UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EVALUAR LAS VULNERABILIDADES DEL REPOSITORIO DIGITAL DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH.

ARIAS CHAVEZ JUDITH AYLIN
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EVALUAR LAS VULNERABILIDADES DEL REPOSITORIO DIGITAL DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH.

ARIAS CHAVEZ JUDITH AYLIN
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

EVALUAR LAS VULNERABILIDADES DEL REPOSITORIO DIGITAL DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH.

ARIAS CHAVEZ JUDITH AYLIN
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 Evaluar las vulnerabilidades del repositorio digital de la Unidad Académica de Ciencias Empresariales de la UTMACH., hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

GONZALEZ SANCHEZ JORGE LUIS
0703333898
TUTOR - ESPECIALISTA 1

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
ESPECIALISTA 2

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 3

Fecha de impresión: viernes 01 de febrero de 2019 - 15:30

URKUND

Urkund Analysis Result

Analysed Document: ARIAS CHAVEZ JUDITH AYLIN_PT-011018.pdf (D47127979)
Submitted: 1/22/2019 9:32:00 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, ARIAS CHAVEZ JUDITH AYLIN, en calidad de autora del siguiente trabajo escrito titulado Evaluar las vulnerabilidades del repositorio digital de la Unidad Académica de Ciencias Empresariales de la UTMACH., otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 01 de febrero de 2019

ARIAS CHAVEZ JUDITH AYLIN
0750031841

RESUMEN

El presente caso de estudio, detalla el proceso para evaluar las vulnerabilidades/amenazas latentes en el repositorio digital de la Unidad Académica de Ciencias Empresariales (UACE), en la Universidad Técnica de Machala (UTMACH). Hoy en día, se vive en la sociedad del conocimiento, donde la información y flujo de datos integran un activo indispensable en toda organización, de forma especial en las instituciones académicas por ser las responsables de la producción científica, a la vez que preparar profesionales en las diversas áreas del saber. Por tal, motivo los repositorios son archivadores online cuya función es almacenar, preservar, difundir documentos derivados de las investigaciones institucionales; gracias a sus prestaciones se puede gestar la transferencia de conocimiento; no obstante, como todo medio informático implica vulnerabilidades o falencias tecnológicas que pueden poner en riesgos la calidad/fidelidad de los archivos, a la vez que dichas afectaciones involucran al desempeño organizacional, haciendo necesario un análisis a través de la auditoría informática para diagnosticar sus debilidades contraponiendo las medidas más eficientes en garantizar la seguridad del sistema; se aplica el método abductivo de índole exploratorio, basado en remedir criterios por medio de una revisión literaria.

Palabras Claves: Repositorio, vulnerabilidades, controles, auditoría informática.

ABSTRACT

The present case study, details the process to evaluate the vulnerabilities / latent threats in the digital repository of the Unidad Académica de Ciencias Empresariales (UACE), in the Universidad Técnica de Machala (UTMACH). Nowadays, people live in the knowledge society, where information and data flow make up an indispensable asset in any organization, especially in academic institutions for being responsible for scientific production, while preparing professionals in the different areas of knowledge. For this reason, repositories are online cabinets whose function is to store, preserve, disseminate documents derived from institutional investigations; thanks to its benefits, the transfer of knowledge can be gestated; However, as any computer means involves technological vulnerabilities or flaws that can put the quality / fidelity of the files at risk, while such affectations involve organizational performance, making necessary an analysis through the computer audit to diagnose their weaknesses counterposing the most efficient measures in guaranteeing the security of the system; the abductive method of an exploratory nature is applied, based on re-evaluating criteria by means of a literary revision.

