UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LAS AMENAZAS Y VULNERABILIDADES A LOS SERVICIOS ACADÉMICOS ONLINE DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE UTMACH.

SUAREZ MOROCHO LIZBETH ALEXANDRA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LAS AMENAZAS Y VULNERABILIDADES A LOS SERVICIOS ACADÉMICOS ONLINE DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE UTMACH.

SUAREZ MOROCHO LIZBETH ALEXANDRA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE LAS AMENAZAS Y VULNERABILIDADES A LOS SERVICIOS ACADÉMICOS ONLINE DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE UTMACH.

SUAREZ MOROCHO LIZBETH ALEXANDRA
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 las amenazas y vulnerabilidades a los servicios académicos online de la Unidad Académica de Ciencias Empresariales de 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

ORDÓNEZ BRICEÑO KARLA FERNANDA
0705031003
ESPECIALISTA 2

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 3

Fecha de impresión: viernes 01 de febrero de 2019 - 10:52

URKUND

Urkund Analysis Result

Analysed Document:	SUAREZ MOROCHO LIZBETH ALEXANDRA_PT-011018.pdf (D47120236)
Submitted:	1/22/2019 6:02:00 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, SUAREZ MOROCHO LIZBETH ALEXANDRA, en calidad de autora del siguiente trabajo escrito titulado Análisis de las amenazas y vulnerabilidades a los servicios académicos online de la Unidad Académica de Ciencias Empresariales de 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

SUAREZ MOROCHO LIZBETH ALEXANDRA
0704696996

RESUMEN

El presente documento delinea el proceso relevante y necesario para evaluar mediante un análisis inferencial aplicando una metodología de carácter exploratorio, las vulnerabilidades/amenazas latentes en los servicios académicos que ofrece la Unidad Académica de Ciencias Empresariales, de la Universidad Técnica de Machala, Provincia de EL ORO; se enfoca a los servicios sustentados en sistemas informáticos que son más usados por los estudiantes en su labor de aprendizaje, en contraste con las posibles debilidades y que controles o medidas pueden responder oportunamente antes tales riesgos; desde la perspectiva de la auditoría informática se ejecuta una revisión teórica de grado comparativa e inductivo para establecer relaciones en las falencias de las plataformas virtuales como correo, aula virtual, Siutmach; con el afán de diagnosticar qué medias de vanguardia podrían aplicarse, además se busca determinar el estado de la problemática a nivel contextual deduciendo, cómo se encuentra la UTMACH en el ámbito de la seguridad informática e identificar cuáles criterios deben emplearse para potenciar el desarrollo institucional a través de las gestiones académicas solventadas en las nuevas tecnologías de la información y comunicación (NTIC´s).

Palabras Clave: Análisis, vulnerabilidades, servicios académicos, auditoría.

ABSTRACT

This document delineates the relevant and necessary process to evaluate by means of an inferential analysis applying an exploratory methodology, the vulnerabilities / latent threats in the academic services offered by the Unidad Académica de Ciencias Empresariales, of the Universidad Técnica de Machala, Provincia de EL ORO; it focuses on services supported by computer systems that are more used by students in their work of learning, in contrast to possible weaknesses and that controls or measures can respond in a timely manner before such risks; from the perspective of the computer audit a theoretical revision of comparative and inductive degree is carried out to establish relationships in the shortcomings of virtual platforms such as mail, virtual classroom, Siutmach; In addition, the aim is to diagnose which avant-garde means could be applied, in addition to determining the status of the problem at a contextual level, by deducting how the UTMACH is in the field of computer security and identifying which criteria should be used to enhance institutional development. through the academic efforts solved in the new information and communication technologies (NICTs).

Keywords: Analysis, vulnerabilities, academic services, audit.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

INTRODUCCIÓN

La era digital solventa la sociedad actual mediante sistemas informáticos, que prestan servicios o plataformas al virtualizar procesos con mejores potencialidades en contraste con los procedimientos cotidianos, en el entorno empresarial es vital lograr la competitividad a través de la optimización de procesos administrativos-productivos sustentados en soluciones tecnológicas que van a la par del desarrollo organizacional, donde impera una gestión íntegra de datos e información (Martelo & Maza, 2018). El papel de las instituciones de educación superior en dicho contexto, es formar profesionales dinámicos, capaces y conscientes al suplir las necesidades/problemáticas en su área de influencia; también se destaca que la ética, responsabilidad e integridad en conocimientos teórico-prácticos depende del desempeño de la entidad educativas, en gran medida se ve afectada por los recursos tecnológicos que viabilizan el proceso de aprendizaje, así como la calidad del cuerpo docente (Avalos, 2017).

