UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LOS RIESGOS INFORMÁTICOS DEL CENTRO DE CÓMPUTO DE LA BIBLIOTECA DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRION RODRIGUEZ DAMARIS CRISTINA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LOS RIESGOS INFORMÁTICOS DEL CENTRO DE CÓMPUTO DE LA BIBLIOTECA DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRION RODRIGUEZ DAMARIS CRISTINA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE LOS RIESGOS INFORMÁTICOS DEL CENTRO DE CÓMPUTO DE LA BIBLIOTECA DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRION RODRIGUEZ DAMARIS CRISTINA
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 ANÁLISIS DE LOS RIESGOS INFORMÁTICOS DEL CENTRO DE CÓMPUTO DE LA BIBLIOTECA DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES, 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: lunes 26 de agosto de 2019 - 07:57

Urkund Analysis Result

Analysed Document:	CARRION RODRIGUEZ DAMARIS CRISTINA_PT-010419.pdf (D54791018)
Submitted:	8/13/2019 2:02:00 AM
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, CARRION RODRIGUEZ DAMARIS CRISTINA, en calidad de autora del siguiente trabajo escrito titulado ANÁLISIS DE LOS RIESGOS INFORMÁTICOS DEL CENTRO DE CÓMPUTO DE LA BIBLIOTECA DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES, 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

CARRION RODRIGUEZ DAMARIS CRISTINA
0704230283

RESUMEN

En la actualidad la revolución informática a través de las tecnologías de información (TI) han cambiado la forma de manejar y manipular la información, ello ha hecho que estas sean de fácil acceso no solo para los usuarios que requieren dicha información, sino de aquellos intrusos que vulneran la seguridad informática. Lo cual ha promovido entre las empresas implementar sistemas de seguridad que eviten el riesgo informático y por ende el mal manejo de su información que es de carácter confidencial; expuesto lo anterior surgió la necesidad de realizar un análisis de los riesgos informáticos del centro de cómputo de la biblioteca de la Unidad Académica de Ciencias Empresariales, para lo cual se tomó en consideración la ejecución de una auditoría informática en base a la metodología OCTAVE, la cual nos acercó a la realidad que vive el centro de cómputo en cuanto a riesgos informáticos, en donde se pudo constatar y asegurar que poseen un programa básico, lo cual está incidiendo para que no cuenten con un respaldo y control de actividades que se llevan dentro del cómputo de la biblioteca de la UACE, por lo que es un tema que requiere mayor atención por parte de los administradores con el fin de evitar riesgo informáticos.

Palabras claves: Tecnologías de información, seguridad informática, riesgo informático, auditoría informática, metodología OCTAVE.

ABSTRACT

At present, the computer revolution through information technologies (IT) have changed the way of handling and manipulating information, this has made them easy to access not only for users who have such information, but for those intruders who violate computer security. Which has promoted among companies to implement security systems that avoid computer risk and for the mismanagement of their information that is confidential; exposed the above surgical need to perform an analysis of the computer risks of the computer center of the library of the Academic Unit of Business Sciences, for which it will be considered in the execution of a computer audit based on the OCTAVE methodology, which He brought us closer to the reality of the computer center in terms of computer risks, where it was possible to verify and control that they have a basic program, which is affecting so that they do not have a support and control of activities that are carried out within of the computation of the UACE library, so it is an issue that requires more attention by administrators in order to avoid computer risk.

Keywords: Information technologies, computer security, computer risk, computer audit, OCTAVE methodology.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLA

INTRODUCCIÓN

El presente trabajo se enfoca en un "Análisis de los riesgos informáticos del centro de cómputo de la biblioteca de la Unidad Académica de Ciencias Empresariales", tiene por objetivo de estudio realizar un diagnóstico de los diferentes riesgos que pueden existir en dicha área, para lo cual se tomarán parámetros de identificación, evaluación y verificación de riesgos informáticos que existen dentro de la misma, por medio de la entrevista estructurada como instrumento de recolección de información cualitativa; además es importante mencionar que, la metodología investigativa implementada para el desarrollo del estudio propuesto, fue la bibliográfica-documentada, esta se ejecutó a través del levantamiento de fuentes conceptuales y contextuales que abordan en tema desde un contexto teórico-científico, para lo que, se reclutó opiniones y argumentaciones documentadas de artículos científicos que respalda científicamente la estructura del presente estudio.

