UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LAS VULNERABILIDADES Y AMENAZAS EN EL CENTRO DE CÓMPUTO DEL LABORATIRO DE LA UACS DE LA UTMACH.

RAMON GUAZHA JAZMIN STEFANY
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LAS VULNERABILIDADES Y AMENAZAS EN EL CENTRO DE CÓMPUTO DEL LABORATIRO DE LA UACS DE LA UTMACH.

RAMON GUAZHA JAZMIN STEFANY
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE LAS VULNERABILIDADES Y AMENAZAS EN EL CENTRO DE CÓMPUTO DEL LABORATIRO DE LA UACS DE LA UTMACH.

RAMON GUAZHA JAZMIN STEFANY
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 23 DE AGOSTO DE 2019

MACHALA
23 de agosto de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado ANÁLISIS DE LAS VULNERABILIDADES Y AMENAZAS EN EL CENTRO DE CÓMPUTO DEL LABORATIRO DE LA UACS 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: viernes 23 de agosto de 2019 - 10:11

Urkund Analysis Result

Analysed Document:	JAZMÌN RAMÒN.docx (D54788248)
Submitted:	8/12/2019 7:20:00 PM
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, RAMON GUAZHA JAZMIN STEFANY, en calidad de autora del siguiente trabajo escrito titulado ANÁLISIS DE LAS VULNERABILIDADES Y AMENAZAS EN EL CENTRO DE CÓMPUTO DEL LABORATIRO DE LA UACS 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.

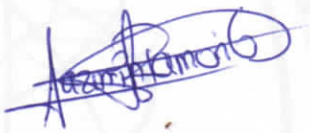
La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

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, 23 de agosto de 2019



RAMON GUAZHA JAZMIN STEFANY
0705592012

RESUMEN

La Universidad Técnica de Machala (UTMACH) gestiona grandes cantidades de datos e información referentes a sus funciones académicas, siendo de carácter imperioso contar con un sistema de seguridad contra amenazas lógicas, cuyas accionantes son competencias de la auditoría informática. El trabajo escrito pertinente relata el estudio efectuado en esquematizar un plan de respuesta en caso de ciber ataques en función de las vulnerabilidades/amenazas latentes en la biblioteca de ciencias sociales, para describir cuales procesos seguir, qué medidas tomar e inducir los mecanismos para defender y salvaguardar los activos informáticos; se aborda la indagación desde una perspectiva cognitiva, exploratoria y heurística para analizar desde varios puntos de vista la mejor alternativa en desarrollar una serie de pasos/medidas coordinadas, al gestionar adecuadamente los recursos virtuales en el centro de cómputo estudiado, también se postulan criterios teóricos, opiniones e integrar herramientas o prestaciones que faciliten el uso de las TIC`s, los controles físicos/lógicos enfocados a un plan estructurado permiten una solvencia adecuada frente a imprevistos, además de contar con respaldos de información/datos, configuraciones y un monitoreo constante mediante la auditoría facilita mantener un orden en la distribución de conocimientos, además coordinar el uso de computadores, prestaciones de libros, consultar e integrar recursos para el desarrollo investigativo de las asignaturas, demanda una responsabilidad que debe ser solventada en base a un plan integral de manejo para procurar el buen uso de las tecnológicas informáticas.

Palabras Clave: Tecnologías de comunicación e información, gestión, riesgos, plan de manejo.

ABSTRACT

The Technical University of Machala (UTMACH) manages large amounts of data and information related to its academic functions, and it is imperative to have a security system against logical threats, whose actuators are competences of computer auditing. The relevant written work relates the study carried out in schematizing a response plan in case of cyber attacks based on the latent vulnerabilities / threats in the social sciences library, to describe which processes to follow, what measures to take and induce the mechanisms to defend and safeguard computing assets; the investigation is approached from a cognitive, exploratory and heuristic perspective to analyze from several points of view the best alternative in developing a series of coordinated steps / measures, when properly managing virtual resources in the computer center studied, theoretical criteria are also postulated ,

opinions and integrate tools or benefits that facilitate the use of ICTs, physical / logical controls focused on a structured plan allow adequate solvency against unforeseen events, in addition to having information / data backups, configurations and constant monitoring Through the audit it facilitates maintaining an order in the distribution of knowledge, in addition to coordinating the use of computers, book provision, consulting and integrating resources for the research development of the subjects, it demands a responsibility that must be solved based on a comprehensive plan of management to ensure the proper use of technology as computer.

