UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE CÓMPUTO DE LA BIBLIOTECA DE LA UAIC DE LA UTMACH

AYALA JARAMILLO JANINE ELIZABETH
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE CÓMPUTO DE LA BIBLIOTECA DE LA UAIC DE LA UTMACH

AYALA JARAMILLO JANINE ELIZABETH
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE CÓMPUTO DE LA BIBLIOTECA DE LA UAIC DE LA UTMACH

AYALA JARAMILLO JANINE ELIZABETH
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 26 DE AGOSTO DE 2019

MACHALA
26 de agosto de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE CÓMPUTO DE LA BIBLIOTECA DE LA UAIC 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

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

ILLESCAS ESPINOZA WILMER HENRY
0704128776
ESPECIALISTA 3

Fecha de impresión: jueves 22 de agosto de 2019 - 14:47

URKUND

Urkund Analysis Result

Analysed Document:	Jannie Ayala.docx (D54790891)
Submitted:	8/13/2019 1:32:00 AM
Submitted By:	jgonzalez@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, AYALA JARAMILLO JANINE ELIZABETH, en calidad de autora del siguiente trabajo escrito titulado EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE CÓMPUTO DE LA BIBLIOTECA DE LA UAIC 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.

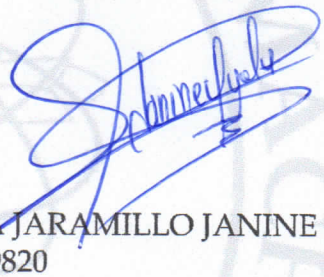
La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

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, 26 de agosto de 2019



AYALA JARAMILLO JANINE ELIZABETH
0704739820

DEDICATORIA

A DIOS, Por otorgarme vida, salud y sabiduría a lo largo de todo el tiempo que he emprendido mi estudio y formación profesional.

A MIS HIJAS ARIANA C. AYALA – EMILY C. AYALA, Que sin ellas no hubiese logrado una meta más en mi vida profesional, porque ellas fueron mi motivación y mi lucha constante día a día, por sacrificar el tiempo con ellas para poder concluir con éxito este proyecto.

A MIS PADRES, FAMILIA y a todas las personas que de una u otra manera me brindaron siempre todo su apoyo en mi labor diaria en el desarrollo de la presente tesis de grado.

JANINE ELIZABETH AYALA JARAMILLO

RESUMEN

La documentación presente tiene la pertenencia de abordar la temática de la auditoria informática, como eje profesional de la carrera de contabilidad y auditoría, siendo una ciencia interdisciplinaria que cimenta al desarrollo empresarial e institucional mediante las bondades de los sistemas informáticos. Los centros de cómputo son una herramienta didáctica en el proceso formativo contemporáneo, sin embargo, exponen una serie de vulnerabilidades y riesgos derivados tanto de su parte lógica como físicos por los usuarios, esto dificulta el desempeño académico e infiere en la utilidad de los servicios gestados en TIC`s. Existe una necesidad imperiosa de aprovechar u optimizar las funciones academias mediante los sistemas digitales; pero no se opera adecuadamente entorno a las condiciones adversas desde la perspectiva de la seguridad, por ende, este proyecto tiene como objetivo evaluar el riesgo informático en los ordenadores de la biblioteca de la Unidad Académica de Ingeniería civil a través de un análisis sistemático, para proponer controles tangibles e intangibles que minimicen las amenazas e incrementen la protección, tanto de los datos como de los recursos computaciones en general. La valoración del riesgo depende de la metodología utilizada en medir su impacto, en este caso se utiliza Cobit 5, competentes a la auditoria informática y valoración cualitativa, denotando un nivel de riesgo Medio frente a un control Bueno que responde superficialmente iterando los aspectos clave delineados por la dirección de TIC`s, no se cuenta con un auditor externo ni un plan de manejo macro, siendo una debilidad latente en todo la UTMACH.

Palabras Clave: Auditoria informática, riesgos, centro de cómputo, controles.

