3. CONCLUSIONES	15
BIBLIOGRAFÍA	16

ÍNDICE DE ILUSTRACIONES

Ilustración 1 Seguridad en máquinas virtuales que gestas entornos de aprendizaje	5
Ilustración 2 Esquematización del entorno virtual de aprendizaje	7
Ilustración 3 Diagrama de flujo de auditoría informática	8
Ilustración 4 Entrada del SIUTMACH.	10
Ilustración 5 Página de inicio del Aula virtual (EVA).	10
Ilustración 6 Página de ingreso a la Base de Datos.	11
Ilustración 7 Relaciones en la seguridad del EVA	13

ÍNDICE DE CUADROS

Cuadro 1 Lista de vulnerabilidades físicas y sus posibles medidas de control.	13
Cuadro 2 Lista de vulnerabilidades lógicas y sus posibles medidas de control.	14

1. INTRODUCCIÓN

En la historia de la humanidad, eminentemente los acontecimientos que han transformado la sociedad han marcado el cambio de *eras*, a partir de la revolución Francesa se gesta la época contemporánea cuya ideología dejó atrás el periodo moderno y en los últimos años sobresale la *era digital* que surge de la sociedad del conocimiento, denominada así por estar caracterizada en la transferencia de información solventado las funcionalidad/potencialidades de procesos mediante tecnologías computacionales, que emigraron de metodologías tradicionales a sistemas informáticos.

En el contexto macro las instituciones de educación superior, cumplen un papel interdisciplinario de carácter pedagógico-formativo induciendo directamente la producción científica, avance de la ciencia y capacitaciones de profesionales activos en investigar proyectos destinados a solventar las problemáticas de la sostenibilidad social (ANTEZANA, GARCÍA, & RAMOS, 2014). Desde la perspectiva académica las universidades facultan una transformación cultural en su localidad, están obligadas a buscar procesos más eficientes en el ámbito laboral, innovar en las ciencias, contribuir a la tecnificación de sus áreas de estudio y trascender *esquemas*; los ambientes virtuales de aprendizaje (AVA) son el medio adecuado para coordinar sistemas académicos en entornos digitales, gracias a que sincronizan foros, chat, video llamadas, evaluaciones, tareas, además de permitir un acceso uniforme a la información, también proponen una nueva forma de sustentar el contenidos de las cátedras basado en plataformas web, a su vez reducen la *brecha digital y desigualdad de género* al armonizar las cualidades en el uso de sistemas informáticos. No obstante, destaca las vulnerabilidades/debilidades propias de los medios virtuales, donde el software o hardware son blancos de amenazas latentes; pese a ello las instituciones educativas se enfrentan al reto de romper paradigmas en los procesos académicos o pre textos culturales en la transferencia de saberes sin las limitantes de espacio-tiempo (Zúñiga, Lozano, García, & Hernández, 2018).

Los entornos virtuales de aprendizaje son un sistema complejo de servicios online, retroalimentación de información y un proceso constante de valoración de indicadores en tiempo real; debido a su contraparte física están solventados en servidores, redes de ordenadores e íntegramente a *internet*; es por eso que una metodología de evaluación es mediante estándares de usabilidad normados a nivel internacional, las consideraciones generales son las siguientes:

- Facilidad de pedagogía
- Facilidad de entendimiento

- Facilidad de ayuda
- Accesibilidad técnica/herramientas/errores
- Grado de atracción
- Adherencia a normas y comodidad
- Flexibilidad
- Interfaz de usuario
- Gestión de contenido/documentos

La seguridad en un entorno virtual se expresa de forma general en la *ilustración 1*.

