UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE CONTROLES DE SEGURIDAD DEL SISTEMA ACADÉMICO DE LA UNIVERSIDAD TÉCNICA DE MACHALA

MORENO ERRAES TANIA RAQUEL
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE CONTROLES DE SEGURIDAD DEL SISTEMA ACADÉMICO DE LA UNIVERSIDAD TÉCNICA DE MACHALA

MORENO ERRAES TANIA RAQUEL
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE CONTROLES DE SEGURIDAD DEL SISTEMA ACADÉMICO DE LA UNIVERSIDAD TÉCNICA DE MACHALA

MORENO ERRAES TANIA RAQUEL
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

ORDÓÑEZ BRICEÑO KARLA FERNANDA

MACHALA, 18 DE JULIO DE 2018

MACHALA
18 de julio de 2018

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado ANÁLISIS DE CONTROLES DE SEGURIDAD DEL SISTEMA ACADÉMICO DE LA UNIVERSIDAD TÉCNICA DE MACHALA, 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.

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
TUTOR - ESPECIALISTA 1

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

PARRA OCHOA EUDORO BENITO
0701063406
ESPECIALISTA 3

Fecha de impresión: martes 17 de julio de 2018 - 20:47

Urkund Analysis Result

Analysed Document:	MORENO ERRAES TANIA RAQUEL_PT-010518.pdf (D40253781)
Submitted:	6/19/2018 3:30:00 AM
Submitted By:	tmoreno_est@utmachala.edu.ec
Significance:	1 %

Sources included in the report:

https://dialnet.unirioja.es/servlet/articulo?codigo=6326645

Instances where selected sources appear:

1

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, MORENO ERRAES TANIA RAQUEL, en calidad de autora del siguiente trabajo escrito titulado ANÁLISIS DE CONTROLES DE SEGURIDAD DEL SISTEMA ACADÉMICO DE LA UNIVERSIDAD TÉCNICA DE MACHALA, 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, 18 de julio de 2018

MORENO ERRAES TANIA RAQUEL
0705724557

RESUMEN:

El presente trabajo documenta un estudio acerca de los controles de seguridad implementados en el sistema académico de la Universidad Técnica de Machala, desde una perspectiva descriptiva e inductiva a nivel macro, meso y micro en base a artículos científicos e investigaciones similares, también se propone los controles a implementar en función de las vulnerabilidades identificas en los servicios online de la Utmach en base a las necesidades como institución según su desarrollo académico, la naturaleza de la problemática es compleja debido a que concatena recursos tanto tecnológicos como lógicos que son responsables de detectar, denegar, informar y tomar acciones retroalimentativas hacia los encargados de resguardar los activos informáticos de la universidad; por ello se postula un análisis comparativo donde finalmente se identifique medidas existentes, además de las posibles amenazas o accionantes a tomar en relación a otras universidades que han pasado por el mismo proceso.

Palabras Clave: Controles, seguridad, sistema, académico, Utmach.

ABSTRACT:

This paper documents a study about security controls implemented in the academic system of the Technical University of Machala, from a descriptive and inductive perspective at the macro, miso and micro level based on scientific articles and similar research. controls to be implemented based on the vulnerabilities identified in Utmach's online services based on the needs as an institution according to their academic development, the nature of the problem is complex because it concatenates both technological and logical resources that are responsible for detecting, deny, inform and take feedback to those responsible for safeguarding the computer assets of the university; for that reason, a comparative analysis is postulated where finally existing measures are identified, in addition to the possible threats or actions to take in relation to other universities that have gone through the same process.

Keywords: Controls, security, system, academic, Utmach.

ÍNDICE DE CONTENIDOS

Contenido

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

1. INTRODUCCIÓN:

La seguridad informática se ha convertido en un activo clave para toda empresa o institución que gestione información en sus procesos tanto internos como externos, debido a que su operatividad requiere una transferencia, actualización y tratamiento dinámico de datos en tiempo real; los controles de seguridad no son un medio ni una imposición sino más bien un adecuamiento de gestiones que constituye una fortaleza imperiosa en la búsqueda de la competitividad, gracias a que aparte de proteger a la red se provee de una retroalimentación constante a los componentes tanto físicos como lógicos que integran los sistemas informáticos de la empresa corrigiendo los errores o fallos apreciados en el desenvolvimiento de la organización. (Miranda, Puga, Mallea, Cobas, & Zequeira, 2016)