Debido a la globalización de los sistemas informáticos en toda noción contemporáneas se ven optimizados las funciones asociadas al manejo de grandes cantidades de información, flujo de datos, accesibilidad a contenido, conectividad a internet (redes sociales); esto demanda la aplicación de la *auditoría informática* como un activo en toda organización, empresa o institución, gracias a que permite estructurar un plan de seguridad integral conjugando las medidas cautelares para reducir vulnerabilidades/amenazas, mantener secretos corporativos e incrementar la eficiencia de forma constante a favor de los objetivos estratégicos, a la vez que se mantiene una cultura jerárquica en los funcionarios tanto externa como interna de carácter retroalimentativa (Parada & Gómez, 2018).

Los servicios académicos son todos los procesos que facilitan el proceso de aprendizaje desde la investigación científica hasta bienestar estudiantil, particularmente en la Universidad Técnica de Machala, se tienen los siguientes servicios: Seguimiento a graduados, Repositorio académico, U.B.E, Centro de idiomas, inscripción D.N.A, Fielweb, Blog, consultorio jurídico, Aula virtual, Biblioteca Universitaria y correo (UTMACH, 2015), el estudio se centra en los controles de seguridad de los servicios más relevantes, que son mayormente empleados por los estudiantes de la Unidad Académica de Ciencias Empresariales, con el objeto de identificar cuáles son sus principales amenazas/vulnerabilidades, proponiendo las posibles soluciones para controlar el grado de afectación al sistema institucional y analizar en qué estado se encuentra el nivel de seguridad implementado en la UTMACH en referencia al entorno macro, meso y micro.

1. FUNDAMENTACIÓN TEÓRICA

En esta sección se destacan las definiciones y terminologías más relevantes en sustentar epistemológicamente la base cognitiva del escrito, es imperioso recalcar que dichos pretextos son caracterizados desde el punto de vista del autor, a favor del desarrollo de la problemática.

1.1 Auditoría informática:

Es un proceso iterativo, que se retroalimentada en cada aspecto de la seguridad en sistemas computacionales, permite evaluar las vulnerabilidades, debilidades, fortalezas y posibilidades de mejoría en el sistema de forma íntegra, mediante la emisión de un informe que detalla las accionantes a implementar. (Arcentales-Fernández & Caycedo-Casas, 2017)

Ilustración 1 Proceso de la auditoría informática
Fuente: Elaboración propia

1.2 Seguridad Informática:

Es una filosofía para la sociedad post moderna, en especial para actividades afines al estudio, debido a las múltiples amenazas/vulnerabilidades relativas al uso del internet, además del uso de celular pone en riesgo la información personal o datos valiosos, dentro de este marco la seguridad se define como un conjunto de saberes interdisciplinarios destinados a prevenir, identificar e integrar mecanismos al garantizar la fidelidad, calidad e integridad de datos en cualquier sistema electrónico (Hernández & Ibarra*, 2018).

1.3 Servicios Académicos:

Son el conjunto de prestaciones que facilitan las herramientas a los docentes para validar su labor y a los estudiantes para gestar su aprendizaje, en las universidades involucran a todo proceso de enseñanza e índole investigativa, actividades curriculares como proyectos o trabajos relacionados a la formación profesional (Vega-Robles, Acosta, Cadena-Badilla, & Quiroga, 2015).

En la Unidad Académica de Ciencias Empresariales los servicios académicos solventados en el portal web, se aprecian en la *ilustración 2.*

Ilustración 2 Servicios académicos que ostenta la UACE
Fuente: (UTMACH, 2015)

1.4 Servicios Online:

Son las prestaciones que pueden desarrollarse mediante procesos virtuales a través de las bondades Cloud Computing o sistemas informáticos en aplicativos web, en el ámbito educativo se refieren a las facilidades en el aprendizaje e innovación pedagógica, fomentan el uso de programas y entornos digitales para romper esquemas, incrementar los parámetros de evaluación, mejorar cualidades de enseñanza, volver más dinámica a la docencia, también se destacan que por su carácter de disponibilidad, almacenamiento e integración paralela a los procesos cotidianos han tenido un impacto positivo, tal es el caso del software Geogebra en el aprendizaje de las asignaturas afines a las matemáticas (Rueda, 2018).