ABSTRACT

The present documentation has the belonging to address the subject of computer auditing, as a professional axis of the accounting and auditing career, being an interdisciplinary science that underpins business and institutional development through the benefits of computer systems. The computer centers are a didactic tool in the contemporary training process, however, they expose a series of vulnerabilities and risks derived from both their logical and physical part by the users, this hinders academic performance and infers on the usefulness of the services gestated in TIC`s. There is an urgent need to take advantage of or optimize academy functions through digital systems; but it does not operate properly around adverse conditions from the perspective of security, therefore, this project aims to assess the computer risk in the computers of the library of the Civil Engineering Academic Unit through a systematic analysis, to propose tangible and intangible controls that minimize threats and increase the protection of both data and computing resources in general. The risk assessment depends on the methodology used to measure its impact, in this case Cobit 5 is used, competent to the computer audit and qualitative assessment, denoting a level of risk Medium versus a control Good that responds superficially iterating the key aspects outlined by the TIC`s management, there is no external auditor or a macro management plan, being a latent weakness throughout the UTMACH.

Keywords: Computer audit, risks, computer center, controls.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

INTRODUCCIÓN

En la actualidad el contexto social es solventado por medios computacionales, sistemas digitales y servidores virtuales que hacen posible la gestión multimedia a nivel macro como Google, Facebook, YouTube, páginas web interactivas, aulas virtuales, modelaciones de proceso a través de activos informáticos con la finalidad de optimizar e impulsar desarrollo de las esferas culturales, mejorando su desempeño; de esto se destaca a la educación como pilar de las ciencias, cuya misión es formar profesionales capaces de resolver las problemáticas en las comunidades, dicha tarea se encomienda a las universidades que debido a la globalización integra a las TIC`s junto a las actividades académicas.

Las virtuales que ofrecen las tecnologías online y medios electrónicos a la ejecución de investigaciones, evaluaciones u operaciones de docentes, se concatenan con la facilidad al impartir conocimientos en forma paralela a las destrezas competentes a la asignatura, también fomentan el modelo desarrollador-integrador pertinente a la UTMACH, mediante las herramientas didácticas en la construcción del conocimiento e incentivando al estudiante a satisfacer sus propias necesidades didácticas.

Las bibliotecas son fuentes de saberes e investigaciones permitiendo efectuar revisiones cognitivas sobre las temáticas estudiadas, en los ordenadores usados por los estudiantes (centro de cómputo) tienen acceso a internet, puntualmente a las bases de datos indexadas, repositorios y biblioteca online para consolidar criterios teóricos; sin embargo, presentan ciertas vulnerabilidades como virus, deterioro del hardware, hackers, daño de archivos o corrupción de datos a través de ataques online, además de daño físico o uso indebido por los alumnos; esto hace necesario tomar medidas para corregir, evitar y prevenir afectaciones a los activos informáticos.

El presente estudio tiene como objetivo principal de evaluar el riesgo informático del centro de cómputo de la biblioteca de la UAIC de la UTMACH, por medio de un análisis sistemática y desde una perspectiva explicativa de carácter holístico, para proponer controles físicos/lógicos que mejoren la seguridad en protección de datos u otros implementos en sistemas digitales.

1.1 FUNDAMENTACION TEORICA

Se exponen los conceptos y terminologías para explicar el encuadre epistemológico del proyecto, indagando en la auditoria informática para encontrar alternativas que permiten solucionar la problemática.

1.1 Auditoria Informática

Es un conjunto de ciencias de carácter interdisciplinario, enfocadas en el uso adecuado de los sistemas computacionales; su principal atributo es evaluar y retroalimentar la eficiencia en las instituciones u organizaciones gestando controles de personal, flujos de caja, políticas de seguridad, protección de datos e integrar en forma sistemática las bondades de las TIC`s paralelamente a la cadena de valor de las entidades corporativas sin importar su naturaleza (publica/privada) o función social (Arcentales-Fernández & Caycedo-Casas, 2017).

Ilustración 1. Esquematización piramidal de la auditoria Informática
Fuente: Elaboración a partir de *(Montaño Fernández, 2016)*

1.2 Seguridad y protección de activos informáticos

Son prácticas, operaciones e inferencias consignadas a salvaguardar los activos digitales, con la meta de conservar los daños a un nivel aceptable e acrecentar los controles para reducir las vulnerabilidades a un costo rentable, en el caso de los centros de cómputo universitarios la razón es de *cultura*, es decir la incompetencia o descuido es el mayor peligro, puesto que por sus propios actos posibilitan ataques, perdidas, daños u otras nulidades en los ordenadores, por lo cual concientizar al recurso humano

es una medida imperiosa en auditoria de sistemas (Roquez Hernandez & Juarez Ibarra, 2018).