Keywords: Repository, vulnerabilities, controls, computer audit.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

INTRODUCCIÓN

La era digital gestada en la sociedad del conocimiento, contrae avances vertiginosos y versátiles en todos los ámbitos, en especial en la *educación* cuyo papel principal es formar profesionales íntegros, que den propuestas para solventar las necesidades comunitarias de forma sostenible. Como función secundaria las universidades tienen la responsabilidad de producir conocimiento e innovar en la transferencia tecnológica que comprende a los procesos de enseñanza-aprendizaje; bajo este preámbulo los repositorios son *medio* necesario en las tareas de diseminar, compartir, almacenar, postular y tratar información, constituyendo un material digital eficiente que dinamiza el arte de investigar tanto para estudiantes como docentes, gracias a ellos los repositorios se han convertido en sinónimos de excelencia académica. (Cesteros, Romero, & Ranero, 2013)

En los últimos años se evidencia la relevancia de la infraestructura informática en las universidades, gracias a que, de su nivel de sofisticación y facilidades a las áreas administrativas, profesorado, cuerpo estudiantil, estadística, e integración de servicios que optimicen las funciones competentes de una institución de educación superior, se derivan el grado de usabilidad de bases de datos, bibliotecas virtuales o repositorios donde los trabajos de titulación sirven como fundamentación en la producción académico-científica, a través de indagaciones en materias de interés. (Mora, Santos, Chico, & Medina, 2017)

Hoy en día todas las organizaciones manejan información, ejercen sus facultades a través de, sistemas de información o plataformas tecnológicas/servicios Cloud Computing; esto sin duda converge en una ventaja competitiva a la vez que maximiza costos, pero también representa un riesgo mayor para las operaciones debido a las vulnerabilidades y amenazas afines a los sistemas digitales. Es el rol esencial de la auditoría informática emitir las respectivas medidas de control, prevención y corrección en la optimización de la seguridad institucional, así como velar por el acatamiento de las políticas/normativas o técnicas a favor de los planes estratégicos de la empresa. (Montealegre, 2015)

Los principales motivos de los atacantes en las bases de datos/sitios web son apropiarse de manera inescrupulosa de secretos corporativos, datos de entidades gubernamentales, sabotaje empresarial, ganancias económicas o simplemente probar su dominio sobre los sistemas electrónicos e informáticos, por ello es de vital relevancia en toda institución educativa implementar controles de seguridad, copias de respaldo, planes de acción para minimizar los riesgos/vulnerabilidades; dentro de las falencias más comunes son falta de expertos (auditores informáticos), poca o nula aplicación de normativas, no contar con servidores propios, sitios no seguros (inyección SQL), poco control a personal e inferencias por descuidos que viabilizan un ciberdelito. (Azán-Basallo, y otros, 2014)

En función de la revisión literal, se esquematiza en la *ilustración 1* los principales factores que inciden en los repositorios, debido a que son objeto de estudio de la auditoría informática.