1.5 Vulnerabilidades:

Son todas las debilidades, errores o falencias en un sistema informático que pueden derivar en ataques o poner en riesgos los datos gestionados; en esencia son de

diseño, implementación y uso, sin embargo, las más comunes en plataformas web de aprendizaje son:

- Cross Site Scripting
- Cross Site Scripting Reflejado
- Cross Site Scripting Persistente
- Conducta de usuarios externos e internos
- Hombre en el medio (Llanos & Erazo, 2018).

Las debilidades citadas aprovechan carencias de seguridad en certificados Https, fallos en el protocolo o descuido de transferencia de datos, además los principales agentes son los scripts, malware u otros medios para manipular el código de la página online.

1.6 Amenazas:

Son los agentes, factores o condicionantes que se valen de las vulnerabilidades para efectuar un ataque al sistema computacional, no forman parte del sistema sino del bando contrario. Están estrechamente relacionada a la vulnerabilidad, si la una no existe la otra; comúnmente son hackers, empresas rivales, usuarios, clientes internos o simplemente profesionales con dominio de la ingeniería de software que buscan beneficio propio a costa de la integridad de datos.

Los principales ataques realizados a sitios web se enlistan a continuación:

- Denegación de servicios distribuida
- Inyección SQL
- Ataques de fuerza bruta
- Inspección manual de código fuente
- Manipulación de cabeceras HTTPS (SÁNCHEZ & PRIETO, 2018)

1.7 Riesgo:

Es la posibilidad de que ocurra un impacto o consecuencia adversa a un sistema, es el resultado de concatenar vulnerabilidad y amenaza en un medio, cuyas accionantes permitan un ataque informático, siempre existe un riesgo sin importar las seguridades implicadas en la protección del entorno (MENDOZA, 2017).

1.8 Medidas de seguridad:

Son los controles, comportamientos, configuraciones y actividades orientadas a garantizar la protección de los activos informáticos, en el ambiente académico han pasado al segundo plano, no obstante, debido al auge de la informática e incidentes

relacionados a redes e internet, se han intensificado los estudios para mejorar las potencialidades de los entornos virtuales a través de la auditoría de sistemas. Su uso no se limita al software ni hardware, exige responsabilidad, comportamiento ético cohesionados por un empoderamiento hacia la institución por parte de todos los involucrados, en especial los estudiantes que son la razón de ser de las universidades (Hernández & Ibarra, Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios, 2018).

Desde la temática se define el proceso necesario para implementar medidas de seguridad en respuesta de las vulnerabilidades, tal como se observa en la *ilustración 3.*

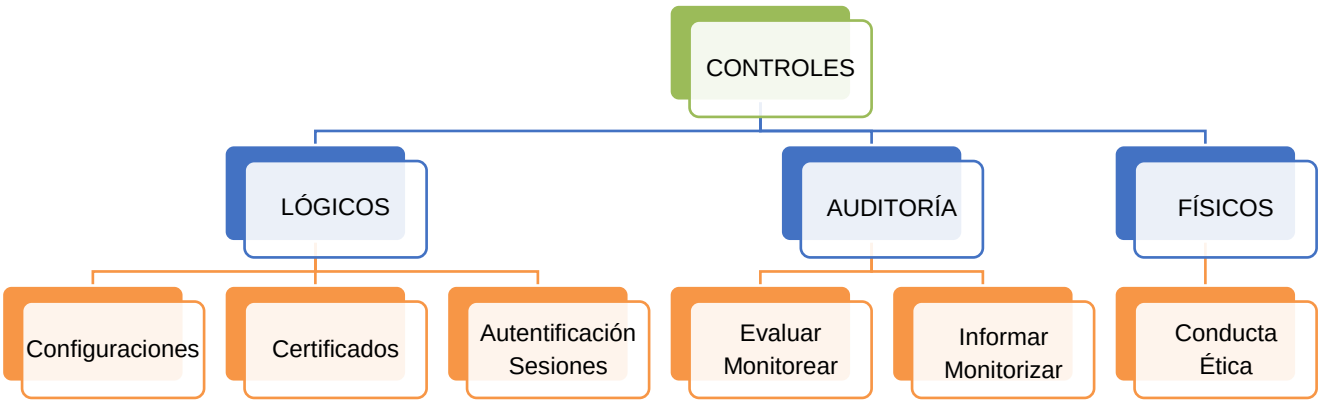

Ilustración 3 Esquema de controles en vulnerabilidades en ambientes virtuales
Fuente: Elaboración Propia

2. METODOLOGÍA

Son las técnicas necesarias para adquirir, tratar e interpretar información que permita sustentar el desarrollo del trabajo desde su concepción epistemológica hasta los resultados objetados en su desarrollo.