Por otra parte, la tecnología se ha vuelto una pieza clave para las nuevas generaciones, en especial de aquellas que están en plena formación universitaria. Autores como Roque y Juárez (2018) señalan que es importante crear conciencia en los universitarios sobre los peligros latentes que existen en la web, así como los riesgos y la importancia de salvaguardar los datos e información virtual.

Según Martelo, Tovar y Maza (2018), el acceso a la informática, es una puerta abierta que al ser utilizada de manera correcta permite innovar los conocimientos tanto en su contexto teórico y práctico, ello ha motivado que los usuario o demandantes de estos conocimientos busquen nuevas capacidades que le permitan mejorar su desempeño en seguridad informática; pero esto también ha hecho que los crackers innoven sus tácticas de vulnerabilidad de los sistemas de seguridad, a pesar de que divulgación de información física o virtual puede traerle consecuencias negativas.

Esto ha provocado que, las entidades implementen protocolos que ofrezcan protección a sus aplicaciones informáticas mediante la ejecución de técnicas y herramientas que les ayude a detectar en el tiempo oportuno espionaje informático; para los autores Hernández y Mejía (2015) en términos generales, la seguridad informática es el proceso se consiste en salvaguardar los datos que están almacenados en un entorno

físico o virtual, con el propósito de conservar su integridad, confidencialidad y disponibilidad.

1. DESARROLLO

La investigación que, se enmarca en el análisis de los riesgos informáticos del centro de cómputo de la biblioteca de la Unidad Académica de Ciencias Empresariales, toma como punto de partida en análisis de información bibliográfica contextualizada sobre la auditoría y seguridad informática, para posteriormente realizar y ejecutar un análisis sobre los riesgos que pueden existir en dicha área, tomando para ello parámetros de identificación, evaluación y verificación de los mismo, y cuyo resultados que exponen en la presente fase de investigación.

1.1. Fundamentación teórica

Para la estructuración del presente capítulo, se tomó en consideración la metodología bibliográfica-documental, la cual permite realizar una descripción de las definiciones que se consideraron necesarias para el desarrollo del trabajo, los criterios teóricos son ejecutados desde la perspectiva del autor. De Gómez, Diego, Aponte y Betancourt (2014) se cita que, la investigación basada en el metodología bibliográfica-documental, le permite al investigador obtener fácil acceso al análisis y evaluación de concepciones y fundamentos científicos que optimizan la parte conceptual y contextual del estudio. En el caso del presente proceso de indagación, se tomaron en consideración las siguientes fundamentaciones:

1.1.1 Auditoría

Es un examen minucioso, que permite identificar y evaluar los procesos, además de las actividades realizadas en una entidad, con el objetivo de corroborar que la información ingresada sea la adecuada (Alcívar, Brito y Guerrero, 2016). Es decir, permite identificar, evaluar y verificar todos aquellos riesgos existentes dentro de un área específica de trabajo.

1.1.2 Auditoría informática

Para autores como Salgado, Osuna, Sevilla y Morales (2017) la auditoría informática, es el proceso que tiene la finalidad de realizar una evaluación y detección de futuros

errores y/o fraudes por parte del usuario o software, se implementa la utilización de herramientas acordes al proceso para lograr salvaguardar la información. Los autores González, De Zayas y López (2015) menciona que, el objetivo de la auditoría financiera es ofrecer a la organización a través del auditor una compresión de los errores que se están dando con el propósito de definir y establecer estrategias correctivas.