Keywords: Communication and information technologies, management, risks, management plan.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

1. INTRODUCCIÓN

La era digital cohesiona inmensurables cantidades de información, obligando a todas las organizaciones adaptarse a la gestión de conocimiento, siendo de forma imperiosa para las instituciones de educación superior administrar en forma eficiente y libre acceso para todo el cuerpo docente/estudiantes.

Las bibliotecas hoy en día constituyen un complejo sistema de información, son indispensables para ejecutar investigaciones, argumentar estudios, documentar proyectos, por lo tanto, debe administrar los usuarios mediante entornos online capaces de permitir acceso a bases de datos, libros, trabajos de titulación; mantener un espacio físico acoplado a las necesidades del estudiante tanto a nivel tecnológico como confort.

Debido a que comúnmente son usadas para efectuar actividades académicas, leer libros, descargar documentos, siendo un portal relevante para ayudar en la formación profesional; además que el acoplar recursos multimedia a través de internet maximiza tanto sus virtudes como los riesgos, en forma paralela a sus potencialidades exigiendo un proceso detallado al garantizar la calidad de sus servicios a la comunidad universitaria.

Los sistemas de gestión son la clave para optimizar cualquier organización, de ellos depende la manera en que se ejecutan las tareas y cómo responden ante eventualidades, en las empresas o instituciones que manejan información o conjuntos de datos, es necesario auditar para estructurar un modelo propio de funcionamiento/desarrollo, bajo una retroalimentación que fomente una mejora continua de sus actividades.

Según Cancelado, un plan de manejo en su nivel más básico incluye:

- Evaluación de los riesgos, priorizando amenazas/vulnerabilidades latentes
- Análisis de posibles ataques, sus afectaciones o daños al entorno de la institución
- Controles utilizados contra las vulnerabilidades, eficiencia de los mismos
- Controles físicos al personal, responsables y autoridades competentes
- Auditoria regular para evaluar al sistema e imponer mejoras. (Cancelado, 2018)

Los mecanismos logísticos de información/comunicación son un eje evolutivo para las industrias, solventan requerimientos y exponencian sus facultades, sin embargo, no sólo implican cambios tecnológicos ni en infraestructura, sino una transformación cultural para las masas, gracias en gran medida la brecha digital reduce el entorno personal físico del paralelo virtual, e inclusive la manera de ver las cosas/prestar servicios ha revolucionado todos los ámbitos sociales en especial la preparación académica.

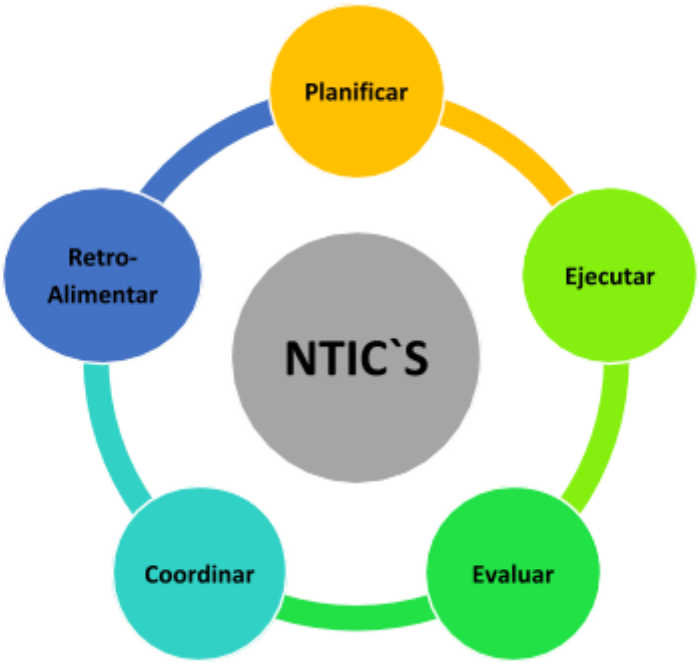


Ilustración 1. Esquema general de un sistema de gestión
Fuente: Elaboración Propia