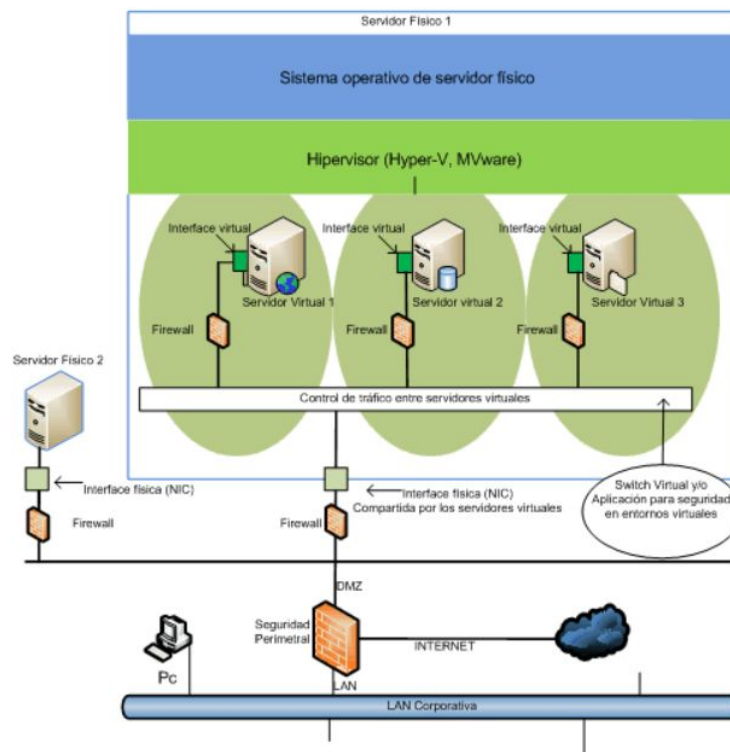


Ilustración 1 Seguridad en máquinas virtuales que gestan entornos de aprendizaje Fuente: (Gallardo, 2018)

La documentación competente tiene por objetivo analizar los riesgos y vulnerabilidades latentes en el entorno virtual de aprendizaje (EVA), en la Unidad Académica de Ciencias Empresariales, mediante una investigación bibliográfica desde una perspectiva teórica-cognitiva a través de un proceso deductivo para proponer las mejores medidas/métodos en responder oportunamente frente a las debilidades del EVA, con la finalidad de proponer una mejora en la seguridad digital aplicando criterios de auditoría informática.

2. DESARROLLO

2.1. FUNDAMENTACIÓN TEÓRICA

En esta sección se describen todos los conceptos y definiciones que fundamentan los criterios citados, abordados desde la perspectiva del autor en función del estudio epistemológico que interviene en la resolución de la problemática.

Riesgos informáticos: Son el efecto que puede producirse sobre un material digital, las herramientas de ataques informáticos que existen hoy en día son diversas, tanto que casi cualquiera podría manipularlas, lo cual conlleva al riesgo de perder información confidencial por parte de profesionales sin ética, *Wireshark* permite capturar todo lo que transita por una red, *Man in the middle* (Hombre en el medio) en donde el atacante tiene una conexión autónoma, con cada víctima enviando mensajes y haciéndolos creer que intercambian contenido entre sí, cuando en realidad están siendo controlados por el ciber delincuente; *Cain & Abel* un software que permite recuperar contraseñas, con lo que se puede obtener claves sin necesidad de tener acceso, herramienta similar a John the Ripper que es un fuerte descifrador de claves; como estos existen otros softwares capaces de filtrar información privada. Así como los *hackers* que representan una amenaza potencial para la privacidad de información (Macías-Valencia, 2017).

Vulnerabilidades: Representa la debilidad que puede tener un servidor informático frente a las amenazas latentes en el medio, esta impotencia permite a cualquier atacante violar la confidencialidad del usuario. Estas debilidades pueden ser resultado de malas configuraciones al momento de diseñar un software o por las limitaciones que el mismo pueda tener o por la falta de control del usuario (Macías-Valencia, 2017).

Entorno Virtual de Aprendizaje EVA: Actualmente se observa la incursión de las Tecnologías de Información y Comunicaciones (TICs) en el ámbito educativo, brindando facilidades tanto a maestros como alumnos para su interacción online en el proceso de enseñanza-aprendizaje, dentro de dicho contexto destacan los EVA que son diseñados principalmente para el uso de estudiantes y maestros, en donde ellos son los protagonistas principales de su formación (Hernán Santiso, 2016).