1.1.3 Seguridad informática

Es el proceso que, fundamenta en reducir al mínimo el acceso no autorizado a la información de una organización específica, haciendo los sistemas menos vulnerables ante posibles ataques utilizando eficientemente el desarrollo continuo de las Tecnologías de la Información (Gil & Gil, 2017). Desde el punto de vista personal, la seguridad informática o ciberseguridad, es el proceso que se implementa con la finalidad de detectar y prevenir el hurto y mal uso de información, así como el de proteger datos de intenciones maliciosas.

1.1.4 Riesgo

Posibilidad de que exista un evento del cual se obtengan consecuencias no favorables, para que se produzca un riesgo primero debe existir algún tipo de amenaza y vulnerabilidad. (Azán, y otros, 2014)

1.1.5 Vulnerabilidad

Debilidades que posee el software de la organización que puede desencadenar las condiciones necesarias para propagar un ataque cibernético, comprometiendo información valiosa cuyo uso indebido genera pérdidas. (Barinas, Alarcón y Calleja, 2014). Ello, hace que los autores Hernández y Mejía (2015) manifieste que, para evitar la vulnerabilidad de ataques informáticos las organizaciones deben implementar técnicas e instrumentos que detecte posibles riesgos.

1.1.6 Amenaza

Posible intrusión al sistema aprovechando la existencia de una vulnerabilidad; solo existe amenaza cuando el sistema presenta vulnerabilidades, por ello la importancia de identificarlas para salvaguardar la integridad del sistema de información. (Espinoza, García y Llanos, 2018)

2 METODOLOGÍA DE LA AUDITORÍA INFORMÁTICA MODELO (OCTAVE)

El modelo (OCTAVE), es el método que permitió la evaluación efectiva de los riesgos existentes en el centro de cómputo de la biblioteca de la Unidad Académica de Ciencias Empresariales, para lo cual se evaluó temas organizacionales concerniente al uso de los equipos e infraestructura del área.

Para el caso de la UACE, la metodología comprendió analizar y evaluar la seguridad de la información, para esto se planificó estrategias de consultoría valiéndonos de la entrevista estructurada, la cual tuvo como objetivo identificar, evaluar y verificar los riesgos informáticos y organizacionales que presenta el área.

2.1 Objetivo de la auditoría informática

- Identificar, evaluar y verificar los riesgos informáticos que existen dentro del centro de cómputo de la biblioteca de la unidad académica de ciencias empresariales

2.2 Activos

El núcleo central de la auditoría, fue el conjunto de criterios basados en el análisis de los activos, que para este caso fueron recursos tecnológicos (sistemas Hardware, Software y Datos) y talento humano (personal que labora en el campus de la biblioteca).

2.3 Fases

La ejecución de la metodología OCTAVE, estuvo desarrollada en tres fases:

- Visión de organización: en este punto, se definió los elementos a evaluar cómo fueron los activos, la vulnerabilidad, la seguridad las amenazas y las normas o políticas.
- Visión tecnológica: para esto se tomó en consideración dos elementos claves los componentes técnicos (sistema operativo) y vulnerabilidad de los componentes estructurales de la auditoría informática.
- Planificación de las medidas y reducción de los riesgos: en este punto, se tomó en consideración la evaluación de los riesgos, así como la ponderación y reducción de riesgos.

2.4 Métodos

El método de la auditoría informática, tomó como base de evaluación la identificación de los elementos críticos y las posibles amenazas a los activos, asimismo se evaluó y

verificó la vulnerabilidad organizacional y tecnológica. Para posteriormente, exponer sugerencias de mitigación de riesgo, convirtiéndose en una prioridad para la organización o área; es importante mencionar que la auditoria informática consistió en una exploración limitada de evaluación, para lo cual se consideró:

- Evaluación de los participantes, para establecer la medición de riesgo y las directrices organizacionales de los activos.
- Crear un perfil de los activos críticos, lo cual permitió limitar los riesgos y a la vez identificar las necesidades de mejoramiento de seguridad.
- Análisis de los riesgos, con el propósito de exponer sugerencias de mitigación.

