UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE VULNERABILIDADES EN LOS PROCESOS ADMINISTRATIVOS A TRAVÉS DE LOS SERVICIOS VIRTUALES EN UACE-UTMACH

ESPINOZA CASTILLO EVELYN SAMANTHA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE VULNERABILIDADES EN LOS PROCESOS ADMINISTRATIVOS A TRAVÉS DE LOS SERVICIOS VIRTUALES EN UACE-UTMACH

ESPINOZA CASTILLO EVELYN SAMANTHA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE VULNERABILIDADES EN LOS PROCESOS ADMINISTRATIVOS A TRAVÉS DE LOS SERVICIOS VIRTUALES EN UACE-UTMACH

ESPINOZA CASTILLO EVELYN SAMANTHA
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 en los procesos administrativos a través de los servicios virtuales en UACE-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 - 14:25

Urkund Analysis Result

Analysed Document:	ESPINOZA CASTILLO EVELYN SAMANTHA_PT-011018.pdf (D47131947)
Submitted:	1/22/2019 11:26:00 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

La que suscribe, ESPINOZA CASTILLO EVELYN SAMANTHA, en calidad de autora del siguiente trabajo escrito titulado Análisis de vulnerabilidades en los procesos administrativos a través de los servicios virtuales en UACE-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

ESPINOZA CASTILLO EVELYN SAMANTHA
0706744901

RESUMEN

Los procesos administrativos son aquellos que coordinan toda actividad aferente a una organización, integrando permanentemente su operación; dentro de tal contexto la información es el principal activo, en especial para las instituciones de educación superior que facultan la producción científica, formación profesional e imperan en el desarrollo de las naciones. En la universidad técnica de Machala se sustentan varios procedimientos gerenciales mediante sistemas informáticos, los mismos que pese a sus prestaciones y potencialidades, evidencian vulnerabilidades/debilidades representando una amenaza inevitable, poniendo en riesgo la información u otros recursos relacionados al tratamiento de datos. Este complexivo aborda la temática de la auditoria informática al analizar los riesgos latentes, en el desarrollo de gestiones burocráticas solventadas en servicios virtuales; también se evalúa el estado de la temática en contraste con otras entidades académicas; la metodología aplicada es un análisis-deductivo de tipo exploratorio para caracterizar a los controles físico/lógicos necesarios al responder con la mayor eficiencia en caso de ataques informáticos enfocados a la Unidad Académica de Ciencias Empresariales de la UTMACH.

Palabras Clave: vulnerabilidades, servicios, virtuales, administración, auditoria.

ASTRACT

The administrative processes are those that coordinate all activity related to an organization, permanently integrating its operation; Within this context, information is the main asset, especially for higher education institutions that empower scientific production, professional training and prevail in the development of nations. In the Universidad Técnica de Machala several managerial procedures are supported by computer systems, the same ones that in spite of their benefits and potentialities, show vulnerabilities / weaknesses representing an unavoidable threat, putting in risk the information or other resources related to the data processing. This complex deals with the subject of computer audit when analyzing the latent risks, in the development of bureaucratic procedures solved in virtual services; the state of the subject is also evaluated levels in contrast to other academic entities; the applied methodology is an exploratory-deductive analysis to characterize the physical / logical controls necessary to respond with the greatest efficiency in case of computer attacks focused on the Unidad Académica de Ciencias Empresariales of the UTMACH.

Keywords: vulnerabilities, services, virtual, administration, audit.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

1. INTRODUCCIÓN

En el ámbito socioeconómico actual es el deber de toda institución o entidad, buscar una mejora continua y eficiencia en sus procesos de manera íntegra; para lo cual se solicitan sistemas informáticos capaces de gestar funcionalidades departamentales de una empresa por medios computacionales, esto optimiza y automatiza procesos de forma secuencia, facilita compilar cientos o miles de gigabytes en tiempo real gracias a las bondades del internet (Perenguez, 2012). Sin embargo, dichas potencialidades han revolucionado la concepción de riesgos/amenazas en las áreas de trabajo, debido a una sistematización de información que demanda controles físicos-lógicos tanto a los equipos como empleados; es la labor de la auditoria informática determinar el estado de la seguridad e implementar un plan estratégico de manejo que describa las reglamentaciones, políticas e infiera medidas para garantizar la fidelidad de los datos; enmarcando un proceso de retroalimentación entre el desempeño de la institución y su rendimiento desde una perspectiva sostenible (armonizar sociedad-economía-ecosistema). (Quiroz-Zambrano & Macías-Valencia, Seguridad en informática: consideraciones, 2017)