El mejor sistema de gestión es aquel que integra recursos en función de proceso eficiente para cumplir exitosamente los objetivos, siendo capaz de auto-organizarse, recompensar en forma conjunta y justa a todos los responsables (Torres Peñafiel, Fierro lopez , Torres Peñafiel, & Ponce Andrade, 2018). Además, plan de acción consciente procura minimizar riesgos, maximizar resultados, armonizar y sintonizar sus cualidades sin perder versatilidad ni fluidez al adaptarse a cambios extremos, como los apreciados en la sociedad contemporánea

El proyecto pertinente tiene por objetivo desarrollar un plan de gestión, paso a paso para responder en forma oportuna a las vulnerabilidades/amenazas presenten en el laboratorio de la Unidad Académica de Ciencias Sociales para mejorar el manejo de las NTIC`s en favor del desempeño académico.

2. DESARROLLO

El proceso para elaborar un plan de gestión de riesgos, primero es identificar cuáles son las vulnerabilidades, falencias e identificar posibles ataques informáticos al laboratorio de la Unidad Académica de Ciencias Sociales, luego se debe explicar cuáles medidas tomar, qué herramientas o pasos seguir para garantizar la seguridad tanto de la información como de los equipos.

2.1 Identificación de riesgos

Se observa que existen daños potenciales a los recursos digitales, debido a complicaciones e inferencias en el mantenimiento, actualizaciones de controles respectivos en la seguridad, pese a ello no se han detectado ni diagnosticado ataques graves o intrusiones que comprometan las funciones institucionales, sino falencias comunes de los sistemas informáticos.

Cuadro 1. Matriz de riesgos en relación causa-efecto

Causa	Efecto	Solución
Virus, malware	Daño de información o equipo	Actualizar antivirus, usar aplicaciones de control, respaldo del sistema
Ataques informáticos, hackers, infiltraciones	Pérdida de información digitalizada/espionaje	Respaldos de seguridad, copias en la nube/monitoreo permanente
Falencias o actos indebidos por estudiantes/personal	Daños de equipos, pérdida o robo de información	Aplicar controles estrictos y logísticos a personal, empoderar al cuerpo estudiantil/docente
Falta de plan de seguridad	Poca o nula respuesta frente a atentados o amenazas	Diseñar e implementar un plan de seguridad
Falta de personal especializado	Errores o fallos en operación del sistema	Contratar personal especializado en riesgo informático
Falta de presupuesto	Poco desarrollo de destrezas del centro de computo	Realizar diligencias y planificar costos de mejoramiento del centro de computo
Desactualización de equipos/infraestructura	Fallos en sistema operativo/incomodidad en usuarios	Re potencialización del centro de cómputo, atención de las autoridades al establecimiento

Fuente: (CARRILLO GUILLEN, 2018)

2.2 Diagnóstico de controles de seguridad

Luego de realizar la investigación de campo, entrevistar al personal y recopilar criterios técnicos sobre las posibles maneras de mejorar la gestión de riesgos, se propone las siguientes consideraciones detalladas en el cuadro 2.