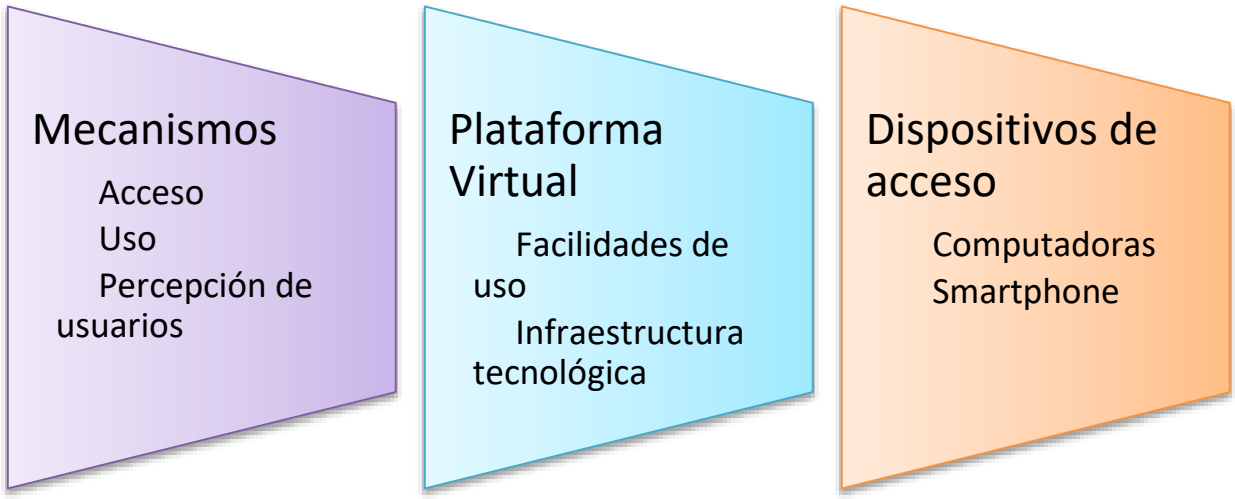

Ilustración 1 Esquematización de la estructura de un repositorio digital

Fuente: Elaboración Propia

El presente proyecto, tiene como objetivo evaluar las vulnerabilidades latentes en el repositorio digital de la Unidad Académica de Ciencias Empresariales, a través de un análisis abductivo para proponer los controles/medidas más eficientes en mejorar la seguridad del entorno virtual estudiado; también se busca determinar el nivel de seguridad que ostenta la UTMACH y en qué estado se encuentra en contraste con las tecnologías de vanguardia.

2. FUNDAMENTACIÓN TEÓRICA

En este apartado se describen las definiciones que conceptualizan el desarrollo del proyecto, los pretextos son interpretados desde el punto de vista del autor, siendo argumentados bajo una investigación documentada.

2.1 Repositorio Digital:

Son gestores de documentos a través de medios electrónicos, permiten la localización y búsqueda de la producción académica de las instituciones educativas; su principal ventaja es la capacidad de integrar el almacenamiento, accesibilidad, e investigación como recursos didácticos en los procesos de enseñanza, trascendiendo las barreras espacio/temporales, optimizando el uso de material bibliográfica en el sustento de entornos virtuales de aprendizaje. (Cesteros, Romero, & Ranero, 2013)

2.2 Auditoría de sistemas:

Es un conjunto de ciencias enfocadas a evaluar la seguridad en sistemas informáticos, analizar las vulnerabilidades, estado del entorno online, valoración de recursos intangibles, manejo de datos e inferir medidas de respuesta en favor de una mejora continua, a través de un informe de carácter dinámico. Su implementación es una necesidad para las instituciones académicas debido a la cantidad de contenidos que gestionan, y la inherente afinidad del internet como sustento en las plataformas/servicios organizacionales. (Tejena-Macías, 2018)

2.3 Seguridad de datos:

Es un concepto complejo, en la actualidad se lo considera como un derecho en la sociedad, garantizar la fidelidad, calidad, disponibilidad e integridad de datos, tanto personales como empresariales o contenido referente a bases de datos en instituciones de diversa razón social; su implementación es de carácter obligatorio, destacando que el papel del factor humano es esencial, de mayor relevancia que la parte lógica gracias a que el hombre programa y gestiona al sistema. (CARVAJAL, 2018)

2.4 Vulnerabilidades:

Son las debilidades o falencias internas en el sistema, son las vías por donde se ejecuta un ataque, dependen de las amenazas, es decir no existe la una sin la otra; el daño o afectaciones derivadas varían de acuerdo a la exposición al riesgo e intensidad del ataque, cuyas accionantes pueden mitigarse mediante controles físicos/lógicos. (Polanía, 2016)

En repositorios son errores en diseño, faltas de certificados de seguridad, mala gestión de datos o descuidos que vulneran los datos.