La información constituye uno de los activos más relevantes en las empresas e incide directamente en los resultados organizacionales, dentro del contexto de las instituciones académicas es vital prestar soluciones online, dar servicios que sustenten las necesidades en el proceso de enseñanza-aprendizaje, con la cualidad de conectarse en todo momento, transferir, compartir, publicar o tratar datos de manera vertiginosa, pese a ello el éxito burocrático depende en gran parte del empoderamiento personal/estructura del sistema donde convergen las potencialidades tangibles e intangibles basados en el adecuado uso de los recursos ofimáticos. (Almazán & Quintero, 2017)

La auditoría de sistemas es un conjunto de ciencias esquematizadas en conjeturas interdisciplinarias que buscan elaborar un informe conciso junto a una consultoría completa de los recursos, actividades, acciones, ganancias, objetivos, misión y visión que caracterizan a una institución, la finalidad es aplicar las medidas competentes/necesarias evaluando su seguridad informática en virtud de las relaciones interpersonales, optimización de procesos, servicios administrativos-gerenciales para medir su capacidad de adaptarse a cambios en el entorno, renovar o actualizar su infraestructura tecnológica sintonizada a sus requerimientos; erigir una metodología específica en la cual se analice beneficio-costo en un periodo rentable que exprese competitividad y desarrollo para todos los ámbitos existentes en el estudio. (MORALES & LUNA, 2016)

En la Universidad Técnica de Machala, como toda entidad pública ejerce una amplia gama de procesos administrativos que van desde la planeación, control, seguimiento y evaluación constante al medir el cumplimiento de sus objetivos institucionales, el presente trabajo se enfoca en los procesos que se llevan a cabo a través de los servicios virtuales como seguimiento a graduados, proceso de titulación, gestión de notas (SIUTMACH), programas de beneficio estudiantil, proceso de aprendizaje (EVA), con el objeto de identificar sus vulnerabilidad a par de una respuesta eficiente fundamentada en la auditoria informática.

2. DESARROLLO

2.1 FUNDAMENTACIÓN TEÓRICA

En todo escrito es imperioso argumentar los criterios teóricos, de tal forma que se sustente los conceptos en virtud del entendimiento de la temática, en esta sección se caracterizan las definiciones que delinean la ejecución del trabajo, apreciada desde el marco epistemológico.

2.1.1 Auditoria Informática

Es un conjunto de procesos enfocados en la evaluación/revisión y mejora continua de las cualidades en sistemas computacionales, implementando controles que garanticen la calidad, fidelidad e integridad de la información; así como asegurar una respuesta adecuada en caso de connatos de ciber ataques u otras amenazas que pongan en riesgo la infraestructura informática. (Barrientos & Alva, 2016)

Ilustración 1 Procese de auditoria informática Fuente: Elaboración Propia

2.1.2 Seguridad en sistemas informáticos

Es un proceso integrador, que tiene como objetivo la protección de datos, máquinas, redes o activos informáticos, es de carácter iterativo de mejora continua, demandando

una participación inclusiva de todos los implicados, tanto usuarios como autoridades, además se gesta bajo normativas/configuraciones que responden oportunamente en la prevención o mitigación de afectaciones al sistema. (Aristides Dasso, 2018)

2.1.3 Servicios Virtuales

Son la prestación de actividades vía internet, se coordinan y realizan procesos en forma digital con semejanza a su desempeño convencional, su principal cualidad es que a través de servidores online permiten interactuar usuario/sistema para solventar alguna necesidad perteneciente a la institución. En el ecuador los servicios académicos gestionados en entornos virtuales han demostrado un crecimiento, a la vez un desarrollo acompañado de mayor acogida, gracias a que influyen positivamente en el alcance de la educación, potencian la educación superior e incrementan el número de estudiantes por romper las barreras espacio-tiempo. (Toala-Dueñas, Cruz-Mendoza, Véliz-Vásquez, Zambrano-Sornoza, & Bolívar-Chávez, 2017)

Los servicios administrativos disponibles en el SITMACH son (Universidad Técnica de Machala, 2015):

- Evaluación docente
- Repositorio Sistema de gestión de calidad
- Matricula

Los servicios administrativos accesibles desde el portal web de la UTMACH son (Universidad Técnica de Machala, 2015):