En este caso de estudio, el EVA sustenta varias potencialidades a través de servicios virtuales, tales como gestor de archivos, chat, notas, evaluaciones online, notas, comunicación, foros e integra un seguimiento de los cursos afines a cada carrera en las unidades académicas, permitiendo una administración dinámica de las clases en base al desempeño del estudiante/docente, por ende, es imperiosa la necesidad de analizar su nivel

de seguridad y que controles son requeridos para garantizar su permanencia como herramienta didáctica.

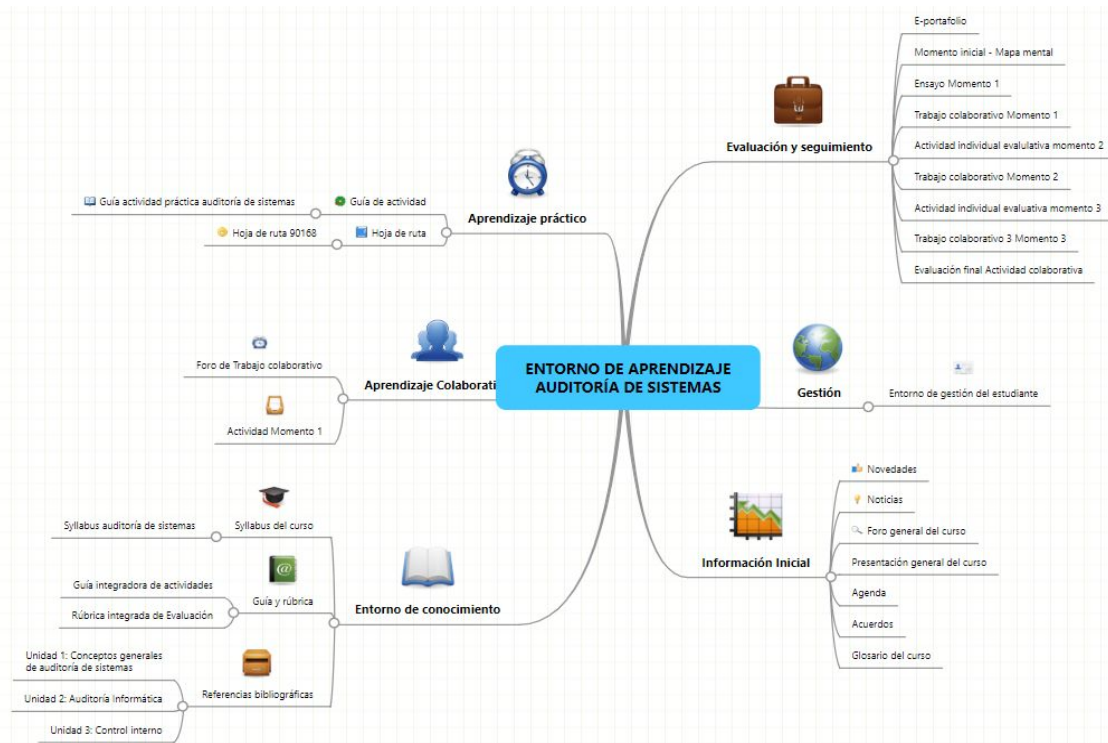


Ilustración 2 Esquematización del entorno virtual de aprendizaje Fuente: (Jairo, 2015)

Controles físicos y lógicos: En el control físico se pretende colocar un tipo de defensas que proteja al hardware de amenazas que vulneren información confidencial, una buena opción son los lectores de huella digital, reconocimiento de voz o facial. Por otro lado está el control lógico está dado por un tipo de protección que cuide del acceso restringido sólo a usuarios autorizados a hacerlo. Son limitaciones que ponen los administradores con el fin de salvaguardar la integridad de la información contenida (Leidy Barrera, 2015).