Paulatinamente con el auge de las TIC´s se ha exponenciado la cantidad de ataques, herramientas, metodologías e incluso los objetivos de la intrusión, lo cual dificulta identificar al agresor o establecer un mecanismo de defensa a nivel institucional, por ello hoy en día existen diversas tácticas en distintas topologías de ataques con la finalidad de adaptarse estratégicamente a los riesgos particulares que ostenta la entidad en sus sistemas. (Carvajal, Bayona, & Bayona, 2013)

1.1 CONTEXTUALIZACIÓN

A nivel general se estiman un conjunto de alternativas de defensa para salvaguardar los sistemas informáticos, tales como servidor implementado en Linux, programa de detección y estimación de ataques, modelo de seguridad básica; de forma oportuna estas medidas buscan equilibrar las vulnerabilidad respecto a las fortalezas del sistema en función de los riesgos que la rodean, sin embargo los hackers, virus, gusanos, malwares, adwares u otros agentes maliciosos evolucionan progresivamente e inclusive con mayor audacia que las medidas de seguridad, además ningún dispositivo por sofisticado que sea libra del mal uso de las redes, así como la falta de controles o fallos en la autorización de actividades. (MOLINA, MENESES, & SILGADO, 2009)

En la mayoría de los casos se dan ataques vía web donde el actuador es un código maliciosos infectado en la URL, también se presentan un porcentaje considerable por parte de los propios usuarios que hacen mal uso de sus privilegios dentro de la red, esto se puede mitigar según las competencias del analista de sistemas encargado u operario designado, desde una perspectiva superficial se analizan las contramedidas a tomar para evitar o disminuir el riesgo de los ataques, tales como algoritmos de detección, plan de manejo logístico en el sistema académico. (Martelo, Tovar, & Maza, 2018).

1.3 OBJETIVO GENERAL

Analizar los controles de seguridad del sistema académico de la Universidad Técnica de Machala

Los objetivos específicos que linealizan el desarrollo del proyecto se describen a continuación:

- Realizar una revisión teórica a nivel macro, meso y micro sobre la temática de estudio a través de una investigación bibliográfica para comprender la problemática.
- Identificar los controles de seguridad que se implementan en el sistema académico de la Utmach mediante un estudio teórico-práctico
- Analizar los controles de seguridad del sistema académico de la Utmach mediante una comparación inductiva-descriptiva para proponer controles de seguridad a implementar.

1.4 VENTAJA COMPETITIVA

La ventaja que representa la investigación pertinentes es contar con una documentación que linealice los procesos relativos a la seguridad del sistema académico en base al estado actual de la temática y sondeo de campo que delimitara las acciones a tomar como medidas en caso de ser necesario, también brinda la oportunidad de mejorar el grado de seguridad tomando como ejemplo otras universidades a nivel internacional que como institución han pasado por problemas similares en su desarrollo académico.

La Universidad Técnica de Machala presta servicios académicos como seguimiento a graduados, correo, biblioteca virtual, aula virtual, repositorio, consultorio jurídico entre otros, que se acceden a través de un login (correo institucional o cedula) y una contraseña, se estudia las vulnerabilidades latentes, controles de seguridad existentes y en qué medida interactúan para proponer controles adicionales de ser necesario.

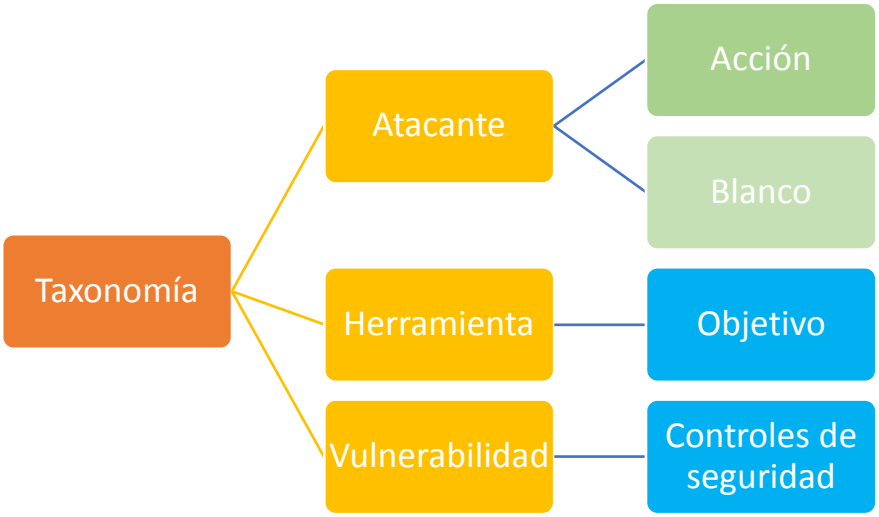
2. DESARROLLO:

El trabajo se puede subdividir en tres pasos, primero una revisión de las vulnerabilidades más comunes, controles aplicados en otras universidades, en segundo punto una inspección de las medidas implementadas en la Utmach en relación a los riesgos latentes en el sistema académico, como punto final un análisis inductivo donde se identifique que directrices pueden ser aplicadas para evitar y predecir amenazas futuras que no se han considerado en el diseño del entorno virtual que gestiona el sistema académico.