- Correo
- Repositorio Académico
- Aula Virtual
- Blog UTMACH

2.1.4 Vulnerabilidades

Es una condicionante mutua entre una debilidad y amenaza, no existe una sin la otra; es un factor tanto interno como externo, su afectación depende de la exposición a la amenaza; en sistemas informáticos son las falencias en el sistema que son aprovechadas, para efectuar ataques como una mala configuración, software obsoleto, gestión errónea de usuarios, puertos abiertos e incluso fallos en la programación del código fuente. (Acuña, 2016)

2.1.5 Amenazas

Es un riesgo latente, de índole interna/externa; se sirve de alguna debilidad o vulnerabilidad del sistema para ejecutar un ataque, asestar un daño significativo a la

calidad e integridad de datos; en esencia se categoriza como fallos humanos, falencias en la configuración, fallos en procesos sistematizados e intenciones maliciosas, las principales son (T, 2007):

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Espionaje, Sabotaje

2.1.6 Controles Lógicos/físicos

Son las operaciones que permiten responder y detener los ataques informáticos, su función es disminuir las vulnerabilidades a la vez que se fortalecen las debilidades; sin embargo, solo son aplicables si todos los implicados ponen de parte, gracias a que la parte física es la conducta humana que depende la ética, mientras que la lógica del software que configura la red de ordenadores.

Ilustración 2 Esquema de controles internos en una organización Fuente: (DEFAZ & ZAMBONINO, 2017)

2.1.7 Procesos Administrativos

Son todas las actividades encaminadas a coordinar, monitorear, seguir, ejercer funciones u operaciones de una entidad/empresa/institución de forma sistematizada. En la UTMACH dichos procedimientos son (Universidad Técnica de Machala, 2015):

- Coordinar los procesos de contratación pública;
- Coordinar y supervisar las áreas administrativas y financiera;
- Efectuar el seguimiento de los planes, programas y proyectos de carácter administrativo y financiero, y establecer los correctivos necesarios;
- Promover acciones de capacitación y estímulo para el personal de la Universidad Técnica de Machala;
- Supervisar los informes de control en la distribución y cumplimiento de la carga horaria de las y los servidores universitarios;
- Supervisar y coordinar el control administrativo de los bienes de la Universidad Técnica de Machala.
- Valorar, mediante estudios, el rendimiento del talento y humano y proponer acciones para optimizar la ubicación y labores del personal administrativo, trabajadoras y trabajadores;
- Innovar y actualizar manuales de funciones y operativos para el mejoramiento institucional;
- Vigilar el cumplimiento del régimen de disciplina y seguridad interna de la Universidad, de acuerdo a lo establecido en el respectivo reglamento;
- Vigilar el cumplimiento de normas de conservación del medio ambiente, mantenimiento de edificios, aseo, ornato, vialidad e iluminación;
- Autorizar y aprobar gastos del área de su competencia,
- Cumplir las actividades dispuestas por la Rectora o Rector

2.2 MARCO CONTEXTUAL

La seguridad de sistemas operativos involucra no solo a ordenadores, sino a cualquier dispositivo enlazado a una red que transfiera datos, en el caso de los Smartphone pese a ser de código abierto (Linux) existen múltiples amenazas haciendo imperiosa la necesidad de diseñar un software capaz de evaluar, de forma sistematizada las debilidades y efectuar controles paralelamente al estimar el grado de vulnerabilidad e informar sobre los riesgos presentes; la aplicación citada destaca que el control de autentificación es el más significativo, mientras que la instalaciones de softwares sin autorización es el mayor problema en dichos sistemas. (Yánez, Barahona, Naranjo, Fassler, & García, 2017)

En el año 2017, se efectuó uno de los mayores ataques informáticos de la historia mediante el malware Ramsoware wanacry, el cual a través de las redes se introduce en los sistemas operativos y ordenadores gestados en Windows para encriptar los archivos, bloqueando la sesión hasta que se realice un pago de $300 en bitcoins. En base a ello se diseñó un sistema de gestión de información Open Source (OSSIM), que se instala en cualquier servidor para brindar la detección, monitoreo, escaneo de vulnerabilidades, informes de estado y actualización de firmas para reforzar continuamente la seguridad; su ejecución por Plugis, fácil manejo combinada con una respuesta dinámica lo hace idóneo en servicio virtuales. (Fernández, 2018)

En la Universidad Técnica de Machala se han realizado estudios similares sobre seguridad en entornos online, un caso destacable es el análisis de las vulnerabilidades de la plataforma web en la banca virtual del Banco Pichincha, donde se determinó que, pese a la rigurosa autenticación y controles lógicos, reconocimientos de patrones e identificación dinámica de posibles ataques, su mayor riesgo radica en los *usuarios* que no están familiarizados con el entorno, no se han capacitado o en ocasiones acceden desde ordenadores no seguros, gestando accidentalmente robo de información que derivan en pérdidas económicas. (MARCELA, 2018)

En la *ilustración 3* se esquematiza el procedimiento para secuencia la seguridad informática, se enfatiza que es de carácter reciproco e iterativo.