2.5 Amenazas:

Son agentes externos e internos que aprovechan vulnerabilidades para efectuar un ataque o impactar de forma negativa a los sistemas digitales; en general son factores de daño potenciales que no pueden ser evitables (KASPERSKY lab, 2018), pero si amortiguados por mecanismos de defensa, en la informática las amenazas más comunes y actuales son:

- Botnets
- Malware, virus informáticos
- Hackers
- Clientes internos/externos
- Espionaje, robo o fugas de datos
- Phishing, Ransomware
- Falta de plan de seguridad e informe de auditoría informática
- Desatención y desactualización de controles físicos/lógicos

2.6 Riesgos:

Es la probabilidad de sufrir un ataque y sufrir daños por afectaciones derivadas de la conjunción de una amenaza-debilidad; en los sistemas informáticos el mayor litigio es la carencia de un plan de auditoría informática, no se cuenta con una cultura en seguridad de sistemas que permite responder adecuadamente ante las amenazas; otra vulnerabilidad latente es la falta de capacitación en personal, poca implementación en controles e inversión casi nula en renovación de infraestructura computacional. (Tola, 2015)

2.7 Ataques a sistemas digitales:

Es un método a través del cual una amenaza logra ejecutar un daño en un sistema informático, tomando el control de las acciones de la red, hurtando e interceptando tráfico de datos, eliminación de archivos/ficheros, transacciones electrónicas, todo golpe cuya detonante sea la mala intención hacia la integridad de datos en una organización, según el proyecto abierto de seguridad en aplicaciones web (OWASP) (Hernández Saucedo & Mejia Miranda, 2015); los ataques principales actualmente son:

- Hombre en el medio
- Redirección de sitios web
- Inyección SQL
- Secuencia de Comandos en Sitios Cruzados
- Configuración de Seguridad Incorrecta:
- Exposición de datos sensibles:
- Falsificación de Petición en Sitios Cruzados (CSRF)
- Firmware Extensible Unificada (interfaz usuario)

2.8 Controles de seguridad:

Son las medidas, actividades, o actividades regulaciones que permiten salvaguardar la información, prevenir, detectar, evitar y responder a cualquier eventualidad que ponga en riesgo al sistema informático (Oficina de Sistemas y Recursos Informáticos OSIRIS, 2018), generalmente se dividen en:Físicos (personal, usuarios, clientes internos)

- Lógicos (seteado, softwares, protocolos, certificados, puertos)

- Roles y responsabilidades (políticas, normativas, leyes internas, leyes nacionales o penales seguridad informática)

Ilustración 2 Esquema de Seguridad de Sistemas

Fuente: (ISO 27000 ESPAÑOL, 2012)

3. MARCO METODOLÓGICO

Comprende los procesos cognitivos para obtener, procesar e interpretar la información citada en el desarrollo de la solución a la problemática expuesta, los procedimientos empleados son:

3.1 Investigación Bibliográfica:

Es la base teórica de todo proyecto, consiste en la búsqueda e indagación en textos, archivos u otro material documentado sobre estudios referentes a la temática; en este caso se citan tesis, trabajos de titulación, artículos de revistas indexadas, archivos de repositorios y cualquier fuente literaria que permita fundamentar los criterios versados en este escrito.

3.2 Método Abductivo:

Es un proceso derivado del razonamiento lógico, que parte de la deducción, análisis e inducción, comprende la facultad de sumar criterios partiendo de un eje común (eje sistemático) e inferir resultados para mediante relacionales objetivas comprender el fenómeno u objeto de estudio. (Martín, 2015)

3.3 Análisis de Contenido:

Es un paradigma en las investigaciones, debido a que es altamente adaptable, su estructura es triangular en tres fases: revisión teórica, descriptiva e interpretación; se enfoca en comparar variables en función de características para establecer una causa-efecto del fenómeno en cuestión. (Herrera, 2018)

4. MARCO CONTEXTUAL

En el nivel internacional los repositorios digitales permiten globalizar la información, formalizar la investigación institucional, a la vez que permiten migrar de las bibliotecas convencionales a una educación virtual, pese a ello su usabilidad depende de la percepción de los estudiantes, interfaces, facilidades de manejo, actualidad de archivos y seguridad que es derogada de las prestaciones tecnológicas que sustentan a la plataforma. (Mora, Santos, Chico, & Medina, Factores que incentivan el uso de la biblioteca virtual en los estudiantes universitarios: un estudio de caso de la Universidad de Gómez Palacio de Durango, 2017)

En lo referente a Latinoamérica, los repositorios son herramientas imperiosas en la transformación de la educación y transferencia de conocimiento a la población en general, además inciden directamente en el prestigio de la Institución de Educación Superior, a la vez que denotan el grado de compromiso con la producción científica y miden el aporte en las diversas áreas de la ciencia.