Cuadro 2. Controles sistemáticos de seguridad informática

DOMINIO	OBJETIVOS	CONTROLES
Políticas de seguridad de información	Directrices de dirección en TIC`s	Conjunto de controles y medidas para seguridad de datos
Organización de seguridad informática	Organización interna	Asignación de responsabilidades, tareas, coordinación interna con autoridades
Seguridad en recursos humanos	Regular comportamiento y factor humano en la gestión de TIC`s	Proceso disciplinarios, acuerdos de confidencialidad, medias de prevención de desacato
Gestión de activos	Responsabilidad sobre activos	Inventarios, propiedad y valoración de activos
Control de acceso	Gestión/privilegios de usuarios	Gestión de derechos y uso del sistema
Cifrado	Controles criptográficos	Gestión de claves/contraseñas encriptadas
Seguridad física y ambiental	Áreas seguras, seguridad de equipos	Protección contra amenazas físicas, mantenimiento, controles de entrada e instalaciones especiales para regular/proteger
Seguridad de las operaciones	Consideraciones de auditoría interna, control de software, registro y monitoreo de actividades, gestión de vulnerabilidades	Aplicar controles de auditoría informática, gestionar amenazas e implementar controles de respaldo, respuesta y defensa
Seguridad en telecomunicaciones	Seguridad en redes e internet, configurar servidores	Controles de red, mecanismos de seguridad, segregación de la red
Desarrollo y mantenimiento en sistemas de información	Seguridad en procesos de soporte y desarrollo	Análisis, políticas de seguridad, adquirir nuevas tecnologías de seguridad, protección de datos

Relación con suministradores	Gestión de prestación de suministros	Supervisión y control de servicios prestados por terceros
Gestión de incidentes en seguridad de información	Gestión de incidentes para aprender y mejorar	Procedimientos, respuesta y recopilar evidencias del incidente
Cumplimiento	Cumplir objetivos institucionales, acuerdos legales y contractuales	Identificar legislación aplicable, propiedad intelectual, proteger datos y privacidad personal

Fuente: (ISO 27002, 2013)

2.3 Plan de acción

En base a los cuadros analizados y observaciones realizadas en el laboratorio estudiado, se proponen los siguientes pasos del plan de gestión de riesgos:

1) Realizar auditoria informática en forma anual.
2) Implementar controles de seguridad contra vulnerabilidades en gestión de red, archivos, contenidos multimedia, virus.
3) Aplicar software de monitoreo y control de activos lógicos.
4) Disciplinar, capacitar, concientizar tanto al personal como estudiantes sobre la seguridad de la información e informática.
5) Realizar copias de seguridad de todos los archivos.
6) Actualizar y renovar sistemas operativos, antivirus, software de administración de ordenadores
7) En caso de incidentes:
    - ❖ Notificar a la dirección de TIC`s
    - ❖ Responder ante la eventualidad/contrarrestar daños
    - ❖ Recopilar evidencia
    - ❖ Evaluar y valorar daños/costo/pérdidas
    - ❖ Tomar medidas legales/penales
    - ❖ Analizar eficiencia de controles de seguridad
    - ❖ Proponer medidas para mejorar el sistema
8) Gestionar fondos/recursos para potenciar/mantener los activos informáticos
9) Retroalimentar constantemente en forma holística la gestión de riesgos

Para reducir la subjetividad al momento de evaluar y cotizar impactos es necesario se desarrollen políticas nacionales de control, regulación, distribución, e integrar

comercialización de soluciones *cloud computing* debido a que generan dependencia de empresas (VALENCIA, MARULANDA, & LOPEZ TRUJILLO, 2015).

2.4 Fundamentación teórica

Este apartado comprende todos las definiciones, acotaciones y terminología referente al desarrollo del proyecto, siendo argumentados desde las investigaciones de autores entendidos en la materia, para ser explicados en relación al enfoque del presente escrito.

Seguridad de la informática e información: Son términos comunes, suelen confundirse porque forman parte de la gestión en riesgos, son de carácter indispensable en toda organización o empresa; la seguridad informática es una disciplina sistemática que conjuga los controles, mecanismos, configuraciones y medidas para garantizar la solvencia de la infraestructura informática.

La seguridad de la información se refiere a proteger los datos para gozar de disponibilidad, calidad, privacidad e integridad sin condicionar al usuario (Figueroa Suarez, Rodriguez Andrade, Bone Obando, & Saltos Gomez, 2017).