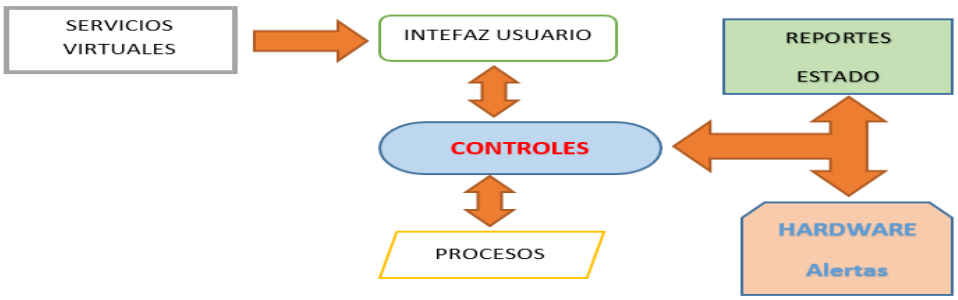

Ilustración 3 Proceso sistemático para identificar/responde a vulnerabilidades en sistemas online Fuente: Elaboración Propia

2.3 MARCO METODOLÓGICO

Son las técnicas racionales que permitan establecer inferencias sobre la problemática, comprender la problemática hasta lograr su resolución fundamentada en la lógica y pericia sobre el tema.

2.3.1 Investigación Bibliográfica

Consiste en adquirir datos e información referente al desarrollo del proyecto, tomados de estudios similares como artículos científicos, trabajos de titulación o cualquier documento que cumpla con el rigor académico competente a un examen complexivo.

2.3.2 Método Lógico Deductivo

Es un procedimiento cognitivo que se compone de indagar del particular a lo general y establecer comportamientos o de lo general a lo especifico, reflejando las nociones que caracterizan las causas-efectos del fenómeno estudiado. (Rodríguez Jiménez & Pérez Jacinto, 2017)

2.3.3 Análisis sistemático

Es un proceso que establece relaciones entre las cualidades y características esenciales del tema, mediante conjeturas basadas en comparaciones hasta lograr una síntesis

lógica del problema, estructurado en interacciones entre las variables que delinean el problema.

2.4 DESARROLLO DEL CASO PRÁCTICO

Uno eje esencial en identificar las vulnerabilidades es conocer las técnicas y metodologías existentes para auditar sistemas, a la par con sus respectivas funcionalidades, los principales son (Miranda, 2015):

- NIST SP 800-30
- OCTAVE
- CRAMM
- MEHARI
- CORAS
- PILAR

Todos los procesos mencionados se basan en analizar entrada del usuario, su interfaz en manejo de información, monitorear procesos e implementar controles para evaluar su desempeño y mejorar constantemente la integridad del sistema.

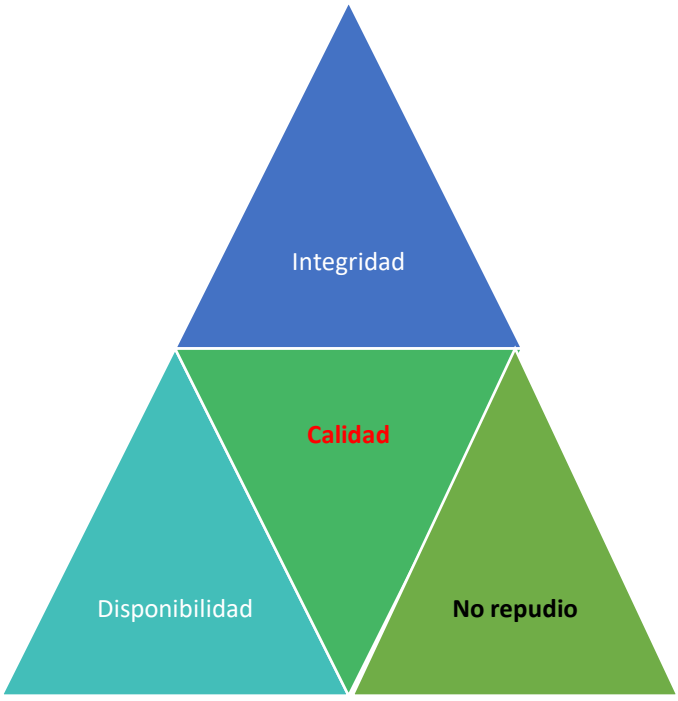

Ilustración 4 Esquema de seguridad en sistemas Fuente: Elaboración propia

2.4.1 Análisis de vulnerabilidades servicios administrativos

Los principales servicios que son susceptibles a falencias y a presentar debilidades en la UACE son:

Correo

Pese a ser institucional, con un sustento corporativo en *Gmail* ostenta ciertas debilidades como infección por vector *malware* que infecta al sistema realizando funciones útiles para el usuario, mientras que en segundo plano realizan funciones nocivas como robo de información, alteración de datos o desactivar seguridades.

La fuga de datos o infiltración también es una amenaza latente, debido a que datos personales, cuentas bancarias o información institucional son objeto de hackers.

El SPAM o correo no deseado es producto de una infección, generalmente por publicidad online que satura la red interna de la empresa mediante incesantes correos tanto a clientes internos como externos.

Aula Virtual

Este sistema opera mediante la plataforma AVA-MOODLE, disponiendo de las siguientes herramientas para evaluar su seguridad:

SQL Map: Inspecciona todos los posibles puntos de la inyección SQL, para analizar el posible comportamiento y salida de aplicativos.

W3AF: Realiza un escaneo de vulnerabilidades en el entorno web a través de pluggins.

Nessus: Es un mecanismo (*Nessus Attack Scripting Language)* que revisa la configuración web, por medio de sondeos programados a modo de aplicación online. (LÓPEZ, ALDANA, & CUERVO, 2014)

Las vulnerabilidades más destacables en entornos virtuales de aprendizaje, de acuerdo a la OPEN WEB APPLICATION SECURITY PROJECT (OWASP) son:

Vulnerabilidad	Descripción
Inyección de código	Inyección SQL que modifica el código del servicio web
Gestión de inicio/rotura de autentificación	Mal manejo en sesiones
Objeto Directo inseguro	Acceso no autorizado por fallos en diseño o configuración
Exposición a datos críticos	Dejar vulnerables datos de inicio, claves, correos o descuidar información valiosa sin encriptación
Uso de componentes	Explota librerías o complementos virtuales para dar acceso al atacante
Redirecciones no válidas	Redirecciones los sitios web a sitios no confiables para suplantar identidad del entorno o infectar con malware

Cuadro 1 Vulnerabilidades en entornos virtuales de aprendizaje según OWASP Fuente: (OWASP, 2018)

Repositorio Digital

Las principales falencias latentes en el medio DSPACE, son:

HTTP Header Injection: Detecta problemas de inyección de cabecera en aplicaciones web que pueden causar serios problemas. El más común de ellos son Cross-site Scripting y secuestro de sesión, tomando la forma de ataques de fijación de sesión.

Insecure Transportation Security Protocol (SSLv2): Verifica que el servidor web está configurado para soportar la comunicación segura a través de un protocolo de transporte inseguro (SSLv2), que posee varias fallas. Los atacantes pueden realizar ataques observando el tráfico de criptografía entre el sitio y los visitantes.

Weak Ciphers Enabled: Identifica que el servidor emplea cifras débiles durante la comunicación segura (SSL), facilitando que intrusos pueden montar ataques de fuerza bruta para descifrar la comunicación segura entre el servidor y los visitantes.

Invalid SSL Certificate: Comprueba que el servidor web utiliza un certificado SSL no válido. Un certificado SSL puede ser creado y firmado por cualquiera, sí el sitio tiene un certificado inválido, los visitantes tendrán dificultad en distinguir entre su certificado y los de atacantes. (Belarmino & Araújo, 2014)

2.4.2 Análisis de controles y medidas de seguridad

Los controles lógicos esenciales, respaldados por la Norma ISO 27002 para evaluación de seguridad en ambientes informáticos online se resumen en el *cuadro 2.*

CONTROL	***DESCRIPCIÓN***
Acceso a las aplicaciones e información	Aislar sistemas sensibles
Gestión de usuarios	Contraseñas, grado de encriptación
Acceso a red	Enrutamiento de red, protección de puertos, aislamiento de direcciones IP, corta fuegos,
Computación móvil y trabajo remoto	Autentificar, verificar protocolos, paquetes de datos, monitoreo de actividades, certificar ejecución de procesos
Acceso a sistema operativo	Identificación, autentificación