1.2.1 Protección de datos

Es un modelo tanto social como tecnológico, puesto que se refiere al sometimiento por información personal, jurídica o institucional; dar un buen uso a las suposiciones tratadas en los buscadores, ordenadores profesionales e incluso bases de datos como las redes sociales, liberando gran debate en torno al derecho al olvido digital demandando una renuncia a la híper accesibilidad que ofrece el internet hacia los usuarios (Minero Alejandre, 2017).

1.2.2 Protección del sistema

Es mantener al mínimo los riesgos del sistema, asegurar la continuidad en las operaciones y acciones solventadas en medios informáticos; así como garantizar la integridad de equipos e implementos de hardware/software frente a cualquier anomalía externo o interna a la organización (Quiroz-Zambrano, 2017).

1.3 Vulnerabilidades en sistemas computaciones

Son todas las debilidades que posibilitan un ataque e ingreso de una amanezca al sistema; en instituciones públicas comúnmente es la falta de fondos para mejorar y potenciar la infraestructura, en centros de cómputo universitarios son los estudiantes quienes por falta de mecanismos de control comprometen la seguridad del entorno (Gil Vera & Gil Vera, 2017).

1.3.1 Físicas:

Son las ocasionadas por el personal, generalmente es el parámetro más difícil de controlar, debido a que la conducta humana no ofrece patrones computables, sino obedece a su perfil psicológico, en este grupo se catalogan a las políticas, sanciones, dispositivos biométricos para frenar las acciones peligrosas al sistema.

1.3.2 Lógicas:

Son las falencias en configuraciones, errores de conexión, intercepciones o anomalías realizadas a través de internet, así como virus informáticos capaces de averiar la parte intangible del sistema.

El deterioro del sistema, debido al paso del tiempo es una debilidad en firmware gracias a que mitiga las funciones del ordenador e incide negativamente en los procesos lógicos, por ello el mantenimiento continuo es una medida clave en centros de cómputo.

1.4 Amenazas en TIC`s

Son los agentes que enuncian un peligro latente, pero no es realizable sin una vulnerabilidad que explotar; se relaciona con las potencialices virtuales aprovechando las redes o activos electrónicos para robar información, sustraer datos y editar caracteres sin la autorización respectiva. (Hernández Saucedo & Mejia Miranda, 2015)

- Inyección SQL, OS, LDAP
- Secuencia de comandos en sitios cruzados
- Configuración de seguridad incorrecta
- Exposición de datos confidenciales
- Falsificación de peticiones al servidor
- Hackers
- Virus, códigos maliciosos
- Deterioro o robo de hardware
- Perdida, hurto o uso indebido de datos (Hernández Saucedo & Mejia Miranda, 2015).

AMENAZAS	MECANISMOS DE DEFENSA
ROBOS	• Cifrar la información almacenada en los soportes para que en caso de robo no sea legible. • Utilizar contraseñas para evitar el acceso a lo información. • Sistemas biométricos (uso de huella dactilar, tarjetas identificadoras, caligrafío).
PÉRDIDA DE INFORMACIÓN	• Realizar copias de seguridad para poder restaurar la información perdida. • Uso de sistemas tolerantes a fallos, elección del sistema de ficheros del sistema operativo adecuado. • Uso de conjunto de discos redundantes, protege contra la pérdida de datos y proporciona la recuperación de los datos en tiempo real.
PÉRDIDA DE INTEGRIDAD EN LA INFORMACIÓN	• Uso de programas de chequeo del equipo, SiSoft Sandra 2000, TuneUp, etc. • Mediante la firma digital en el envío de información a través de mensajes enviados por la red. • Uso de la instrucción del sistema operativo Windows, sfc (system file checker).
ENTRADA DE VIRUS	Uso de antivirus, que evite que se infecten los equipos con programas malintencionados.
ATAQUES DESDE LA RED	• Firewall, autorizando y auditando las conexiones permitidas. • Programas de monitorización • Servidores Proxys, autorizando y auditando las conexiones permitidas.
MODIFICACIONES NO AUTORIZADAS	• Uso de contraseñas que no permitan el acceso a la información. • Uso de listas de control de acceso. • Cifrar documentos.