Auditorías informáticas: Constituye la serie de actividades que deben realizarse periódicamente para controlar las actividades realizadas por un servidor y garantizar el acceso seguro a las plataformas virtuales, detectando accesos no permitidos y rastreo de IP desconocidas (Hernán Santiso, 2016).

2.2. MARCO CONTEXTUAL

Se realiza una búsqueda de controles en seguridad informática, considerando el entorno espacial, a modo abductivo para redimir el estado actual de la problemática y a qué nivel se encuentra la Universidad Técnica de Machala, en contraste con organizaciones similares.

2.2.1 MACRO

En España con el fin de realizar una auditoría para combatir los riesgos informáticos presentes en las universidades y centros educativos, la Agencia Española de Protección de Datos (AEPD) ha impulsado un plan Sectorial de Oficio sobre la enseñanza reglamentada, de políticas dinámicas en análisis de seguridad en sistemas, tal como se aprecia en la *ilustración 3*.

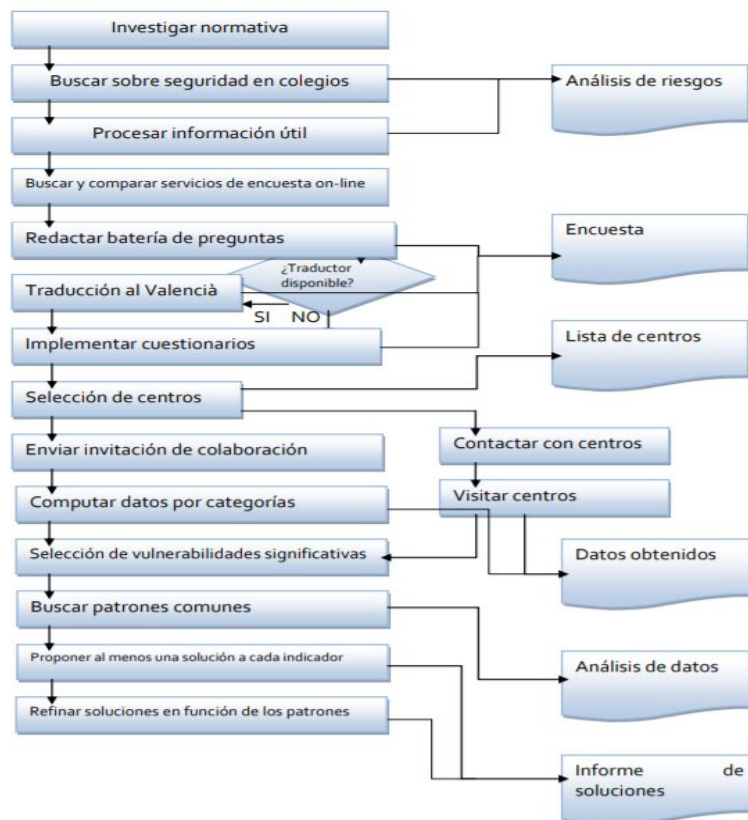


Ilustración 3 Diagrama de flujo de auditoría informática Fuente: (Frutos, 2011)

En la Universidad de Ciencias Médicas de Holguín (UCM), del Ministerio de Salud Pública (MINSAP) de Cuba, consta una persona encargada de brindar la seguridad requerida a toda la información contenida en sus plataformas virtuales, su función principal es realizar auditorías permanentes para detectar y mitigar cualquier amenaza que ponga en peligro la integridad del contenido privado. La idea es tener alguien a quien recurrir en momentos cuando, se sabe que el sistema informático está siendo vulnerado por alguien ajeno a la institución (Yanet Díaz Ricardo, 2014).

2.2.2 MESO

En el ámbito Nacional, la Universidad Técnica de Babahoyo tiene una intranet poco segura que pone en riesgo las acciones computacionales de la institución, puesto que, por la facilidad de acceso, cualquier usuario puede conectarse a la red.

Esta vulnerabilidad pone en peligro la integridad de la información, debido al mal control de los puertos de red que perjudicarán en un gran porcentaje a su infraestructura tecnológica, es decir este centro de Educación Superior no cuenta con un buen sistema de seguridad en la red (Geovanny Vega Villacís, 2017).