Cuadro 2 Controles lógicos normados ISO 27002 Fuente: (ERAZO, GARCES, & MUÑOZ, 2015)

Un control esencial en todo proceso ofimático o servicio virtual es la autentificación e identificación de usuarios; el cual mientras más riguroso sea da mayores garantías; en la UTMACH se gestan mediante contraseñas con signos, combinación de números, letras y mediante mensajes de texto a celulares, además si no reconoce dirección Internet Protocol (IP) de la máquina, donde habitualmente inicia sesión

automáticamente notifica a través de un correo al propietario. La *ilustración 5* expresa el control de inicio en los servicios virtuales.

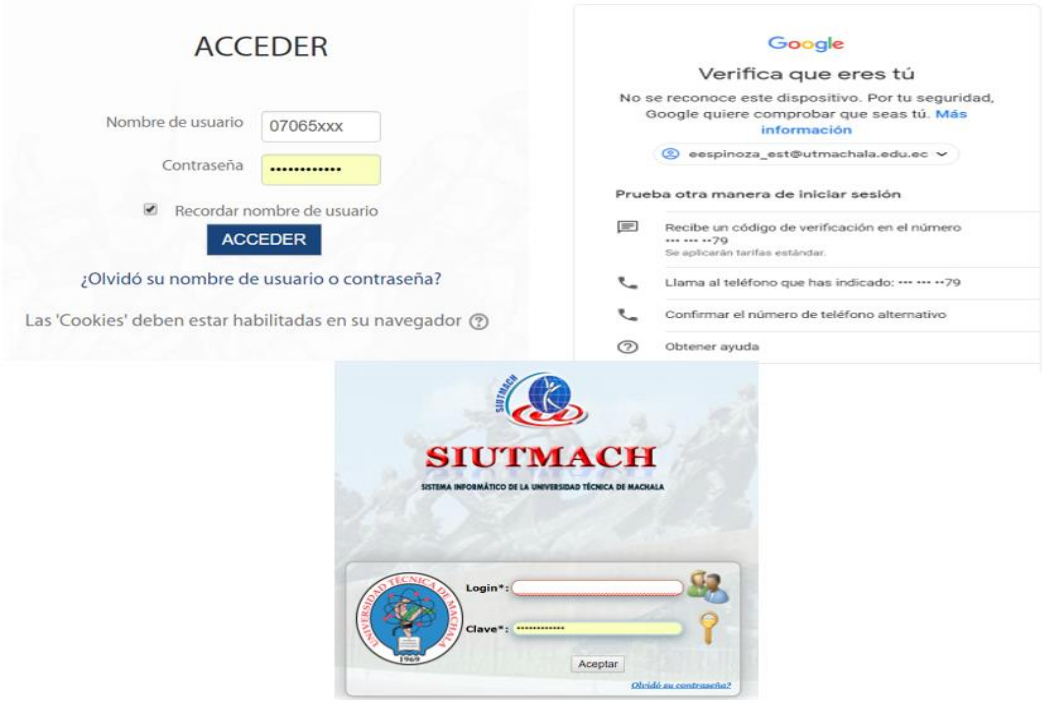

Ilustración 5 Control en el inicio de sesión en servicios online Fuente: (Universidad Técnica de Machala, 2015)

Otro control básico, que se necesita implementar es el certificado Secure Socket Layer (SSL), el cual permite activar el protocolo de seguridad Https, que permite el cifrado de los mensajes intercambiados entre el servidor y ordenador, esto sucede debido a que la UTMACH no cuenta con servidor propio en el EVA (Entorno Virtual de Aprendizaje).

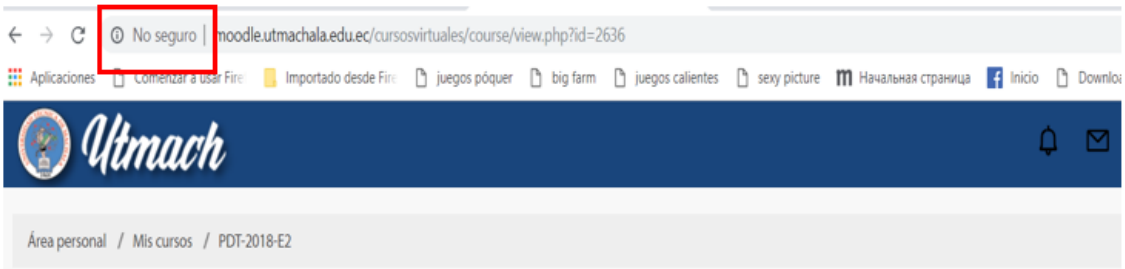

Ilustración 6 Falencias de seguridad en el EVA Fuente: (UTMACH, 2018)