2.1 VULNERABILIDADES Y CONTROLES DE SEGURIDAD MÁS COMUNES

Se esquematiza los principales aspectos en la taxonomía de los ataques a redes informáticas de forma general, en la figura 1 se aprecia tales criterios.

Figura 1. Aspectos Principales de un ataque a un sistema digital

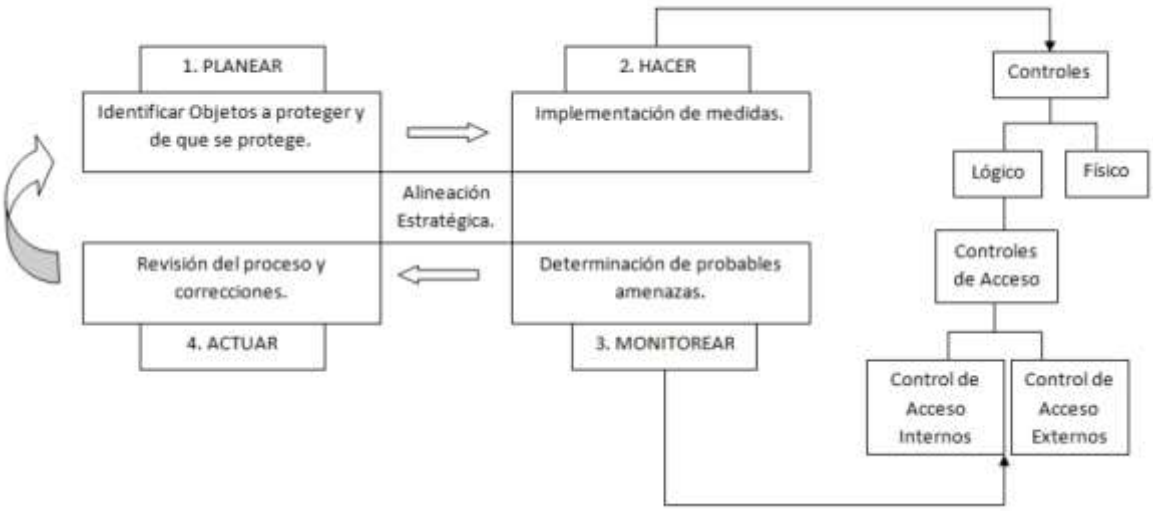


ELABORADO POR: El Autor

El atacante como ente acosador casi siempre es un código malicioso o un hacker movido por ambiciones personales o bien contratado por alguna causa ilícita, su vía suele ser intercambio de información a través de internet donde se busca sustraer contenidos, alteración de datos u otros como monitorear la entidad atacada; las vulnerabilidades esenciales son diseño del sitio web, configuración del servidor o errores en la implementación que no responden antes las intrusiones. El objetivo una vez se ingresa al sistema puede ser adquirir una ganancia política, económica e inclusive cambio de estatus a nivel institucional.

En base al diagramo apreciado en la figura 2 se deduce que la seguridad en un sistema virtual es un conjunto de procesos de carácter dinámico que debe evolucionar a la par de las innovaciones en el mundo digital para estar al tanto de las posibles afectaciones y no convertirse en un blanco fácil para los ciberdelincuentes.

Figura 2. Estructura básica de seguridad lógica



Fuente: (Martelo, Tovar, & Maza, 2018)

Los controles de seguridad que se han implementado tomando como referencia la Universidad de Cartagena y medidas a nivel macro se describen en el cuadro 1.

Cuadro 1. Controles de seguridad y sus accionantes en la seguridad informática.