2.4.1 Plan de gestión de riesgos en bibliotecas.

Es la protección de todos los aspectos competentes: edificación e instalaciones, a las personas, acervo bibliográfico; comúnmente se depende de un área que destina plan de manejo organizacional, enfatizando en los activos digitales donde, debe converger lo siguiente:

- Políticas de seguridad informática institucionales
- Reglas e instructivos propios de biblioteca
- Controles físicos y lógicos
- Planes de contingencia para documentaciones físicas y en ordenadores
- Guías para usuarios en uso de recursos informáticos
- Responsabilidad de encargados/estudiantes
- Desarrollar o acoplar filosofías de gestión para una administración heurística
- Auditoría permanente para medir riesgos y respuesta frente a ellos. (Corda, Viñas, & Coria, 2017)

2.4.2 Auditoría Informática.

Es una ciencia encargada de monitorear, evaluar, probar y retroalimentar los sistemas digitales para regular la seguridad de la información, detectar errores o integrar nuevas medidas que optimicen el desempeño de la organización; en lo relacionado a empresas es

una doctrina que certifica una mejora continua en los procesos (Salgado Soto , Osuna Millan , Sevilla Caro, & Morales Garfias, 2017).

2.4.3 Riesgos en entornos informáticos e información

El análisis de riesgos resuelve tres interrogantes, qué se va a proteger, de qué se protege y cómo se protege, generalmente en activos digitales la seguridad es tanto lógica como física, analizando las debilidades que generar vulnerabilidad, saber cuáles amenazas son más probables de ocurrir; en conjunto se diseña un entorno capaz de resistir ataques, actuar en forma oportuna y minimizar los daños eficazmente.

Los riesgos comunes son virus, pérdida/alteración de datos, hackeos, violaciones de reglas por personal, uso indebido de información o factores como desatención, falta de mantenimiento u otras condiciones que deterioren la calidad del sistema informático (Tejena Macías, 2018).

2.4.4 Controles de seguridad.

Se refiere a todas las medidas necesarias para mitigar, prevenir y regular todos los factores de riesgo; comprende la mecánica para procesar contenidos, administrar labores académicas y garantizar la protección de todos los documentos físicos/digitales (Molina Miranda, 2017).

Es importante que como *control* se denomine a la capacitación constante tanto a personal como estudiantes universitarios, de las medidas, aptitudes e instaure una cultura de seguridad informática, en especial sobre sus datos personales, así como respetar las normas de la era digital.

Un forma eficiente de regular los riesgos es concientizar al personal sobre la relevancia de la seguridad informática desde el colectivo hacia todas las áreas de una organización permite un desarrollo paralelo a las potencialidades virtuales (Roque Hernandez & Juarez Ibarra , 2018).

2.4.5 Sistemas de información en bibliotecas.

Son la integración de mecanismos que automatizan, sintetizan y simplifican procesos, requieren lenguajes de programación de libre acceso, categorización de indexada para búsqueda de documentos, interacción con correo institucional para préstamo de libros, integran repositorios institucionales, soporte virtual para plataforma de usuarios,

digitalización de procesos bibliotecarios; todos estos ítem pueden ser sustentados mediante entornos en la nube con plena seguridad y eficiencia (Sánchez & Sánchez, 2018).