2.1 Investigación Bibliográfica

Es indagar en documentos afines a la problemática, como artículos de revistas científicas, publicaciones de bibliotecas virtuales de universidades, PDFs, trabajos de grado o cualquier estudio similar que permita argumentar las opiniones expresadas en el proyecto.

2.2 Análisis de Contenido

Comprende las relaciones establecidas entre criterios de diversos autores sobre el objeto de estudio, su carácter es tanto cualitativo como cuantitativo, además de inductivo/deductiva dependiente exclusivamente de las capacidades cognitivas de quien lo utiliza, al interpretar la información apreciada.

2.3 Observación

Es una técnica que infiere comportamiento de un fenómeno o describe una situación mediante la contemplación sistemática y detallada de las cualidades, sin intervenir en las relaciones de las variables ni modificar sus características para obtener una abstracción lo más natural de la realidad cuestionada (Pulido Polo, 2015).

3. MARCO CONTEXTUAL

El estado de la problemática, referenciado a nivel espacial de lo general al caso particular de la localidad, en el cantón Machala expresa que consideraciones o tendencias deben considerar en su tratamiento actual.

3.1 Macro:

En el medio internacional se evidencia una constante evolución de malware, códigos auto programables de difusión automática que burlan e afectan sistemas, como el renombrado caso *Ransomware WannaCry* que busca exigir un rescate o simplemente dañar datos o corromper la información; uno de los detonantes es la falta de cultura en seguridad de los usuarios que no vieron actualizaciones automáticas como amenaza, ni se percataron de tráfico web malicioso cifrado anexado en las paquetes de datos extremo a extremo; esto evidencia la falta de una normativa de carácter regulatorio, de taxonomía, penalización e integración de las naciones frente a la protección de datos, que ya despunta como problema social en toda organización o entidad pública/privada (CISCO, 2018).

Una falencia común es la falta de una *Plan Maestro de seguridad*, en municipios, universidades, instituciones u organización que no invierte lo suficiente, para mantener una inseguridad óptima en sus activos informáticos.

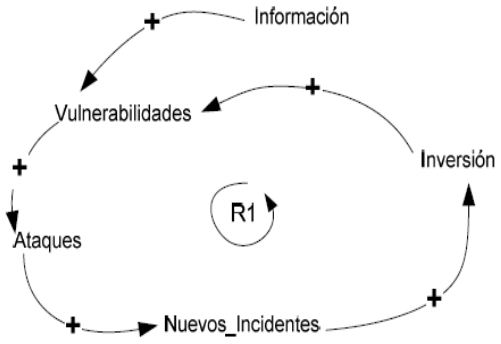

Ilustración 4 Variables en medidas de seguridad en instituciones
Fuente: (Gil Vera & Gil Vera, 2017)

3.2 Meso:

En el Ecuador en los últimos años, se ha tomado mayor conciencia sobre la ciber seguridad e integridad de datos, como resultado se han implementado normativas: *ACUERDO NO. 166 DEL 19 DE SEPTIEMBRE DE 2013 ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) Y* LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS, que buscan proteger tanto al usuario como al sistema, también se denota que el mayor problema es la *ingeniería social*, descuidos en controles físicos al personal interno; a la vez se concluye que la mejor alternativa es el *hardening* siendo capaz de robustecer al sistema por medio de la autenticación, cifrado, y respaldo con la meta de dificultar el robo de información a quien intenta vulnerarla (Pablo Adriano Alarcón Salvatierra, 2016).

Nacionalmente se ha intensificado el acceso a internet, desarrollo en calidad de servicios online, empoderamiento de datos como activos empresariales, pero se evidencia poca acogida a normativas internacionales o convenios de lucha contra ciberdelitos, además desmarca una falta de cultura en seguridad de información, en especial en la índole personal que se traduce como debilidad institucional.

Ecuador se encuentra en el sexto puesto de 19 países de Latinoamérica en cuestiones de ciberseguridad, también es importante destacar que los problemas más recurrentes se dan por *redes sociales*, estafas en empresas y *robo de cuentas* en las entidades bancarias (Anchundia-Betancourt, 2017).