Ilustración 2. Amenazas y mecanismos de defensa en seguridad Lógica
Fuente: (Vega Villacís & Ramos Morocho, 2017)**.**

1.5 Riesgo Informático

Son la contra parte dual de las bondades cloud computing e inferencias nocivas relativos a sistemas computacionales; exclusivamente en bibliotecas son las probabilidades de efectuarse daños a los datos, redes, equipos, archivos e instalaciones, exigiendo una gestión solventada en políticas, prácticas y responsabilidades de todos los implicados (Corda, Viñas, & Coria, 2017); los riesgos principales en centros de cómputo universitarios son:

- Infraestructura
- Organización y coordinación
- Relación
- Integridad de datos
- De acceso

1.6 Controles de seguridad

Comprenden las medidas administrativas, disciplinarias e infraestructura tecnológica efectuadas para custodiar a niveles aceptables los riesgos, también permiten una operatividad estable de los atributos digitales, brindan una Gestión estratégica al regularizar la seguridad y forman un plan institucional consignado a proteger los sistemas informáticos, a través de una medida horizontal tanto al personal como activos lógicos (antivirus, políticas de seguridad, redes, servidores, sistema operativo, entre otros) (Martelo , Tobar , & Maza , 2018).

2. METODOLOGÍA

Comprende la descripción de las técnicas científicas aplicadas al buscar, procesar e interpretar información referente a la temática, con la finalidad de sustentar en forma lógica y coherente los criterios expuestos desde la perspectiva del autor; dichos métodos son:

2.1 Investigación Literaria:

Es la revisión de documentos e investigaciones publicadas en la misma línea de estudio, particularmente en revistas científicas para recopilar criterios, experiencias y resultados en casos similares con el objeto de fundamentar la solución expuesta en este proyecto (Iño Daza, 2018).

2.2 Análisis Sistémico:

Es un proceso holístico cuya utilidad reside al tratar con medios informáticos, para clasificar, comparar valores o experiencia en un mismo argumento desde varios puntos de vista e inferir resultados afines, basados en la lógica y razones expuestas, a partir de

instigaciones críticas debidamente justificadas (Rodríguez Jiménez & Pérez Jacinto, 2017).

2.3 COBIT:

Sus siglas significan *Objetivos de Control para Información y Tecnologías Relacionadas* públicas por Instituto de Control de TI y la ISACA (Asociación de Auditoría y Control de Sistemas de Información; permiten diferenciar la gestión del control de TIC`s con el objeto de potenciar las estrategias en función de los activos informáticos, presentan una serie de modelos, herramientas de auditoría e integran mociones de mejora continua en la organización tanto para la automatización de procesos o seguridad en infraestructura computacional; en la *Ilustración 3* se observan sus principales consideraciones.

Ilustración 3. Habilidades y destrezas de la metodología COBIT
Fuente: (Yrigoyen Quintanilla , 2016)

2.4 Descriptivo:

Es un método ampliamente utilizado en las investigaciones, en especial aquellas de carácter cualitativo, gracias a que facilita explicar las propuestas gestadas y relaciones entre sus variables, denotando las posturas del autor en forma detallada, sintetizando lo analizado en forma dialéctica (Gauchi Risso, 2017).

3. DESARROLLO

En esta sección se expresan los hallazgos y apreciaciones relacionadas a la gestión del riesgo en la biblioteca de ingeniería civil en la UTMACH, mediante cuadros comparativos, síntesis de vulnerabilidades y análisis de las alternativas para solventar la problemática tratada en el estudio.

3.1 Identificación de vulnerabilidades y amenazas

La principal debilidad es la carencia de un plan de gestión de riesgos a nivel macro, es decir que integre todas las potencialidades, competencias y destrezas entre las carreras o departamentos de la UTMACH, sin embargo, la dirección de TIC`s dispone de directrices para regular los riesgos informáticos, aunque es poco conocido, sus sanciones no son drásticas ni se inculta un programa para culturizar a todos los responsables directa e indirectamente.

Otro punto crucial es los sistemas operativos, paqueterías de software y antivirus no son licenciados, sino versiones de prueba u open source pese a ser una entidad estatal.

La falta de recursos monetarios, deriva en un control poco flexible, mantenimiento preventivo nulo y desactualización en general; demostrando que la gestión exige ser tomada dentro de los presupuestos anuales, así como renovar la infraestructura tecnológica; pero no se encontraron debilidades graves o daños fuertes en las instalaciones que comprometan su continuidad.