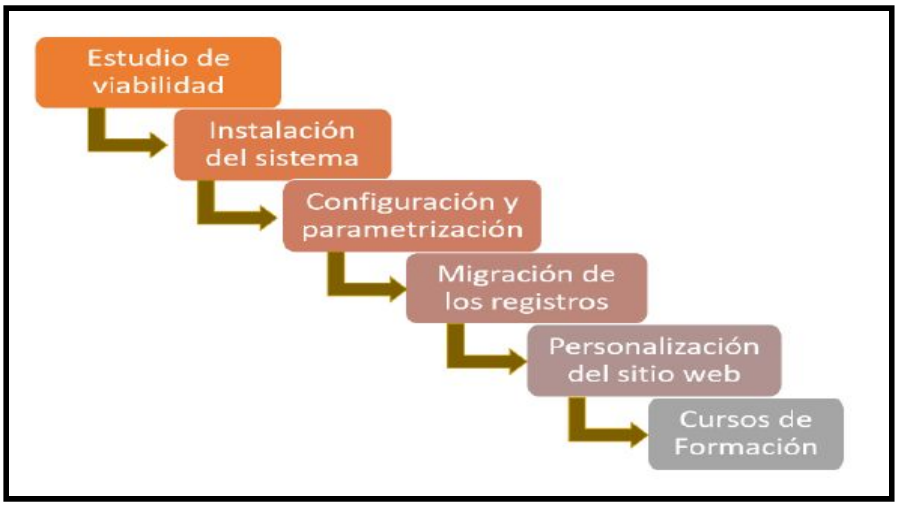


Ilustración 2. Esquema de sistema gestor bibliotecario
Fuente: (Sahagun Montoya, Barrios Garcia , Nava de la rosa, & Bañuelos Rodarte , 2017)

2.4.6 Políticas UTMACH

La Universidad Técnica de Machala (2015) cuenta con normativa propia sobre la seguridad y protección de activos informáticos e información con el fin de gestionar en forma eficiente las TIC´s en función de su responsabilidad institucional, los principales lineamientos son:

- La Dirección de Tecnología de la información y Comunicación son los encargados de regular, desarrollar, automatizar y suplir las necesidades informáticas de la UTMACH
- El acceso de los ordenadores se restringe de acuerdo a los roles y perfiles de cada funcionario
- El control de softwares, aplicaciones, antivirus o cualquier programa es competencia de la dirección de TIC's
- Cuando un usuario cambia o cesa sus funciones se debe dar de baja a sus privilegios y asegurar la integridad en el buen uso de activos digitales
- Es competencia de cada usuario navegar en forma consciente evitando contenidos inapropiados e inferir en actividades con fines ajenos a los académicos
- La instalación de antivirus, mantenimiento y revisión de ordenadores se ejecuta en forma periódica coordinando con la dirección de tic´s
- La correcta administración del correo institucional es responsabilidad de cada usuario, así como evitar contacto con posibles amenazas

- ❖ Es responsabilidad de cada funcionario gestionar las copias de respaldo de datos, documentos e información en forma periódica evitando pérdidas importantes
- ❖ Los acuerdos de confidencialidad se deben firmar a todo el personal que se relacione con la UTMACH con la finalidad de evitar filtraciones, proteger y dar buen uso a los datos (Universidad Técnica de Machala, 2015).

2.4.7 Políticas referentes la Constitución del Ecuador

En la sección tercera referente a comunicación e información, se resumen los siguientes puntos referentes al manejo de TI:

- ❖ La información es un derecho individual, colectivo y organizacional, siendo competencia del estado garantizar su desarrollo-gestión
- ❖ Toda persona tiene derecho al libre acceso de información producida por entidades públicas o privadas
- ❖ El estado garantiza la transparencia e igualdad en condiciones de recursos informáticos
- ❖ El acceso universal a las tecnologías de información y comunicación.

(República del Ecuador, 2008)

Los métodos usados son las técnicas aprendidas en las cátedras afines a la auditoría informática, en forma práctica y técnica al conjugar los mejores criterios para resolver la problemática.

2.4.8 Metodología para gestión de riesgos.

Hoy en día existen procedimientos sistemáticos que mediante pasos ordenados auditan los riesgos, MARGERIT es un método para gestión de riesgos basado en PILAR que es una herramienta software para detectar amenazas, medir la probabilidad e impacto a los activos y determinar criterios de aceptación de riesgos, junto a los controles de seguridad necesarios.