3.3 Micro:

En la Unidad Académica de Ciencias Empresariales, se realiza la auditoría informática de los laboratorios de cómputo, donde se determinó que las vulnerabilidades derivan de no implementar políticas de seguridad, protocolos de comportamiento, restricciones a los usuarios, falta de capacitación y concientización en el uso de recursos virtuales: se verificó que los ordenadores, redes e insumos cuentan con lo necesarios para cumplir con las funciones afines al ejercicio de la cátedra (LILIBET, 2018).

Una indagación de vulnerabilidades en los servicios web del Banco de Pichincha, avalada por la UTMACH notifica que, pese a los estrictos controles en inicio de sesión, autenticación, comportamiento y monitoreo de procesos, la principal deficiencia está en el cliente, ya sea por descuido o desconocimiento de aperturas que viabilizan la ejecución de los ataques, culminando en robo de cuentas o pérdidas económicas (MARCELA, 2018).

4. DESARROLLO

Los servicios académicos que son de mayor urgencia, por su impacto en el desarrollo del aprendizaje y prestaciones pedagógicas, son evaluados en base a la relación vulnerabilidad-control, bajo sintaxis de causa-efecto.

4.1 Red WLAN (Wireless Local Area Network)

Es el principal servicio, gracias a que permite la libre circulación de información facilitando el acceso a internet a través de laptop, dispositivos móviles, ordenadores de escritorio, a más de sustentar los entornos digitales que dan cabida a los servicios web académicos.

El primer paso en gestionar la seguridad es conocer los posibles ataques, luego evaluar las vulnerabilidades que posibilitan dichos connatos, finalmente aplicar medidas que contrarresten las afectaciones, dentro de los estándares internacionales más relevantes como IEEE 802.11i, WEP (Wired Equivalent Privacy), WPA (Wireless Protected Access) y OWASP (Open Web Application Security Project), cuyo análisis se resumen en el cuadro 1.

		WEP	WPA	802.11i	IPsec VPN
Autenticación	Autenticación	WEP	802.1X + EAP	802.1X + EAP	IKE de máquina, X-AUTH de usuario
	Pre-autenticación	No	No	802.1X (EAPOL)	Si
Cifrado	Negociación del cifrado	No	Si	Si	Si (DES, 3DES, AES)
	Cifrado	RC4 40-bit o 104-bit	TKIP: RC4 128-bit	CCMP: AES 128-bit	ESP: DES 56-bit, 3DES 168-bit, AES 168, 128, 192, 256
	Vector de inicialización	24 bits	48 bits	48 bits	DES-CBC 8 bytes
	Integridad de la cabecera	No	MIC	CCM	AH
	Integridad de los datos	CRC-32	MIC	CCM	AH/ESP
	Protección de respuesta	No	Fuerza secuencia de IV	Fuerza secuencia de IV	Si
	Gestión de claves	No	Basada en EAP	Basada en EAP	IKE (Diffie-Hellman)
	Distribución de clave	Manual	802.1X (EAP)	802.1X (EAP)	Diffie-Hellman
	Clave asignada a:	Red	Paquete, sesión y usuario	Paquete, sesión y usuario	Usuario
	Clave por paquete	Concatenación de IV	Mezclado TKIP	No necesario	ESP
Otros	Seguridad ad-hoc	No	No	Si (IBSS)	No

Cuadro 1 Medidas aplicables a redes de internet en la UTMACH
Fuente: (Pellejero, Lesta, & Andreu, 2018)

4.2 Correo institucional

Este medio permite la comunicación entre docentes, estudiantes e integrantes de la comunidad universitaria, con actividades estrictamente relacionadas a fines académicos, pese a su control en identificación de usuario, autenticación por celulares

y reconocimiento de IP, se propone una nueva medida que combina el cifrado con un reconocimiento facial para validar que solo el propietario, tenga permiso de iniciar sesión, esta técnica identifica el rostro, calcula coeficientes de correlación y mediante derivadas realiza una secuencia de caracteres cifrados en virtud de los parámetros biométricos del usuario, dando una clave diferente en cada inicio, además estima cambios en el error de autentificación dando mayor confiabilidad al acceso.

En la *ilustración 5*, se observa el diagrama de flujo del algoritmo mencionado.