Controles	Medida	Accionante
Lógico	Módulos de auditoria, registro y respuesta.	Comportamiento e interacción del conjunto de software frente a un ataque.
Físico	Hardware actualizado y dispositivos de seguridad informática.	Configuración de la red a nivel de infraestructura.
Acceso	Nivel de Privilegios.	Limita acciones de usuarios.
Servidor	Configuración unidireccional, protocolos de control	Restringe archivos y activaciones de programas
Encriptación	Resguardo de información, algoritmos de compresión de datos	Respaldo de datos en bancos virtuales bajo capas de codificación
Lenguaje de Influencias	Recursos administrativos y normativas	Gestión de plataforma y hardware

ELABORADO POR: El Autor

Uno de los inconvenientes más graves es identificar el fallo en la aplicación que permitió efectuar el ataque, el cual no es lo mismo ser analizado desde interior al exterior que desde un nivel estructural en su código base e inmiscuir en sus configuraciones preliminares cuya interacción faculta el funcionamiento del sistema.

La integración de módulos con un orden escalonado de usuarios, núcleo y auditorias permiten realizar un monitoreo constante de las políticas de seguridad implementadas a la vez que se motiva al compromiso del personal como parte del sistema de seguridad de la institución.

Esto evidencia que pese a nivel micro (Utmach) existen políticas de seguridad y control informático, a nivel meso (nacional) se carece de una normativa integradora que sea aplicable a servicios Cloud Computing que influyen en los procesos ejecutables de un sistema académico, siendo uno de los impedimentos de desarrollo informático en el país. (GONZÁLEZ SÁNCHEZ, 2016)

En base a lo expuesto se resalta la importancia de realizar un software de seguridad que maneje la identificación, control de acceso y encripte los datos de forma automática para mantener un nivel mínimo de confianza sobre los activos lógicos de la UTMACH, mismos criterios que debieron tenerse en cuenta en el diseño de la interfaz web tanto local como global. (Montecé, Verdesoto-Arguello, & Vargas-Marín, 2017)

2.2 CONTROLES DE SEGURIDAD IMPLEMENTADOS EN LA UTMACH EN BASE A SUS VULNERABILIDADES INFORMÁTICAS

La Universidad Técnica de Machala mantiene un conjunto de políticas que regulan la seguridad informática desde el punto de vista institucional, usuario y responsabilidades de la Dirección de la Tecnología de Información y Comunicación; entre los ítems relacionados a la investigación pertinente son:

- *Aplicaciones Informáticas:* La instalación de cualquier software en computadoras de uso académico es responsabilidad de la Dirección de TIC; el acceso a los sistemas se restringe dependiendo de los roles y perfiles de cada funcionario, cuando un empleado deja la UTMACH es responsabilidad de su superior inmediato retirar toda la información afín a la institución.
- *Control de Software Malicioso:* Es responsabilidad del usuario revisar que su ordenador no contenga softwares maliciosos que pueda afectar a la red UTMACH, no se permite instalar o desinstalar cualquier programa de seguridad impuesto por la dirección de TIC, en caso de notar un comportamiento extraño debe ser notificado al departamento encargado.
- *Acceso a internet:* Implementar herramientas y configuraciones para regular el recurso, siendo responsabilidad de cada usuario darle usos estrictamente académicos, prohíbe navegar por páginas pornográficas o sitios web de dudosa categoría que puedan provocar infecciones a la red de la UTMACH.

- *Correo Electrónico:* Es responsabilidad de cada usuario darle un uso correcto a dicho medio, se prohíbe ser usado como contacto en redes sociales enviar contenido multimedia, es competencia de cada funcionario darle fines corporativos al correo institucional.
- *Equipos Informáticos:* El uso de cada equipo debe ser gestado a través de la Dirección de TIC, solo se permite actividades institucionales en caso de ser dañado o reparado debe ser tratado por el personal competente de la UTMACH, cada funcionario es responsable de su ordenador de trabajo. La información debe protegerse mediante contraseña y solo usarse durante la jornada de trabajo.
- *Gestión de contraseña de usuarios:* El usuario no debe darles a terceros su contraseña ni guardarla en su table o celular, tampoco puede ingresarla a la vista de todos ni usar claves demasiado obvias, además el cambio de contraseña debe contener los caracteres mínimos y se cambiada periódicamente.
- *Copias de Respaldo:* Es responsabilidad de la dirección de TIC establecer los mecanismos, medios de almacenamiento del respaldo de información académica garantizando la seguridad de la misma.
- *Acuerdos de Confidencialidad:* Todas las personas que temporalmente realicen actividades en la institución deben aceptar y firmar un acuerdo de confidencialidad donde se estipulan los lineamientos a respetar en los recursos tecnológicos e informáticos que gestione la UTMACH. (UTMACH, 2015)