<table>
<tr><th>PHVA</th><th colspan="3">ISO 27005</th><th colspan="2">ISO 31000</th></tr>
<tr><td rowspan="9">Planear</td><td colspan="3"></td><td colspan="2">Mandato y compromiso de la dirección</td></tr>
<tr><td colspan="3">Definir Plan de gestión de riesgos</td><td colspan="2">Diseño del marco de trabajo para gestión de riesgos</td></tr>
<tr><td colspan="2">Establecimiento del contexto</td><td rowspan="9">Proceso de gestión del riesgo</td><td colspan="2">Entender la organización y su contenido</td></tr>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">Definir responsabilidades</td></tr>
<tr><td colspan="2">Recursos</td></tr>
<tr><td colspan="2">Integración con procesos</td></tr>
<tr><td colspan="2">Establecer mecanismos de comunicación</td></tr>
<tr><td>Identificación del riesgo</td><td rowspan="3">Valoración del Riesgo</td><td colspan="2" rowspan="3"></td></tr>
<tr><td>Estimación del riesgo</td></tr>
<tr><td>Evaluación del riesgo</td></tr>
<tr><td colspan="2">Desarrollar el plan de tratamiento del riesgo</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td></tr>
<tr><td rowspan="3">Hacer</td><td colspan="3"></td><td colspan="2">Establecer políticas para la gestión del riesgo</td></tr>
<tr><td colspan="2">Implementar el plan de tratamiento</td><td>Implemnetación del marco de trabajo para la gestión de riesgos</td><td>Implementar el proceso de gestión de riesgos</td></tr>
<tr><td colspan="2">Implementar el plan de comunicación del riesgo</td><td colspan="2"></td></tr>
<tr><td>Verificar</td><td colspan="2">Monitoreo y revisión del riesgo</td><td colspan="2">Monitoreo y revisión del marco de trabajo</td></tr>
<tr><td>Actuar</td><td colspan="2">Mantener y mejorar el proceso de gestión</td><td colspan="2">Mejora continua del marco de trabajo</td></tr>
</table>

Ilustración 3. **Modelo PDCA (Plan, Do, Check, Act) para gestión de riesgos mediante normativa ISO**
Fuente: *(Arevalo Moscoso, Cedillo Orellana, & Moscoso Bernal, 2017)*

3. CONCLUSIONES Y RECOMENDACIONES

La auditoría informática es imperiosa en toda organización, en especial en las instituciones de educación superior debido a que gestionan en forma obligatoria grandes cantidades de información, datos de estudiantes, notas, recursos y activos informáticos necesarios en el desempeño académico al propiciar en forma paralela la formación profesional, servicios/prestaciones mediante plataformas digitales, acorde a las competencias de cada especialidad e integrar destrezas tecnologías para su ejercicio en el ámbito laboral.

Un plan de gestión de riesgos permite un desarrollo concreto de las labores institucionales en forma segura y confiable, gracias a que regula detalladamente los imprevistos, ataques o incidentes referentes a la información, tomando todas las medidas relativas al control tanto físico como lógico; no obstante existe cierto grado de incertidumbre debido a que las prestaciones tecnológicas se basan en soluciones que se adaptan rápidamente, a una velocidad mayor del crecimiento de la UTMACH, haciendo hincapié en el requerimiento de un sistema de gestión de riesgos macro que conjugué a toda la universidad, así como velar por la renovación, actualización y potenciación de la infraestructura informática para incrementar la eficiencia organizacional de nuestra alma mater.

Los riesgos son la convergencia de dos factores amenazas y vulnerabilidades, derogadas por desatenciones o falencias en la operatividad del sistema, por ende, es urgente contar con servidores propios, configuraciones seguras en redes e internet, renovar periféricos, dispositivos, ordenadores, router e integrar herramientas de control/calidad en auditoría informática que se acoplen a estándares internacionales de seguridad, para gestar en forma holística concatenando con una logística interna capaz de optimizar todos los procesos gracias a que la mayoría de ellos son sustentados digitalmente.