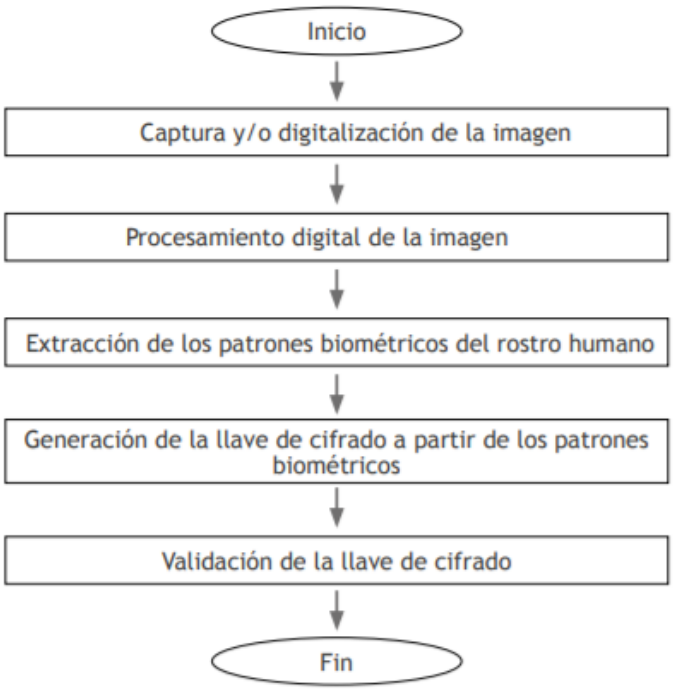

Ilustración 5 Proceso de cifrado basado en biometría para acceso a correos
Fuente: (Rodríguez, 2015)

4.3 SIUTMACH

Debido a que un sistema complejo, constante de múltiples usuarios, chat online, gestor de archivos, foros, notas, y más, se recomienda implementar un control versátil que responda a todas las vulnerabilidades combinando defensa/ataque, esto se logra con la método Domain Flux, se deriva de los procesos Double Flux/Fast Flux; consiste en usar el comportamiento de los botnets (programas robot), En un cambio constante y asignación de múltiples FQDN (Fully Qualified domain name) a una única dirección IP, lo que hace es asignar dinámicamente direcciones IP aleatorias que duran alrededor de un día, confundiendo a los malware o atacantes que al intentar conectarse una a una a las miles de direcciones, terminan sin identificar la correcta, gracias a que alteran automáticamente su dominio. (ORTEGA, 2018)

4.4 Repositorio

Es un archivo online donde se almacenan los documentos derivados, de la producción científica o estudios de la UTMACH, por lo que su mayor vulnerabilidad es la pérdida de información que se puede evitar mediante copias de seguridad periódicas, almacenamiento en la Nube, y educar a los usuarios para que cuiden la red informática de la universidad, no pongan en riesgos a los activos intangibles.

5. CONCLUSIONES Y RECOMENDACIONES

- Las vulnerabilidades en esencia son debilidades desatendidas, los controles son medidas de reforzar dichas falencias, haciendo al sistema resistente a los ataques, pese a ello la auditoría informática es vital para toda institución, en la UTMACH aún no se toma cultura en seguridad digital, por lo cual, aunque existen tecnologías, alternativas de protección, sino se evalúa ni gestiona adecuadamente los activos informáticos, no sirve aplicar controles lógicos ni físicos.
- Se evidencia una necesidad imperiosa de renovar las normativas de seguridad y políticas de uso de sistemas informáticos, ponerse al tanto de las últimas innovaciones en controles de seguridad y estar alerta para evitar ataques, un claro ejemplo es la metodología Domain Flux que oculta al sistema de sus amenazas, a la vez se requiere la intervención de profesionales especializados para potenciar los servicios académicos gestados en plataformas web e investigar mejores bondades tecnológicas en el desarrollo institucional de la UTMACH.
- El eslabón débil en todo sistema computacional a nivel nacional, son los USUARIOS o clientes internos, quienes, por falta de conocimiento, confusiones éticas, descuido o falta de empoderamiento ponen en riesgo a la calidad de datos, debido a que son el principal medio por el cual se efectúan los ataques, se concluye que el control más importante es la culturización de los estudiantes promoviendo un cambio en la mentalidad de la población, donde las universidades juegan un rol trascendental, gracias a su papel como entidad educadora.
- Actualmente en el mercado existen excelentes medidas que permiten robustecer a un entorno web, facultan su desarrollo y eficiencia, sin embargo, la UTMACH se queda rezagada hasta cierto punto, por no invertir ni investigar en desarrollo o implementación de tecnologías de vanguardia en la seguridad informática, además no realiza capacitaciones para retroalimentar conocimientos en el área.
- Se aconseja realizar un escaneo exhaustivo de todo el sistema informático de la universidad, con la finalidad de identificar oportunamente vulnerabilidades y aplicar controles, el hackeo ético o softwares de monitoreo (Kali Linux), facilitan dicha tarea e incluso acogen normativas internacionales en el campo de la ciberseguridad.