Cuadro 1 Diagnóstico de vulnerabilidades y amenazas informáticas en biblioteca UAIC

VULNERABILIDAD	FUENTE DE AMENAZA
No existe un plan para gestionar los riesgos ni un procedimiento de cómo actuar frente a desastres, no están asegurados los activos informáticos ni existe fondos para respuesta inmediata	Fenómenos Naturales (sismos, tormenta eléctrica)
Daños en los equipos por variaciones de voltaje, instalaciones eléctricas vetustas, falta de mantenimiento instalaciones en general y fallos en reguladores de voltaje o cableado	Falla eléctrica o incendio
Hackeos Intercepción de información Inyección SQL Configuración inadecuada en servidor Falta de seguridades a nivel de red UTMACH	Crímenes cibernéticos
Falta de un plan macro para responder ante riesgos o ataques Desconocimiento de las políticas de seguridad (Departamento de dirección de TIC`s)	Administrativa/Política

Poca aplicación de políticas del centro de computo Falta de recursos económicos Gestión ineficiente de activos computacionales	
Uso indebido de ordenadores Virus, spam, botnet, códigos maliciosos Hurto de periféricos o datos Falta de capacitación Conducta inapropiada	Usuarios
Falta de mantenimiento No existe personal técnico disponible Desactualización de sistema operativos y Hardware	Descuido en ordenadores y equipos
Comportamiento poco ético Falta de control hacia los usuarios Desacato de políticas y acuerdos institucionales	Personal
Sanciones poco severas en políticas Carencia de un plan de seguridad integro Controles superficiales y poco tecnificados Baja implementación de métodos para prevenir y monitorear amenazas externas Desconocimiento en materia de auditoria Informática	Gestión de seguridad

Fuente: Elaboración Propia

3.2 Controles implementados e impacto de amenazas

Las medidas de seguridad son suficientes para responder a peligros relativamente bajos, pero la principal amenaza es la interna, no existe un pleno control u organización del personal ni empoderamiento institucional, destacando al factor humano como un agente a ser regulado no solo por leyes sino por medidas disciplinarias combinadas con tecnologías biométricas, además de carecer de un protocolo de respuesta inmediata y en caso de efectuarse un hackeo u otro ciber delito no se cuenta con la infraestructura para monitorear o mitigar el daño; además que según estudiantes los ordenadores no cuentan con la capacidad para agilizar una tarea, debido a su estado e incluso la red interna presenta fallos constantes.

Cuadro 2 Controles presentes en el centro de cómputo de biblioteca en UAIC

AMENAZAS	CONTROLES	DESCRIPCIÒN
Naturales, sismos, inundaciones e incendios	Detectores de humo	Detectar y actuar rápidamente en caso de incendios
	Respaldos	Backud de datos e información en la nube, discos duros externos y archivadores físicos
	Generadores de emergencia, seguridad en cableado	Suministro eléctrico a ordenadores y reguladores de voltaje con batería
Recurso humano, personal, estudiantes y factores accidentales	Capacitación	Personal profesional en el ingeniería de sistemas, seminarios de seguridad
	Auditoria interna	Existe control por parte de la Dirección de TIC`s y responsables del centro de computo
	Contraseñas	Uso de claves fuertes en ordenadores y correos institucionales, acceso de privilegios solo a personal autorizado
	Usuarios	Registro de uso de PC`s mediante carnet y firma
	Reglamentos y políticas	Acatar las directrices de la UTMACH designadas por el departamento de dirección de TIC`s
Lógicas e infraestructura digital	Antivirus Firewall Dirección IP de ordenadores y MAC en red interna UTMACH	No se tiene licencia corporativa ni activaciones pagadas del software, el servidor ofrece seguridad en base a certificados web y enrutamiento de dominios

Organizacionales	Garantías Seguros	Se cuenta con servicios técnicos y garantías de equipos, licencia Open source y personal calificado

Fuente: Elaboración Propia

No se realiza autoría en forma constante ni se ha retroalimentado las medias acordes a las nuevas amenazas de los sistemas informáticos, debido renovar las políticas de seguridad según las condiciones actuales de los sistemas y proyectas medios para vigilar, examinar e interpretar posibles problemas, tampoco se aplica una metodología estandarizada ni se cuenta con personal cuyo postgrado sea en seguridad computacional.