Red Nacional de Investigación y Educación del Ecuador, en marzo del 2018 realizó un congreso con las instituciones de educación superior, entidades académicas y municipalidades, para exponer las necesidades en seguridad informática, prevención de riesgos, respuesta a vulnerabilidades/ataques/amenazas, evidenciando que actualmente se ha tomado conciencia sobre el potencial de los activos informáticos en el desarrollo socioeconómico nacional, además en los foros se concluyó que las redes sociales son un factor clave, para culturizar sobre la relevancia de los sistemas virtuales en la vida tanto personal como profesional (RED CEDIA, 2018).

2.2.3 MICRO

A nivel local, la Universidad Técnica de Machala cuenta con plataformas virtuales que facilitan la interacción del alumno con el docente y a su vez con la institución de educación, la cuales tiene protocolos de seguridad con el fin de restringir el acceso a cualquier persona, pero aun así no dejan de ser vulnerables a cualquier riesgo existente en el medio. Estas barreras son: la utilización de usuario-contraseña para ingresar al SIUTMACH (plataforma virtual que contiene toda la información del estudiante), el Aula Virtual (Entorno Virtual de Aprendizaje en donde se maneja información académica como deberes o contenido académico) y la Biblioteca Digital que posee varias bases de datos dispuestas al uso de los estudiantes. Pero hay una desventaja al momento de intentar ingresar a cualquier sitio online de la Universidad desde afuera, el sistema detecta el IP desconocido y envía un mensaje al usuario pidiéndole que confirme su acceso, pero si se intenta ingresar a cualquier plataforma desde dentro del campus universitario en una computadora que tiene estadia permanente en la universidad, se lo puede hacer sin problemas, por lo que se corre el riesgo de que cualquier persona ingrese a la cuenta personal de algún estudiante o docente.

Es importante denotar que no se cuenta con estudios íntegros sobre seguridad informática en los sistemas administrativos, ni académicos, haciendo hincapié en profundizar en dicha área, para sentar las bases de una renovación tecnológica que optimice los procesos online de la UTMACH.



Ilustración 4 Entrada del SIUTMACH. Fuente: (UTMACH, 2018)

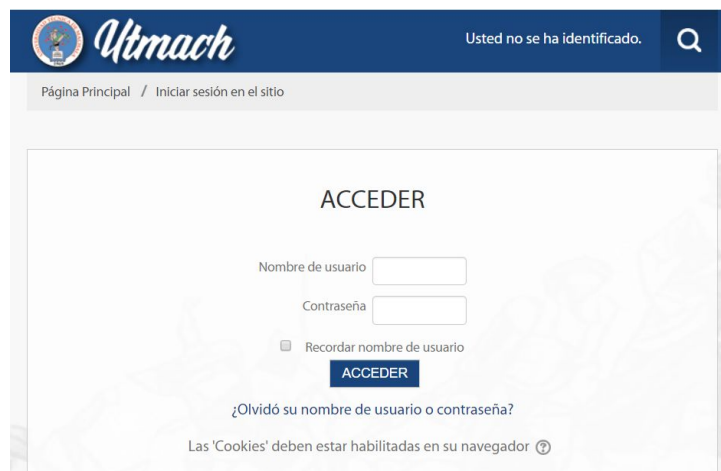


Ilustración 5 Página de inicio del Aula virtual (EVA). Fuente (UTMACH, 2018)