Cuadro 2. Servicios académicos y controles aplicados en la Utmach

Servicio Académico	**Control**
Seguimiento a graduados	Identificación, autentificación y autorización para usuarios
Repositorio digital	Restricción de acceso a programas y archivos
Unidad de Bienestar estudiantil	Restricción de programas y archivos que no correspondan
Centro de Educación Continua	Seguridad en uso de datos y procesos correctos
Fiel Web	Información recibida y destinada
Inscripción DNA	Barreras Firewall
Blogs	Configuraciones especiales
Consultorio Jurídico	Tunning en base de datos
Aula Virtual	Escaneo con antivirus
Biblioteca Universitaria	Aplicación de normas o políticas de control
Correo	

ELABORADO POR: El Autor

Las vulnerabilidades y amenazadas informáticas que enfrente el sistema académico se detalla mediante el cuadro 3, tomando como referencia un estudio efectuado por la ESPE a nivel meso que en contraste con la UTMACH da las siguientes connotaciones.

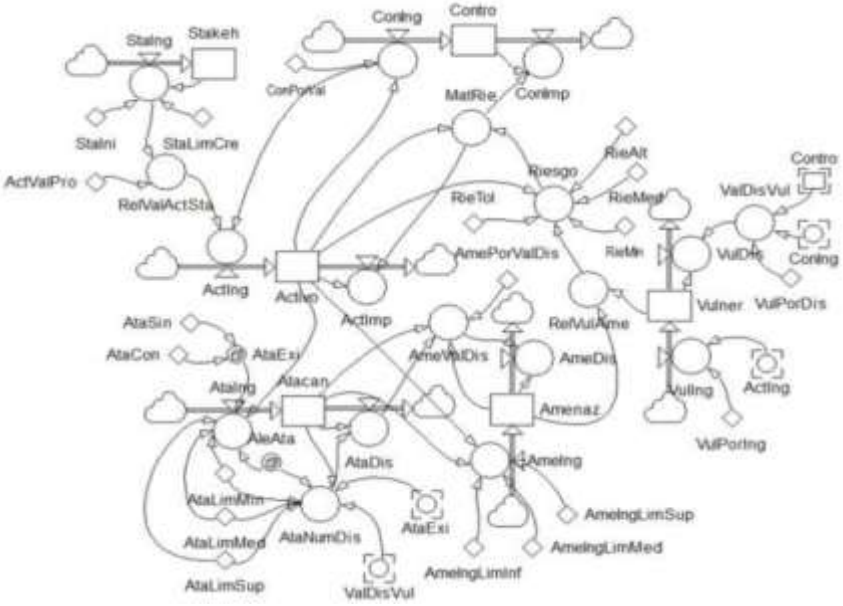
Cuadro 3. Matriz de doble entrada de vulnerabilidad-amenazas sistema informático

Vulnerabilidad-Amenaza	Información	Usuarios	Software	Externos
Diseño	Pérdida	Acceso	Fallos en ejecución y seguridad	Daño por agua o fuego
Configuraciones	Cruce	Autorizaciones		Errores de operación
Políticas Deficientes	No regular		Infraestructura deficiente	Errores de manejo
Desconocimiento y conducta de los usuarios	Mal uso	Acciones maliciosas		Robos o alteración
Errores en programación o puertas traseras	Fugas			Hackeos

ELABORADO POR: El Autor

Los parámetros de control conforman un flujo complejo, interrelacionado e interdependiente tanto de políticas legales, protocolos de programación, configuración de servidores, herramientas de control, conducta de usuarios, servicios online, plataformas Cloud e integrar un sin número de variables en sus distintos niveles, tal cual se observa en la figura 3.

Figura 3. Diagrama de flujo-Nivel de los componentes de seguridad



FUENTE: (Parada, Flórez, & Gómez, 2018)

2.3 ANÁLISIS DE CONTROLES DE SEGURIDAD EN FUNCIÓN DE POSIBLES AMENAZAS ADICIONALES

Una alternativa a considerar basada en una comparación meso podría ser la de implementar un servidor de telecomunicaciones que garantice la seguridad desde la red WI-FI a través de software libre que además de proveer medidas de seguridad más robustas que potencie las áreas informáticas en las universidades a la vez que disminuye el coste de mantenimiento de los sistemas académicos. (Valle, 2017)

Norma ISO 27001: Aporta las bases de por qué es importante la implantación de un Sistema de gestión de seguridad de la información, proporciona una introducción, pautas, controles, arquitectura, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua).