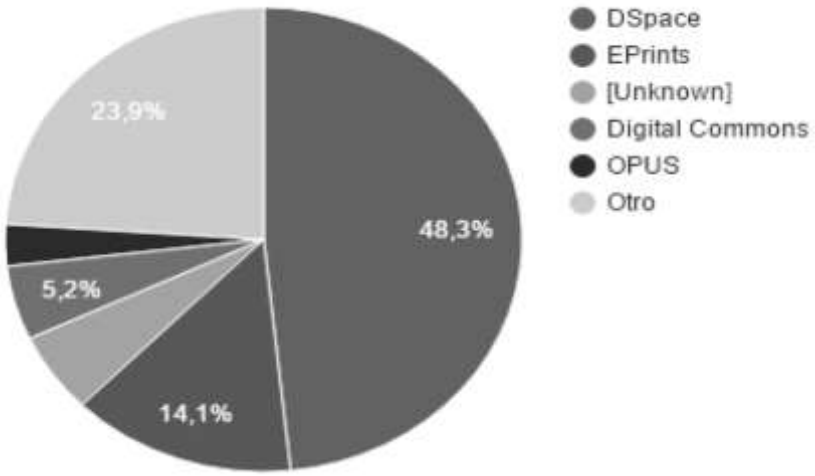

Ilustración 3 Software más usados en repositorios digitales

Fuente: (Alvarado, 2017)

En el Ecuador, se realiza la implementación de la *Red de Repositorios de Aceso Abierto del Ecuador-RRAAE,* cumple normativas nacionales e integra estándares internacionales con el fin de facilitar la gestión de información a todo público, su meta es impulsar la producción del conocimiento académico. (Red nacional de investigación y educación del Ecuador, 2018).

La Universidad Técnica de Machala, cuenta con un repositorio con meta datos y sistema de búsqueda por carreras en función de las unidades académicas, su plataforma es DSpace; además forma parte de la red *Repositorios Digitales y Bibliotecas del Ecuador*, lo cual indica que en los últimos años las bibliotecas universitarias contribuyen al desarrollo intelectual de toda la población, gracias a su aporte científico a nivel local, regional e incluso nacional.

Ilustración 4 Consorcio de bibliotecas Universitarias del Ecuador
Fuente: (Repositorios digitales y bibliotecas del Ecuador, 2017)

4.1 DESARROLLO:

Esta sección se describen las vulnerabilidades presentes en el repositorio digital, desde su plataforma DSpace hasta sus debilidades como entorno web, luego se analizan las técnicas de vanguardia que pueden aplicarse, para responder eficientemente ante dichas eventualidades.

Las vulnerabilidades, se catalogan en función del riesgo que representan al sistema en orden descendente:

4.1.1 Nivel Crítico:

Es aquel que puede impactar a toda la infraestructura ocasionando un daño irreversible, cuyas afectaciones imposibilitan totalmente al sitio.

Inyección SQL: Se caracteriza por error en validación de datos, infiltrando código en la programación del sitio web que altera su funcionamiento y permite efectuar un ataque contundente que da control total al infractor.

4.1.2 Nivel Alto:

Contraseña transmitida a través de HTTP: Determina los datos transferidos a través del HTTP, un hacker puede acceder al repositorio para capturar el login/clave de un usuario.

Cross-site scripting (XSS): Es un método que permite ejecutar un programa dinámico en la aplicación, su meta es secuestrar la sesión de los usuarios o adquirir privilegios de administrador para modificar el código HTML.

SVN Detected: Detectar archivos de origen: comma separated values (CVS), Software de control de versiones (GIT), software de revisión (SVN), para tener acceso al código fuente de la página.