En el portal web de la Universidad Técnica de Machala, donde se pueden acceder a todos los servicios, en especial los informáticos como sección de noticias, blog, servicios académicos y administrativos, gestión de matrículas entre otros, sí cuenta con certificado Https, tal como se observa en la *ilustración 7.*

Ilustración 7 Certificado de seguridad Https en portal web Fuente: (Universidad Técnica de Machala, 2015)

2.4.3 Controles Físicos

Son las regulaciones a *empleados, personal o responsables* de la seguridad y que manipulan al hardware/software que componen al sistema informático, en el cuadro 3 se resumen desde la perspectiva de la investigación.

CONTROLES	***DESCRIPCIÓN***
Antivirus	Mantener instalado y actualizados constantemente
Capacitación	Informar y preparar al personal para responder/prevenir vulnerabilidades informáticas
Biometría e identificación	Implementar reconocimientos a los responsables de la seguridad e integrar medidas rigurosas de autentificación
Copias de seguridad	Respaldar la información y generar copias de seguridad de forma periódica
Normativas y políticas	Diseñar, aplicar y evaluar permanentemente reglamentaciones orientadas a mejorar la seguridad e imponer sanciones a quienes las incumplan

Cuadro 3 Controles físicos aplicables para responder a las vulnerabilidades Fuente: Elaboración Propia

3. CONCLUSIONES Y RECOMENDACIONES

Las vulnerabilidades son manejables mediante gestiones internas e implementos tecnológicos basados en la auditoria informática, las amenazas son externas e inevitables, pero pueden ser disminuidas a través de revisiones periódicas de la seguridad y una mejora continua de defensas/controles del sistema.

Los controles físicos son el eje que desempeña la seguridad en toda institución, la UTMACH no es la excepción por ello capacidad, preparar y contratar personal adecuado al evaluar, monitorear, mejorar e integrar nuevas formas de empoderar al talento humano, gracias a que si esta falla, el sistema es *vulnerado* sin importar los controles lógicos implementados.

Las vulnerabilidades más comunes son la intercepción de datos, falta de certificados de seguridad online, secuestro de sesión, inyección SQL, re direccionamiento web; por lo cual los controles intangibles al software son medidas que reflejan las debilidades para volver al sistema resistente a dichos ataques, no obstante es insuficiente debido a que las amenazas se optimizan día a día, haciendo imperiosa la necesidad de anexar una fase de escaneo de vulnerabilidad y simulación de ataques para estar siempre alertas, denotando una eficiencia constante en el soporte de los procesos administrativos soportados en entornos virtuales.

La seguridad de los servicios administrativos sustentados en sitios web es de calidad regular, cumple con requisitos mínimos, pero sería incapaz de responder o evitar daños a la integridad de datos, tampoco se demuestra que existan copias de seguridad ni encriptación de datos para dificultar su hurto, además de acuerdo al análisis contextual la UTMACH se está quedando atrás en relación a las tecnologías de vanguardia, y evidencia poco desarrollo en la actualización de activos informáticos en especial en la parte del hardware.

Se aconseja que se invierta más en seguridad y renovación de hardware, no solo para mejorar las prestaciones informáticas, sino para automatizar ciertos procesos que son susceptibles a sistematizarse online, también se puede profundizar en el área de auditoria en el diseño de redes institucionales más robustas/confiables.

Se recomienda realizar una investigación más profunda, por la carrera de ingeniería de sistemas que podrían proponer mejores opciones en controles de seguridad y dar un criterio técnico sobre los puntos a trabajar en la UACE, desde la perspectiva de la auditoria informática.

BIBLIOGRAFÍA

Acuña, J. (2016). Análisis de la Vulnerabilidad Institucional en el Distrito Metropolitano de Caracas. *Terra Nueva Etapa, XXXII*(52), 151-175.

Almazán, D. A., & Quintero, Y. S. (2017). Influencia de los sistemas de información en los resultados organizacionales. *Contaduría y Administración , 62*, 303-320.

Aristides Dasso, A. F. (2018). Evaluación de la Seguridad en Sistemas Informáticos . *XX Workshop de Investigadores en Ciencias de la Computaci´on* (págs. 1016-1020). San Luis: Universidad Nacional de San Luis .