4. REFERENCIAS BIBLIOGRÀFICAS

Arevalo Moscoso, F. M., Cedillo Orellana, I. P., & Moscoso Bernal, S. A. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Revista Killkana Técnica. Vol. 1, No. 2*, 31-42.

Cancelado, A. (2018). *Gestiopolis.* Obtenido de Administración de riesgos en tecnología informática: https://www.gestiopolis.com/administracion-de-riesgos-en-tecnologia-informatica/

Cano-Pita, G. E. (2018). Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones. *Dominio de las Ciencias Vol. 4 Num.1*, 206-217.

CARRILLO GUILLEN, K. (2018). *EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE COMPUTO DE LA BIBLIOTECA DE LA UACE-UTMACH.* Machala: UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES-UTMACH.

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, núm. 1*, 1-18.

Figueroa Suarez, J., Rodriguez Andrade, R., Bone Obando, C., & Saltos Gomez, J. (2017). La seguridad informática y la seguridad de la información. *Polo del Conocimiento Vol. 2 No. 12*, 145-155.

ISO 27002. (2013). *Organización Internacional de Normalización ISO* . Obtenido de La norma ISO 27002 complemento para la ISO 27001: https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/

Mieles, J. M., & Toro, D. P. (2018). LOS SISTEMAS DE GESTIÓN BIBLIOTECARIOS Y SU USO EN LAS UNIVERSIDADES MANABITAS. *Revista Caribeña de Ciencias Sociales*.

Molina Miranda, M. F. (2017). ANÁLISIS DE RIESGOS DE CENTRO DE DATOS BASADO EN LA HERRAMIENTA PILAR DE MAGERIT. *Espirales revista multidisciplinaria de investigación Vol. 1 No.11*, 1-9.

Oscar Molina, C. S. (109-134). Tipos de Problemas que Provocan la Generación de Argumentos Inductivos, Abductivos y Deductivos. *Bolema, Rio Claro (SP), v. 33, n. 63*, 2019.

Pulido Polo, M. (2015). Ceremonial y protocolo: métodos y técnicas de investigación científica. *Opción, vol. 31, núm. 1*, 1137-1156.

República del Ecuador. (2008). *CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR .* Quito: Asamblea Constituyente.

Roque 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, núm. 14*, 2-13.

Sahagun Montoya, L. A., Barrios Garcia , J. A., Nava de la rosa, M. G., & Bañuelos Rodarte , M. (2017). Sistema para la administración de biblioteca de la Universidad Tecnológica del Estado de Zacatecas con Koha-Kobli. *Revista de Sistemas y Gestión Educativa Vol.4 No.13*, 35-43.

Salgado Soto , M., Osuna Millan , N., Sevilla Caro, M., & Morales Garfias, J. I. (2017). La Auditoría Informática en las organizaciones. *Revista Electrónica sobre Cuerpos Académicos y Grupos de Investigación en Iberoamérica Vol.4 No 8.*, 1-14.

Sánchez, L. S., & Sánchez, R. C. (2018). Sistema de Gestión Bibliotecaria ABCD 3.0. *Revista Publicando, 5. 14 (3)*, 583-593.

Tejena Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo del Conocimiento. (Edición núm. 18) Vol. 3, No 4*, 230-244.

Torres Peñafiel, N., Fierro lopez , P. E., Torres Peñafiel, S., & Ponce Andrade, A. L. (2018). LA CONCEPTUALIZACIÓN DE ORGANIZACIÓN DESDE UN ENFOQUE SISTÉMICO. *SATHIRI Vol. 13 – N° 1*, 147-159.

Universidad Técnica de Machala. (2015). *Politica general de seguridad de la información de la universidad técnica de Machala.* Machala: Dirección de TIC´s.

VALENCIA, F. J., MARULANDA, C. E., & LOPEZ TRUJILLO, M. (2015). Gobierno y gestión de riesgos de tecnologías de información y aspectos de información y aspectos diferenciadores con el riesgo organizacional. *Revista GerenciaTecnológica Informática, 14(40)*, 65-77.