6. BIBLIOGRAFÍA

Anchundia-Betancourt, C. E. (2017). Ciberseguridad en los sistemas de información de las universidades. *Dominio de las Ciencias*, 200-217.

Arcentales-Fernández, D. A., & Caycedo-Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias*, 157-173.

Avalos, R. A. (2017). *Modelo ServQual Académico como factor de desarrollo de la calidad de los servicios educativos y su influencia en la satisfacción de los estudiantes de las carreras profesionales de la Universidad Nacional Chimborazo Riobamba – Ecuador.* Lima: UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS.

CISCO. (2018). *Reporte Anual de Ciberseguridad de Cisco.* San José -EEUU: Comparativo de Capacidades de Seguridad de Cisco.

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de Sistemas. *Scientia Et Technica, vol. 22*, 193-197.

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

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

LILIBET, R. M. (2018). *AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LOS LABORATORIOS DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH.* Machala: Universidad Técnica de Machala-UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES.

Llanos, D. F., & Erazo, L. D. (2018). Metodología contra Vulnerabilidades en Ambientes de Aprendizaje Virtuales. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 282-291.

MARCELA, S. P. (2018). *ANÁLISIS DE LAS VULNERABILIDADES, AMENAZAS Y RIESGOS DE LA PLATAFORMA WEB DE LA BANCA VIRTUAL DEL BANCO PICHINCHA.* Machala: Universidad Técnica de Machala-UACE.

Martelo, R. J., & Maza, L. C. (2018). Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. *Información Tecnológica, 29*(1), 3-10.

MENDOZA, D. F. (2017). *ANÁLISIS DE RIESGOS APLICADO A LA SEGURIDAD DEL SITIO WEB DE LA CORPORACIÓN DESARROLLO Y PAZ DEL CANAL DEL DIQUE Y ZONA COSTERA.* CARTAGENA DE INDIAS: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD).

Pablo Adriano Alarcón Salvatierra, R. A. (2016). LA IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA EN LAS INSTITUCIONES GUBERNAMENTALES (ECUADOR). *Caribeña de Ciencias Sociales*, 2-9. Obtenido de Caribeña de Ciencias Sociales: http://www.eumed.net/rev/caribe/2016/11/seguridad.html

Parada, D. J., & Gómez, A. F. (2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. *Análisis de los Compone, 29*(1), 27-38.

Pulido Polo, M. (2015). Ceremonial y protocolo: métodos y técnicas de investigación científica. *OPCIÓN*, 1137-1156.

Rueda, R. A. (2018). Uso del servicio en la nube GeoGebra durante el proceso enseñanza-aprendizaje sobre las matemáticas. *Revista Iberoamericana para la investigación y el desarrollo Vol.18*, 1-30.

SÁNCHEZ, M. V., & PRIETO, D. A. (2018). *ANÁLISIS DE AMENAZAS, RIESGOS Y VULNERABILIDADES DEL PORTAL WEB DEL COLEGIO CATÓLICO JOSÉ ENGLING MEDIANTE HACKEO ÉTICO PARA EL DISEÑO Y DESARROLLO DE UN APLICATIVO WEB DE MONITOREO DE INCIDENCIAS.* QUITO: UNIVERSIDAD POLITÉCNICA SALESIANA.

UTMACH. (2015). *UTMACH (PORTAL WEB)*. Recuperado el Diciembre de 2018, de https://www.utmachala.edu.ec/portalwp/

Vega-Robles, A., Acosta, A. M., Cadena-Badilla, M., & Quiroga, J. V. (2015). Análisis de la calidad de los servicios académicos: caso de estudio Ingeniería Industrial y de Sistemas Campus Caborca, Universidad de Sonora, México. *Revista de la Facultad de Ingeniería Industrial*, 20-26.