3.3 Medidas a implementar

En base a los análisis ejecutados, se plantean las siguientes consideraciones para reforzar la seguridad e incrementar protección informática:

3.3.1 Control de ordenadores por software

Hoy en día se disponen de programas de uso libre como *ciber admin 5* que solventa varias necesidades como gestión de usuarios, permiso de acceso, contenidos web, programas, grabación, acceso remoto e incluso alertas al desconectar un puerto USB o desactivar algún parámetro preestablecido.

3.3.2 Cámaras de Seguridad

Colocar video vigilancia en tiempo real, permite controlar las acciones, registrar los daños o responsables de actos indebidos, además mantiene una presión psicológica sobre los usuarios del centro de cómputo.

3.3.3 Licencias en sistema operativo

Por ser una entidad estatal y financiarse por el recurso público debe utilizar licencias libres de acuerdo a los objetivos estratégicos del plan nacional de desarrollo, que aconseja migrar para flexibilizar la informática, además de economizar recursos monetarios.

3.3.4 Redes privadas e infraestructura virtual

Optar por servicios en la nube o bondades cloud computing, ayudarían a respaldar información en forma dinámica, potenciarían las funcionalidades del centro de cómputo y se reforzaría la seguridad, puesto que Google integra mecanismos confiables en telemática.

Los firewall y servidores prestados no es suficiente ante un hacker, pese a no darse casos se debe prever una repotenciación a los dominios IP, redes internas, enlaces externos e incentivar medidas predictivas como monitoreo en tiempo real.

3.3.5 Reglamentos y biométrica

Diseñar políticas institucionales, directrices, sanciones, mecanismos disciplinarios y argumentos legales para actuar en caso de ataques, así como proponer al área administrativa en el departamento de compras públicas que gestionen fondos para mejorar la infraestructura tecnológica, en especial aquellas TIC`s de uso académico, siendo un eje paralelo en toda la UTMACH.

3.3.6 Concientización

En estudios similares se evidencia, que el mayor riesgo es la carencia de un plan estratégico, y el *factor humano* debido a su conducta irracional e ilógica, desacatando las mociones de seguridad, por ende culturizar a los estudiantes y capacitar continuamente al personal, aplicar incentivos e instruir programas de protección informática reducirá la incertidumbre, minimizara vulnerabilidades e incrementa el empoderamiento, siendo la prevención una medida eficiente evitando la amenaza desde su concepción.

3.4 Propuesta de plan de gestión de riesgos informáticos

El conjunto de tácticas que componen el plan son:

- Auditoria informática en forma periódica, al menos dos veces años al iniciar y culminar cada ciclo educativo.
- Diagnosticar vulnerabilidades y amenazas.
- Gestionar fondos, recursos e investigar soluciones desde la ingeniería en sistemas o desarrollo de software.
- Aplicar los controles citados o diseñar propuestas similares.
- Registrar ataques o daños informáticos para aprender e interpretar.
- Implementar un reglamento interno más severo y en acuerdo con las necesidades actuales.
- Socializar un plan estratégico de auditoria con todos los estudiantes y personal encargados para establecer responsabilidad-participación institucional.
- Adoptar una metodología para auditar como COBIT, seguir sus lineamientos al gestionar activos computaciones en base al desempeño organizacional.

- Retroalimentar en forma holística, no solo en biblioteca o laboratorios, sino disponer de una serie de acciones perfectamente descritas en toda la UTMACH, para analizar y responder integrantemente ante cualesquiera riesgos informático.

3.5 Evaluación del riesgo

El nivel de riesgo se califica como MEDIO, de los cuadros expuestos los cuatro peligros más prominentes son: Factor Humano, falta de fondos, carencia de un plan y mantenimiento; esto causa que el deterioro por el uso, deriva en fallos operativos en los equipos; algunas desatenciones como control riguroso a estudiantes, horarios de atención, baja velocidad de internet, ausencia de servidores propios y falta de conocimientos en seguridad informática originan los percances, puesto que aun sin intención se cometen falencias accidentales o humanas, expresando un riesgo aparente.

Es necesario medir cualitativamente el nivel de protección, calificado como BUENO puesto que existen controles aplicados frente a todas las amenazas detectadas, esto da noción para indagaciones futuras sobre los puntos a mejorar en el centro de cómputo de biblioteca en la Unidad Académica de Ingeniería Civil.