Barrientos, O. T., & Alva, M. R. (2016). Auditoría de Sistema de TI como medio de aseguramiento de control en las empresas del Siglo XXI. *Revista Iberoaméricana de las ciencias computacionales e informática, 5*(10), 1-6.

Belarmino, V. F., & Araújo, W. j. (2014). Análise de vulnerabilidades computacionais em repositórios digitais. *Biblios No 56*, 2-17.

DEFAZ, D. F., & ZAMBONINO, K. G. (2017). *FRAUDE INFORMÁTICO, ANÁLISIS DE VULNERABILIDAD EN LAS EMPRESAS DEL SECTOR INDUSTRIAL DE LA PROVINCIA DE COTOPAXI.* Latacunga: UNIVERSIDAD DE LAS FUERZAS ARMADAS.

ERAZO, H. A., GARCES, L. A., & MUÑOZ, P. A. (2015). *IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN DOCUMENTAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA INGELEC S.A.S.* PASTOS: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD.

Fernández, J. L. (2018). *Análisis y gestion de vulnerabilidad en sistemas informáticos con software libre.* Cataluña: Universidad Obserta de Catalunya.

LÓPEZ, A. B., ALDANA, A. C., & CUERVO, M. C. (2014). Vulnerabilidad de ambientes virtuales de aprendizaje utilizando SQLMap, RIPS, W3AF y Nessus*. *INFORMÁTICA No 30*, 247-260.

MARCELA, S. P. (2018). *ANÁLISIS DE LAS VULNERABILIDADES, AMENAZAS Y RIESGOS DE LA PLATAFORMA WEB DE LA BANCA VIRTUAL DEL BANCO PICHINCHA.* MACHALA: UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES-UTMACH.

Miranda, M. F. (2015). *PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA APLICADO EN LA ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.* Madrid: Universidad Politécnica de Madrid.

MORALES, A. P., & LUNA, Y. A. (2016). *ANALISIS DE RIESGOS PARA UNA EMPRESA DE CONSULTORÍA.* BOGOTÁ: INSTTUCIÓN UNIVERSITARIA POLTÉCNICO GRAN COLOMBIANO.

OWASP. (2018). *The OWASP Foundation*. Obtenido de https://www.owasp.org/index.php/Main_Page

Perenguez, L. Y. (2012). *AUDITORÍA INFORMÁTICA EN EL ÁREA DE SISTEMAS E INDICADORES DEL FUNCIONAMIENTO DEL HARDWARE EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S DEL DEPARTAMENTO DE NARIÑO.* Pasto: Universidad de Nariño.

Quiroz-Zambrano, S. M., & Macías-Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, 3*(4), 137-156.

Rodríguez Jiménez, A., & Pérez Jacinto, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista Escuela de Administración de Negocios, núm. 82*, 1-26.

T, C. H. (2007). AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN. *Criminología, 28*(84), 137-146.

Toala-Dueñas, R. A., Cruz-Mendoza, J. C., Véliz-Vásquez, J. R., Zambrano-Sornoza, J. M., & Bolívar-Chávez, O. E. (2017). Valoraciones de los entornos virtuales de aprendizaje en la comunidad universitaria. Ecuador. *Polo del Conocimiento, 2*(5), 1057-1066.

Universidad Técnica de Machala. (2015). *Sistema Informático de la Universidad Técnica de Machala*. Recuperado el Diciembre de 2018, de https://app.utmachala.edu.ec/siutmach/public/

Universidad Técnica de Machala. (2015). *Unidad Académica de Ciencias Empresariales*. Recuperado el Diciembre de 2018, de https://www.utmachala.edu.ec/portalwp/index.php/uace/

Universidad Técnica de Machala. (2015). *VICERRECTORADO ADMINISTRATIVO*. Recuperado el Diciembre de 2018, de https://www.utmachala.edu.ec/portalwp/index.php/vicerrectorado-administrativo/

UTMACH. (2018). *AULA VIRTUAL*. Obtenido de ENTORNO VIRTUAL DE APRENDIZAJE: http://moodle.utmachala.edu.ec/cursosvirtuales/my/

Yánez, H. M., Barahona, A. S., Naranjo, P. M., Fassler, M. I., & García, C. D. (2017). Detección de vulnerabilidades en aplicaciones que funcionan sobre el sistema operativo Android, mediante el desarrollo de una aplicación tecnológica. *ESPACIOS VOL.39*, 1-17.