La UTMACH debe apuntar hacia la excelencia, por ende, es necesario conocer que estándares internacionales deben ser alcanzados para brindar una seguridad optima a sus sistemas académicos, a la par que se profundiza la investigación en el campo de la auditoria informática que ha pasado de ser un requisito pasivo a un activo en el desarrollo institucional.

Figura 4. Esquema de gestión de seguridad Informática

FUENTE: (Normas ISO, 2014)

- **Criptografía:** El cifrado como medida de seguridad permite enviar datos mediante un canal seguro, a la vez que se codifican en caracteres cifrados por medio de iteraciones matemáticas hasta secuenciar las combinaciones posibles en base a una clave o contraseña que ambas partes deben poseer, está alternativa es la de mejor facilidad

pero es susceptible a ataques de fuerza bruta con ordenadores de mayor potencia; por ello se la recomienda como medida complementaria. (Travieso, 2003)

- **Firewall-Linux:** Un firewall como mediador entre las redes externas e internas sesteado a través de protocolos Linux brinda un medio más robusto y regulable que protege de ataques desde un vía de acceso unilateral que controla como host las direcciones internas (privadas) en flujo de datos desde redes locales o globales, esto verifica la IP de solicitud mientras prioriza su autorización evitando conexión en caso de ser desconocido o sospechoso, además por ser software libre es menos susceptible a virus, permite una instauración extra de reglas capaces de ser adaptadas a casi cualquier sistema informático.
- **Red Fast-Flux:** Es una técnica relativamente nueva que asocia múltiples direcciones de IP a un dominio, cambiando de manera periódica y constante de la dirección del servidor a la vez que desvía el ataque a direcciones múltiples dificultando localizar la máquina a atacar, esto ayuda a ocultarse de los intentos de intrusión en el sistema, pero demanda una mayor potencia en los anchos de banda-equipos informáticos. (Zhou, 2015)
- **Programación Genética:** Esta técnica consiste en realizar análisis múltiples desde una gama de puntos de vista interesantes donde se identifique las mejores contramedidas para los casos más probables en base a las instancias clasificadas como patrón de aprendizaje del algoritmo que al final concibe un conjunto de propuestas y reglas donde se determina que causa afecta particularmente a un punto específico del sistema informático. Las entidades financieras y públicas son más susceptibles a virus o troyanos en comparación con empresas de comercio; por otro lado, se determina que empresas sin fines de lucro casi no sufren ataques informáticos. (Montealegre, 2015)
- **Recurso Humano:** Capacitar, concientizar y empoderar al personal es un punto clave en el cuidado de los sistemas informáticos, puesto que, aunque existan controles de seguridad automáticos no descarta la posibilidad de vandalismo interno o fallos derogados por funcionarios de baja calidad moral, que en la mayoría de casos llevan a vender información de su empresa con fines de lucro personales. (MSc. Mirta Julieta García García, 2013) También es necesario resalar que a nivel local se debe crear una cultura sobre seguridad informática que sirva como herramienta en la toma de decisiones de estrategias de seguridad de forma permanente en constante retroalimentación que permita aprender de los errores formando expertos en seguridad cuyo rasgo principal sea la responsabilidad consigo mismo y sus semejantes más que su dominio de la ingeniería de software. (Suárez & Fontalvo, 2013)

2.4 CIERRE

El desenlace del proyecto deriva en verificar cuales medidas de seguridad se implementan y analizar su respuesta entorno al sistema académico.