4. CONCLUSIONES Y RECOMENDACIÓN

En función a lo expuesto en el trabajo se concluye lo siguiente:

La valoración del riesgo depende de la metodología utilizada en medir su impacto, en este caso se utiliza Cobit 5, apreciaciones competentes a la catedra de auditoria informática y una valoración cualitativa, denotando un nivel de riesgo Medio frente a un control Bueno que responde superficialmente iterando los aspectos clave delineados por la dirección de TIC`s, no se cuenta con un auditor externo ni un plan de manejo macro, siendo una debilidad latente en todo la UTMACH.

La principal amenaza es *interna* la falta de cooperación del cuerpo estudiantil, carencia de conocimiento e inculturación en materia de seguridad informática convergen en una serie de vulnerabilidades afines al recurso humano y particularmente en la parte administrativa, que no toma las debidas acciones ni deroga la relevancia necesaria en potenciar las bondades computaciones sistemáticamente en forma paralela a los objetivos institucionales.

Las instalaciones, ordenadores, personal encargado y en general se cumplen con regulares tanto políticas, como físicas y lógicas; prestando un cierto grado de respuesta frente a problemas como virus, daños, perdida de datos e inferencias que aprovechan debilidades bajas como desatenciones o falta de mantenimiento; no se cuenta con el recurso monetario ni especializado en caso de efectuarse un hackeo o incluso detectar alguna anomalía desde internet.

Los controles propuestos integran el plan de gestión en forma holística, pero de carácter cognitivo aconsejando un análisis concatenado con ingeniería de software y de sistemas para de manera interdisciplinaria diseñar mecanismos de seguridad con mayor eficiencia; se recomienda elegir bondades cloud computing por ser el eje transversal donde se solventan tanto funciones administrativas como académicas, además de optimizar el desempeño informático en la Universidad Técnica de Machala.

En el campo de la protección de datos es imperioso ser consciente del potencial y peligrosidad de la telemática, usar sus cualidades para fines investigativos permite fundamentar epistemológicamente estudios, sin embargo el abuso de redes sociales, juegos, entretenimiento, entre otros han distorsionado sus fines hacia el consumismo, en especial para los estudiantes quienes no aprovechan las bases de datos ni redes internas para fines educativos; por lo tanto actualizar las directrices de la dirección de TIC`s según las nuevas vulnerabilidades reforzaría el control actual en forma dinámica, recomendando renovarlos cada cinco años.

5. REFERENCIAS BIBLIOGRÁFICAS

Arcentales-Fernández, D. A., & Caycedo-Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias Vol. 3*, 157-173.

Corda, M. C., Viñas, M., & Coria, M. K. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra Clave (La Plata), vol. 7, n° 1*, 1-18.

Gauchi Risso, V. (2017). Estudio de los métodos de investigación y técnicas de recolecciónde datos utilizadas en bibliotecología y ciencia de la información. *Revista Española de Documentación Científica, 40(2)*, 1-13.

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, núm. 2*, 193-197.

Hernández Saucedo , A. L., & Mejia Miranda, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *ReCIBE. Revista electrónica de Computación, Informática Biomédica y Electrónica, núm 1*.

Iño Daza, W. G. (2018). Investigación educativa desde un enfoque cualitativo: la historia oral como método. *Voces De La Educación; 3(6)*, 93-110.

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

Minero Alejandre, G. (2017). Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea. *Anuario Jurídico y Económico Escurialense*, 13-58.

Montaño Fernández, M. (2016). Nuevas tendencias en auditoría: análisis de datos y aseguramiento continuó. *Fides Et Ratio - Volumen 12*, 193-208.

Quiroz-Zambrano, S. M. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias; Vol. 3, núm. 5*, 676-688.

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

Roquez Hernandez , R. V., & Juarez Ibarra, C. M. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. *Paakat: Revista de Tecnología y Sociedad; Año 8, número 14*, 1-13.

Vega Villacís , G., & Ramos Morocho, R. A. (2017). VULNERABILIDADES Y AMENAZAS A LOS SERVICIOS WEB DE LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO. *3C Tecnología (Edición 21) Vol.6 – Nº 1*, 53-66.

Yrigoyen Quintanilla , M. (2016). Modelo de referencia de gobierno de las tecnologías de la información para instituciones universitarias. *Interfases, No 9*, 87-115.