Hombre en el medio: Es la intercepción de tráfico de datos para descifrarlos, se asemeja a un hombre pasa el balón entre dos destinatarios y un tercero lo intercepta, su analogía hace referencia a las cookies que no son seguros en la navegación de un sitio web.

4.1.3 Nivel Regular:

Inyección HTTP: Cuando no se tiene servidor propio, en la cabecera falta el certificado HTTP que permite secuestro de sesión y problemas como scripting/cross-site.

Transporte inseguro protocolo (SSLv2): Cuando el servidor web permite flujo de paquetes de datos en una comunicación segura, soportado por un protocolo inseguro, el cual es el medio para desencriptar la información.

Weak Ciphers Enabled: Detecta que el servidor permite usar cifrado débil en comunicación seguro, esto la vulnera frente ataques de fuerza bruta que pueden adivinar de forma iterativa las contraseñas.

Certificado inválido SSL: verifica que el servidor usa un certificado no validado, lo cual permite que un ente externo observe la comunicación entre sitio y el usuario. (Belarmino & Araújo, 2014)

4.1.4 Nivel Bajo:

Auto Complete Enabled: la función Autocompletar se ha activado en uno o más campos de formulario sensibles, como contraseñas. Los datos introducidos en estos campos se almacenar en caché por el explorador. Un atacante que puede acceder a la computadora de la víctima podría robar esta información. Esto es especialmente importante si la aplicación se utiliza comúnmente en ordenadores públicos.

Social Security Number Disclosure - identifica Números de Seguridad Social (SSN) en el sitio. Los números de seguridad social han sido utilizados por atacantes en el robo de identidad ya que muchas organizaciones incluyendo empresas, agencias gubernamentales, hospitales e instituciones de enseñanza utilizan el SSN como el identificador primario para sus sistemas de mantenimiento de registros. (Belarmino & Araújo, 2014)

4.1.5 Contraseña con cifrado:

Este método emplea el encriptado asimétrico, para diseñar una firma digital con algoritmos que generan dos claves complementarias, la una es pública disponible para los administradores y la otra es únicamente portada por el usuario propietario. Este sistema permite regular y restringir el acceso de personas no autorizadas al repositorio protegiendo las cuentas e incrementando el nivel de seguridad general de todo el entorno virtual.

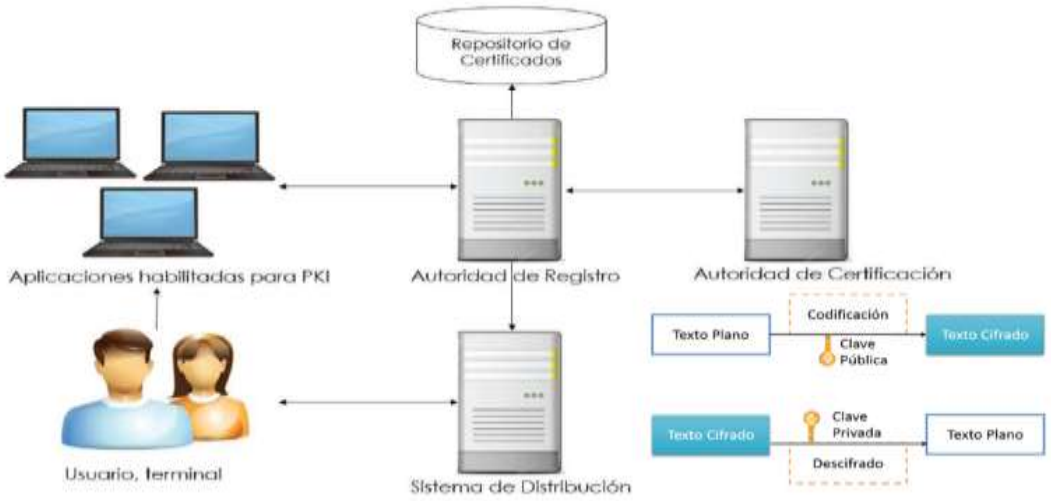

Ilustración 5 Arquitectura de autorización mediante clave de cifrado

Fuente: (García1, 2018)