2.4.1 ARGUMENTACIÓN DE RESPUESTA

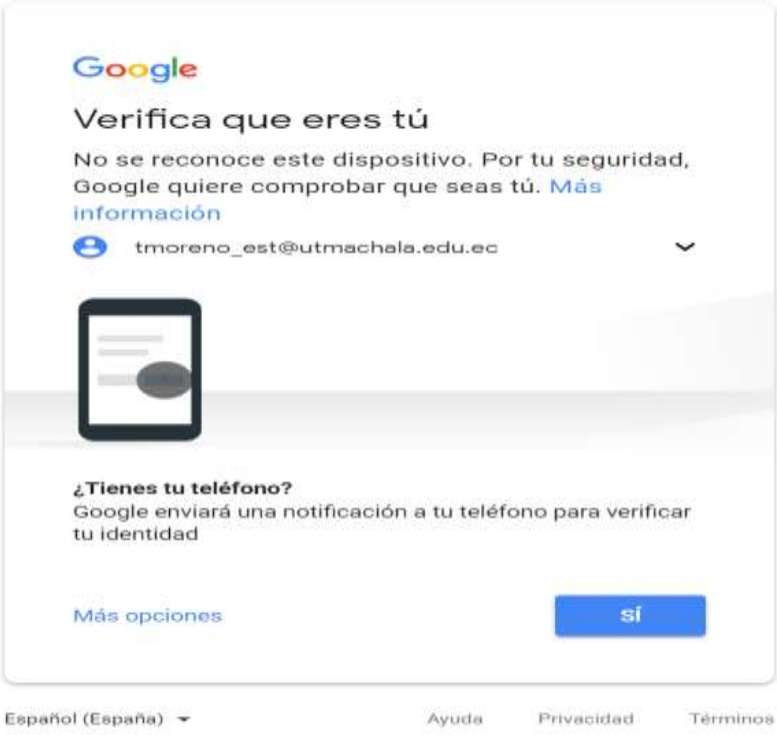
Evidenciamos a continuación:

2.4.2 EVIDENCIA DE HABER CUMPLIDO EL OBJETIVO

En la UTMACH se aplican controles de seguridad, tales como la autentificación de identidad por medio de contraseña, correo y configuraciones adicionales que ponen como medida ingresar un código que es enviado al celular del usuario en caso de abrir su correo desde una IP desconocida, dicho proceso se aprecia en la figura 5.

La interfaz de usuario al aula virtual y Siutmach requieren número de célula, contraseña un conjunto de caracteres combinando mayúsculas, minúsculas, signos (#$%&) y números para dar un nivel medio de seguridad, esto se observa en la figura 5.

Figura 5. Verificación de identidad al ingresar al correo institucional



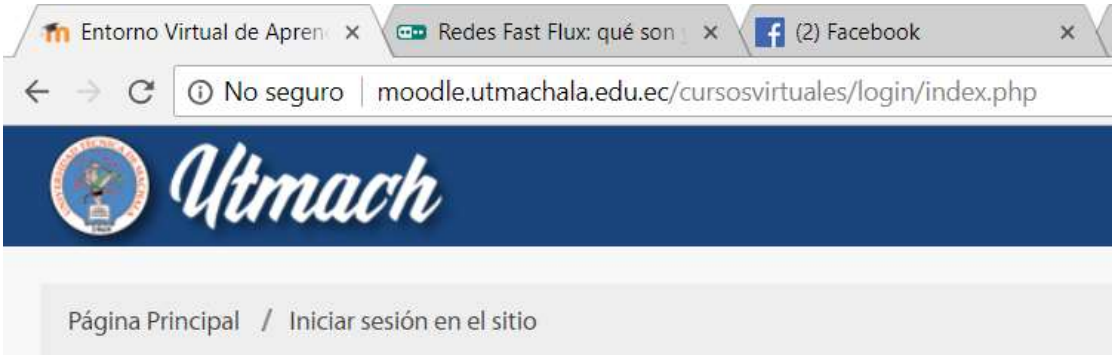
Fuente: (Google, 2018)

Figura 6. Interfaz de ingreso de usuario al sistema académico

Fuente: (UTMACH, 2018)

En el inciso 2.2 a 2.3 se analizan las medias implementadas y posibles alternativas para reforzar la seguridad del sistema académico, sin embargo, hay alarmas que se aprecian a simple vista como el dominio de la misma Web de la Universidad la cual no es segura por usar HTPPS, por lo cual Google recomienda no otorgar información confidencial en tal sitio. (ver figura 7).

Figura 7. Certificado de seguridad del sitio web



Fuente: (UTMACH, 2018)

3. CONCLUSIONES Y RECOMENDACIONES

A partir de los criterios expuestos en el presente texto se concluye y aconseja lo siguiente:

La UTMACH cuenta con políticas de seguridad, personal capacitado e individuos especialistas en seguridad informática pero no constata un compromiso general en tanto al resguardo de su sistema académico, se desconoce o no se identificado ataques anteriores ni acontecimientos importantes que motiven una implementación más sofisticada de controles de seguridad.

Los controles aplicados en el sistema académico dan un nivel medio de seguridad desde el punto de vista de la regulación de personal y vulnerabilidades, no obstante, a nivel macro está quedando retrasada en la implementación de controles con mayor eficiencia, cuya sutileza en modelos como servidor configurado en Linux, Firewall o encriptación también disminuiría los costos de operación y mantenimiento gracias a que se aliena a las políticas nacionales de actualización informática.