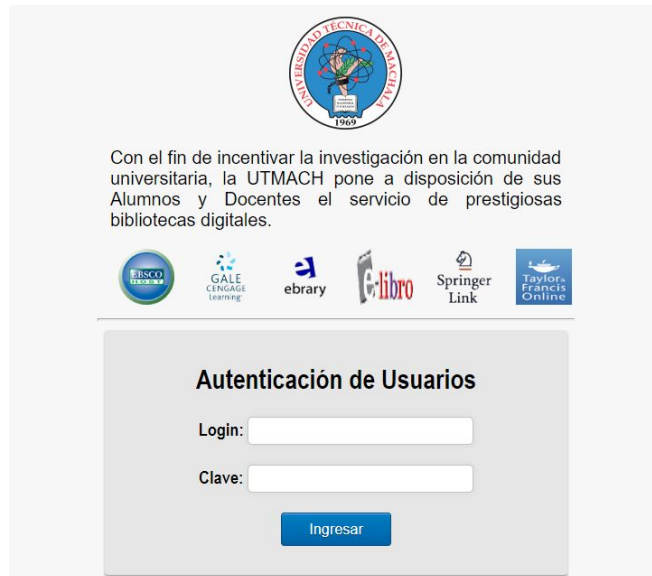


Ilustración 6 Página de ingreso a la Base de Datos. Fuente: (UTMACH, 2018)

2.3. METODOLOGÍA

Describe los procesos mediante los cuales se lleva a cabo el desarrollo de la problemática planteada en el siguiente documento.

2.3.1 Investigación documentada:

Se fundamenta en la base de información teórica extraída de documentación como artículos científicos, artículos de revistas, secciones de libros, informes y cualquier otro medio confiable que contribuya a la formación de criterios para la elaboración del proyecto.

2.3.2 Análisis deductivo:

Consiste en la unión de pequeños fragmentos de conocimiento, tomados desde diferentes fuentes de información con el fin de formar una visión amplia del tema, facilitando su comprensión e interpretación.

2.3.3 Observación:

Esta metodología se aplica describiendo lo observado en el campo sin realizarle ningún tipo de alteración y emitiendo criterios sobre lo que se ha podido percibir, dando lugar a leyes o inferencias sobre el fenómeno estudiado, en base a conjeturas o rasgos sujetos al razonamiento lógico.

2.4. DESARROLLO

Se da a conocer los riesgos y vulnerabilidades a los que constantemente se encuentra expuesta la plataforma virtual de la Universidad Técnica de Machala, pese a esto existe un sin número de medidas que pueden tomarse con el fin de prevenir o mitigar los

ciberataques, a continuación, se mencionan los que se considera son los más eficientes para lograr este fin, proponiendo una síntesis a través de los *cuadros 1 y 2*.

2.4.1 Gestión de roles

Este es un proceso simple que utiliza la autenticación de rol del usuario dentro de una institución, en donde se distingue cuando un usuario pertenece a un determinado rango, presentando la posibilidad de analizar y detectar cuando algún usuario intenta ir contra las condiciones del servicio (R., 2012).

2.4.2 Cambio periódico de contraseña

Consiste en realizar el cambio de la clave de acceso a una plataforma virtual de manera periódica, es decir en un lapso determinado de tiempo, que generalmente debe ser corto con el fin de evitar el espionaje y robo de información; en caso de no hacerlo el administrador del sistema debería asignar una contraseña aleatoria y segura que sería enviada al correo institucional del estudiante. Esta es una medida de seguridad informática que funciona bien evitando contravenciones en el sistema. Esto deja en claro que no solo depende de las medidas de avance tecnológico sino más bien de la organización de la institución y sus colaboradores.

2.4.3 NMAP

También se puede tomar en cuenta el uso de aplicaciones que brindan seguridad al usuario, NMAP es una herramienta muy útil que permite detectar los equipos o dispositivos conectados en una red, verificar que estén conectados solo los autorizados y cubrir o cerrar los que son intrusos, pero así mismo es una herramienta de doble filo, pues debido a su uso común es también muy utilizado por los hackers para acceder a información privada (Martha Irene Romero Castro, 2018).

2.4.4 Metasploit

Es un programa muy útil similar al anterior mencionado, es de código abierto que tiene la particularidad de que permite identificar la vulnerabilidad del servidor, lo que vuelve más fácil combatir las amenazas virtuales. Así mismo es una herramienta que puede jugar en contra de la seguridad informática, debido a que al ser utilizada por las personas equivocadas puede fácilmente filtrarse datos privados de una institución (Martha Irene Romero Castro, 2018).