4.1.6 Sistema de Prevención de Intrusos:

Una medida es evitar a través de un escaneo la oportunidad de ataques, la infraestructura del *Snort v2.9* solventada en Linux Ubuntu es un entorno virtual que monitorea el tráfico de la red en tiempo real, permite gestionar la conexión entre servidores y entre las redes en paquetería de datos, emplea DAQ 2.0.6 para capturar firmas de usuarios registrado y negar acceso a agentes no validados. (MEDINA, 2017)

4.1.7 Sistemas de control en respuesta a riesgos

Los principales riesgos derivados de las posibles vulnerabilidades tanto físicas como lógicas, se resumen en el *cuadro 1.*

RIESGOS	CONTROL
Amenazas web	Monitoreo continuo, configuraciones aseguras, mecanismos de defensa y prevención
Pérdida de información/datos	Copias de seguridad regulares
Robo de archivos	Encriptación en bases de datos, restringir acceso a terceros, contraseñas robustas
Usuarios	Políticas, normativas, capacitaciones periódicas, aplicar prácticas y cultura de seguridad
Ataques de malware	Certificados de seguridad, firewall, antivirus
Robo de identidades	Configuración de puertos, seguridades en acceso y gestión de privilegios en usuarios
Suplantación de dominio, Dirección IP, botnets	Configuración SSL, sistema de fast flux, gestión dinámica de dominios
Adecuación/mantenimiento	Solicitar auditoria permanente de cada área, actualizar y renovar infraestructura informática acorde a las exigencias del sistema

Cuadro 1 Controles en respuesta a riesgos en repositorios

Fuente: Elaboración propia

Se debe considerar que el repositorio es un sistema online, por lo cual evidentemente acarrea debilidades propias de la infraestructura lógica, en contraste con el manejo de los usuarios o personas responsables de la seguridad en la institución académica.

CONCLUSIÓN

Los repositorios digitales permiten optimizar las funcionalidades academias, en virtud de ser fuente fidedigna de documentación en argumentar proyectos, a su vez potencia las bondades en el proceso de aprendizaje facilitando información tanto al campus como a la ciudadanía en general, siendo clave en la actualización de conocimientos en la sociedad.

Todo sistema virtual gestado online, ostenta vulnerabilidades que avanzan a la par de sus prestaciones, por lo tanto, no basta con implementar controles de vanguardia, sino desarrollar cultura en seguridad informática para mantener la renovación de medias permanentemente, además estar al tanto de nuevas técnicas para mejorar la seguridad en infraestructura informática.

Las debilidades son productos de falencias en el servidor e incidencias en la conducta de los usuarios, que por faltas de políticas estandarizadas carecen de sustento o base legal para ser aplicadas, un control eficiente es educar al personal externo e interno, enseñar que la importancia de cuidar el activo informática, haciendo hincapié en el empoderamiento institucional como eje en la mejora sistemática de las prestaciones académicas/administrativas de la UTMACH.

Se evidencia que las amenazas no pueden evitarse, pero se pueden estar alerta a través de la auditoría informática que expresa las medidas óptimas para responder frente a posibles ataques, además por ser un repositorio la mejor alternativa sería copias de seguridad alojadas en servidores virtuales, que ahorran en infraestructura y facilitan el crecimiento de la base de datos.

Se aconseja realizar estudios afines para evaluar los mecanismos, servicios, arquitectura computacional, softwares e implementos tecnológicos que pueden el rendimiento de los entornos virtuales en relación al beneficio-costo.

BIBLIOGRAFÍA

Alvarado, S. D. (2017). Repositorios institucionales digitales: Análisis comparativo entre SEDICI (Argentina) y Kérwá (Costa Rica). *e-Ciencias de la Información*, 2-31.