Se evidencia un desconocimiento acerca de las amenazas latentes en el medio local, mismas no han sido consideradas en el diseño de controles complejos, esto acompañado de la falta de normativas nacionales da deficiencia en el diseño del entorno web, por ende, se aconseja evaluar periódicamente los acontecimientos de inseguridad como base al plantear nuevas metodologías que conformen estrategias integradoras tanto de bondades lógicas, físicas y humanas en el sistema de seguridad académica.

Se recomienda linealizar el diseño de los servicios web basada en la normativa ISO 27001 para dotar de medidas verificadas a nivel internacional sobre la gestación de la seguridad e sistemas informáticos, que son la plataforma del sistema académico, además implementar una red fast flux reduciría en gran medida la cantidad de posibles ataques de forma innovadora sin representar un costos significativo a la Dirección de TIC.

REFERENCIAS BIBLIOGRAFÍCAS

Carvajal, C. J., Bayona, D. N., & Bayona, Z. O. (2013). Extensión de taxonomía y tratamiento de valores faltantes sobre un repositorio de incidentes de seguridad informática. *Ingeniería*, 24-49.

GONZÁLEZ SÁNCHEZ, J. L. (2016). *ANÁLISIS REGULATORIO Y COMERCIAL PARA EL DESARROLLO DE SERVICIO DE CLOUD COMPUTING PARA LA PROVINCIA DE EL ORO – ECUADOR.* Guayaquil: ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

Google. (2018). *Gmail*. Obtenido de https://accounts.google.com/signin/v2/sl/pwd?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&osid=1&service=mail&ss=1&ltmpl=default&rm=false&flowName=GlifWebSignIn&flowEntry=AddSession&cid=1&navigationDirection=forward

Imbaquingo, D., & Púsda, M. (2015). *Evaluación de amenazas y vulnerabilidades del módulo de gestión académica-Sistema informático integrado universitario de la Universidad Técncia del Norte Aplicando ISO 27000.* Sangolqui: Universidad de las Fuerzas Armadas (ESPE).

Martelo, R. J., Tovar, L. C., & Maza, D. A. (2018). Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. *Universidad de Cartagena, Facultad de Ingeniería, Grupo de Investigación en tecnología de las comunicaciones e informática*, 3-10.

Miranda, C. M., Puga, O. V., Mallea, I. P., Cobas, R. P., & Zequeira, R. S. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas*, 14-26.

MOLINA, K. J., MENESES, J. P., & SILGADO, I. Z. (2009). Firewall – Linux: Una Solución de Seguridad Informática para Pymes. *UIS Ingenierías,*, 155 - 165.

Montealegre, C. (2015). Extracción de reglas de clasificación sobre repositorio de incidentes de seguridad informática mediante programación genética. *Tecnura*, 109-119.

Montecé, F. W., Verdesoto-Arguello, A. E., & Vargas-Marín, H. J. (2017). Software de seguridad que permita la confidencialidad de los datos del sistema de gestión y servicios académicos para planteles de educación media (SiViSA). *Ciencias Informáticas*, 91-107.

MSc. Mirta Julieta García García. (2013). Utilización del razonamiento como apoyo en la toma de desiciones de seguridad informática. *Revista Técnica de la Empresa de Telecomunicaciones de Cuba S.A.*

Normas ISO. (2014). *ISO 27001.* Sevilla: ISO.

Parada, D. J., Flórez, A., & Gómez, U. E. (2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. *Análisis de los Componentes*, 27-38.

Suárez, D., & Fontalvo, A. Á. (2013). Una forma de interpretar la seguridad informática. *Engineering and Technology*.

Travieso, Y. M. (2003). La Criptografía como elemento de la seguridad informática. *Centro Provincial de Información de Ciencias Médicas.*

UTMACH. (2015). *POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE MACHALA.* MACHALA: Dirección de TIC.

UTMACH. (2018). *Página Principal*. Obtenido de http://moodle.utmachala.edu.ec/cursosvirtuales/login/index.php

Valle, C. S. (2017). *ESTUDIO DEL COMPORTAMIENTO DE UN SERVIDOR DE VoIP BASADO EN RASPBERRY PI Y SU INCIDENCIA EN LA COBERTURA PARA CLIENTES MÓVILES EN REDES WI-FI.* Guayaquil: Escuela Superior Politécnica del Litoral.

Zhou, S. (2015). A Survey on Fast-flux Attacks. *Information Security Journal: A Global Perspective*, 79-97.