En la *ilustración 7*, se esquematiza la seguridad del sistema EVA, integrando al usuario como agente de riesgo que debe ser monitoreado, para gestionar de forma adecuada la seguridad del sistema.



Ilustración 7 Relaciones en la seguridad del EVA Fuente: Elaboración propia

A continuación, se presenta un cuadro con las vulnerabilidades físicas/lógicas y la forma de controlarlas, en contraste con la literatura citada.

Vulnerabilidades físicas	Control
Sobretensión, riesgo alto en instalaciones antiguas. En caso de ocurrencia se vería afectada el arranque de alimentación	Conexión moderada de equipos informáticos, sin exceder el número de los mismos, actualmente se tiene mayor control del problema proponiendo un número específico de ordenadores en una red.
Sabotaje, vigilancia o sustracción de información	Uso de softwares que permitan examinar el equipo como TuneUp, Malwarebytes Anti-Malware, SiSoft Sandra 2000 o CCleaner.
Robo de identidad estudiantil	Puede utilizarse un Lector Magnético (carnet estudiantil o tarjeta de identificación) que contenga un chip, el cual debe garantizar un registro único para cada usuario.
Intranet insegura con fácil acceso a usuarios externos a la red y entrada libre a sus sitios WEB	Firewall y servidores Proxys que realicen auditorías de las conexiones permitidas. Software de monitoreo.

Cuadro 1 Lista de vulnerabilidades físicas y sus posibles medidas de control. Fuente: Elaboración propia

Vulnerabilidades lógicas	Control
<p>Password débiles o por default, usuarios con muchas libertades o el uso de protocolos de encriptación obsoletos (que con aplicaciones se pueden crackear en minutos)</p>	<p>Uso de contraseña segura con número de caracteres no menor a 8, utilización de simbología y mayúsculas sin usar datos personales en su estructura o apuntes de la misma en sitios no seguros.</p>
<p>Configuración incorrecta de firewalls. Falta de definición de los objetos, no revisión de logs</p>	<p>Sophos iView es una herramienta que explora datos desde terminales de diferente ubicación, crear copias de seguridad y realizar auditorías. Registra niveles de riesgo y los categoriza. Rastrea ataques DDoS, dificultades en la red o usuarios inusuales en el sistema.</p>
<p>Envío de archivos cifrados por medios no seguros, lo cual vulnera la confidencialidad de la información.</p>	<p>Empleo de firma digital. Debe gestionarse permisos con la entidad correspondiente. Se puede utilizar herramientas de texto virtuales como Significant que permite firmar y guardar el archivo con clave, HelloWorks permite convertir archivos de PDF y firmarlos, OpenOffice Writer permite firmar electrónicamente.</p>
<p>Conexiones de red no seguras.</p>	<p>Utilización de VPN o red de ordenadores que brinda conexiones seguras de la red LAN sobre una red pública.</p>
<p>Vulnerabilidades ocultas</p>	<p>Escaneo web de las debilidades, Acunetix trabaja con proxys que permiten capturar información y a partir de ello puede modificarla, buscar brechas de seguridad en las plataformas web.</p>

Cuadro 2 Lista de vulnerabilidades lógicas y sus posibles medidas de control. Fuente: Elaboración propia