Azán-Basallo, Y., Bravo-García, L., Rosales-Romero, W., Trujillo-Márquez, D., García-Romero, E. A., & Pimentel-Rivero, A. (2014). Solución basada en el Razonamiento Basado en Casos para el apoyo a las auditorías informáticas a bases de datos. *Revista Cubana de Ciencias Informáticas, 8*(2), 52-68.

Belarmino, V. F., & Araújo, W. j. (2014). Análise de vulnerabilidades computacionais em repositórios digitais. *Biblios*, 2-17.

CARVAJAL, E. T. (2018). TECNOLOGÍAS, SEGURIDAD INFORMÁTICA Y DERECHOS HUMANOS. *IUS ET SCIENTIA* , 19-39.

Cesteros, A. M., Romero, E. D., & Ranero, e. I. (2013). Análisis de la evolución de los Repositorios Institucionales de material educativo digital de las universidades españolas. *Revista Latinoamericana de Tecnología Educativa, 12*(2), 11-25.

Cesteros, A. M.P., Romero, E. D., & Ranero, I. d. (2013). Análisis de la evolución de los Repositorios Institucionales de material educativo digital de las universidades españolas. *Revista Latinoamericana de Tecnología Educativa, 12*(2), 11-25.

García1, F. Y. (2018). Análisis de la firma digital con base en la infraestructura de clave pública. *Revista semestral de divulgación científica*, 94-104.

Hernández Saucedo, A. L., & Mejía Miranda, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *ReCIBE. Revista electrónica de Computación, Informática Biomédica y Electrónica,*, 3-18.

Herrera, C. D. (2018). Investigación cualitativa y análisis de contenido temático. Orientación intelectual de revista Universum. *Revista General de Información y Documentación*, 119-142.

ISO 27000 ESPAÑOL. (2012). *El portal de ISO 27001 en Español*. Obtenido de Ciber seguridad: http://www.iso27000.es/

KASPERSKY lab. (2018). *KASPERSKY LAB PREDICCIONES SOBRE AMENAZAS PARA EL 2018.* Moscú: Boletín de seguridad.

Martín, M. d. (2015). Abducción, método científico e historia. *Páginas*, 125-141.

MEDINA, R. L. (2017). *SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS IPS PARA LA VLAN DE SERVIDORES DE LA SOCIEDAD MINERA DE SANTANDER S.A.S. EN BUCARAMANGA (SANTANDER).* BUCARAMANGA: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.

Montealegre, C. J. (2015). Extracción de reglas de clasificación sobre repositorio de incidentes de seguridad informática mediante programación genética. *Tecnura, 19*(44), 109-119.

Mora, O. Y., Santos, S. A., Chico, M. C., & Medina, E. C. (2017). Factores que incentivan el uso de la biblioteca virtual en los estudiantes universitarios: un estudio de caso de la Universidad de Gómez Palacio de Durango. *Biblios, 66*, 98-111.

Mora, O. Y., Santos, S. A., Chico, M. C., & Medina, E. C. (2017). Factores que incentivan el uso de la biblioteca virtual en los estudiantes universitarios: un estudio de caso de la Universidad de Gómez Palacio de Durango. *Biblios*, 90-111.

Oficina de Sistemas y Recursos Informáticos OSIRIS. (2018). *MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.* Bogotá: ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO.

Polanía, G. A. (2016). Metodología para el análisis de vulnerabilidades. *Tecnología, Investigación y Academia*, 20-27.

Red nacional de investigación y educación del Ecuador. (2018). *GRUPO DE TRABAJO: DE REPOSITORIOS.* Cuenca: CEDIA.

Repositorios digitales y bibliotecas del Ecuador. (2017). *Consorcio de bibliotecas universitarios del Ecuador*. Obtenido de http://www.bibliotecasdelecuador.com/cobuec/

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo del conocimiento*, 230-244.

Tola, A. M. (2015). *ANÁLISIS DE RIESGOS APLICANDO LA METODOLOGÍA OWASP.* Obtenido de DOCPLAYER: https://docplayer.es/39436742-Analisis-de-riesgos-aplicando-la-metodologia-owasp.html