3. CONCLUSIONES

- El monitoreo de ingreso a la plataforma virtual propuesto por la Universidad Técnica de Machala a los usuarios, ayuda en parte, a controlar el riesgo que existe de que se filtre información privada, pero esto solo se vuelve eficiente si se realiza un respectivo seguimiento a cada usuario, en sus actividades dentro del sistema.
- Con el avance de la tecnología y la utilización de nuevas TICs en la formación académica se observa que el riesgo al robo de información también crece, por lo que es conveniente detectar estos problemas a tiempo con el fin de combatirlos antes que causen daños irreparables al sistema o provoquen pérdidas importantes.
- Se aconseja capacitar de manera correcta a los usuarios de las plataformas virtuales, sobre el correcto uso de las cuentas, usuarios y claves; apartando costumbres que puedan perjudicar la seguridad de su cuenta, como escribir la contraseña en lugares inseguros o abrir la misma cuenta en diferentes ordenadores de seguridad limitada.
- Es recomendable utilizar aplicaciones o programas que ayuden a restringir el libre acceso de personas no deseadas a un servidor privado, estas herramientas son útiles para detectar el ingreso inoportuno de individuos y limitar su acceso a la red.
- Se recomienda que, si no es posible almacenar copias de seguridad en sitios de custodio de la institución, se empleen servicios online que manejan políticas de privacidad/seguridad que ayuden a dar protección a las copias de esos datos, cifrando y dándoles una clave de acceso que limitaran el libre acceso a ellas.

BIBLIOGRAFÍA

- ANTEZANA, C. N., GARCÍA, R. S., & RAMOS, G. L. (2014). Evaluación del Aprendizaje en un Ambiente Virtual de Aprendizaje: Un enfoque axiológico. *Universidad Pedagógica de Durango, Universidad Autónoma de Nayarit, CUCSH*, 1-14.
- Frutos, J. V. (2011). *Vulnerabilidades comunes en sistemas de información escolares y posibles soluciones*. Valencia: UNIVERSIDAD POLITÉCNICA DE VALENCIA.
- Gallardo, E. S. (2018). *Universidad Nacional Autónoma de México-Seguridad Informática en entornos virtuales*. Recuperado el Diciembre de 2018, de <https://revista.seguridad.unam.mx/numero-20/seguridad-inform%C3%A1tica-en-entornos-virtuales>
- Geovanny Vega Villacís, R. A. (2017). VULNERABILIDADES Y AMENAZAS A LOS SERVICIOS WEB DE LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO. *3C Tecnología*, 53 – 66.
- Hernán Santiso, J. M. (2016). Seguridad en Entornos de Educación Virtual. *Memoria Investigaciones en Ingeniería*, 2301-1092.
- Jairo, J. (2015). *mind meister*. Recuperado el Diciembre de 2018, de <https://www.mindmeister.com/es/93911009/entorno-de-aprendizaje-auditor-a-de-sistemas?fullscreen=1>
- Leidy Barrera, M. L. (2015). *UNIVO*. Colón. Obtenido de Universidad del Oriente: <https://lovosfrancisco.jimdo.com/app/download/9167889769/SEGURIDAD+FISICA+Y+LOGICA.pdf?t=1504554721>
- Macías-Valencia, S. M.-Z. (2017). Seguridad en informática: consideraciones. *Dominio de las ciencias*, 3(5), 676-688.
- Martha Irene Romero Castro, G. L. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. ALCOY (ALICANTE): Editorial Área de Innovación y Desarrollo,S.L.
- R., J. A. (2012). GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESO DESDE UNA PERSPECTIVA ORGANIZACIONAL. *Ing. USBMed*, Vol. 3, No. 1, 23-34.

- RED CEDIA. (2018). VI CONGRESO ECUATORIANO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. *CAMPUS REVISTA INFORMATIVA DE RED CEDIA #8*, 6-30.
- RUIZ, G. (2010). *La sociedad del conocimiento y la educación superior universitaria*. Recuperado el Diciembre de 2018, de <http://revistas.unam.mx/index.php/rmcpys/article/viewFile/48322/43435>
- UTMACH. (30 de diciembre de 2018). *Universidad Técnica de Machala*. Obtenido de <https://app.utmachala.edu.ec/siutmach/public/>
- Yanet Díaz Ricardo, Y. P. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias. *Ciencias Holguín*, 1-14.
- Zúñiga, R. P., Lozano, P. M., García, M. M., & Hernández, E. M. (2018). La sociedad del conocimiento y la sociedad de la información como la piedra angular en la innovación tecnológica educativa. *Ride Revista Iberoamericana para la investigación y desarrollo educativo*, 8(16), 2-24.