3 EJECUCIÓN DE LA AUDITORÍA

El levantamiento de información para la auditoría informática al centro de cómputo de la Unidad Académica de Ciencias Empresariales, se realizó en el rango de fecha del 15 al 23 de julio del 2019, con el objetivo de recopilar información que permita identificar, evaluar y verificar los riesgos informáticos que existen dentro del área.

La biblioteca se encuentra ubicada en la planta baja de la Facultad de Ciencias Empresariales. En la parte de infraestructura la biblioteca se considera que está en buen estado, la iluminación es deficiente por el motivo que existen bombillas en mal estado y la climatización es buena. Se realizó un acercamiento con la encarga de la biblioteca, quien supo manifestar que el departamento cuenta con 20 ordenadores de los cuales están distribuidos: 4 computadoras para el personal administrativo y 16 para alumnos.

Tabla 1. *Características de los ordenadores del centro de cómputo de la UACE*.

Hardware	
Número de ordenadores:	20
Procesador:	Intel® Core™ i7-4790 36GHz
Memoria:	6.00GB
Tipo de sistema:	Sistema operativo de 64 bits
Software	
Sistema operativo:	Windows 7 ultimate Service pack 1
Paquete ofimático:	Microsoft office professional Plus 2013
Antivirus:	ESET NOD32

Fuente: *El Autor, 2019*

3.1. Guía de auditoría del centro de cómputo de la UACE

En el proceso se realizó la delimitación de las actividades evaluadas en la auditoría, las mismas que fueron divididas en cuatro categorías y asignado un valor de calificación, adicional se desarrolló las políticas que serán queridas para ejecutar la ponderación del proceso.

Tabla 2. *Delimitación de las actividades evaluadas en la auditoría*.

ACTIVIDAD	PONDERACIÓN
1.- Mantenimiento de los ordenadores	20%
2.- Difusión de las políticas de la biblioteca	5%
3.- Software de Controles para acceso a los ordenadores	25%
4.- Evaluación y uso de las instalaciones de la biblioteca	50%

Fuente: *El Autor, 2019*

3.2. Políticas

Para la ejecución de la matriz de evaluación de actividades, se consideraron varias políticas, las cuales son sugeridas desde el punto de vista del autor con la finalidad de realizar la adecuada ponderación en cada actividad.

3.2.1. Mantenimiento de los ordenadores.

- Cada semestre se realiza el respectivo mantenimiento a todos los ordenadores, con la finalidad de que el centro de cómputo se encuentre funcionando correctamente.
- Todos los ordenadores poseen licencia de Windows, así como también del paquete Office y Antivirus.

3.2.2. Difusión de las políticas de la biblioteca.

- Las políticas de la biblioteca se encuentran ubicada al lado de la puerta de ingreso, pero lamentablemente no logra su objetivo ser visualizada por maestros y estudiantes, ya que se encuentra impresa en una hoja con letras pequeña que no logra captar atención.

3.2.3. Software controles para acceso a los ordenadores.

- A través de la entrevista realizada a la Ing. encargada del Dpto., supo manifestar que se lleva un control mediante la utilización del sistema Control Ciber. Lo que le permite tener conocimiento del tiempo que lleva cada estudiante en el ordenador, pero cabe

recalcar que este sistema no le permite recopilar información para realizar mejoras en el área.

- Los ordenadores tienen ciertas restricciones con páginas web, pero eso no impide poder acceder a redes sociales u otras páginas mediante la utilización de sitios web que permiten desbloquear estos espacios virtuales.
- La encargada de la biblioteca manifestó que desde su computador pueden observar en cualquier momento que está realizando el estudiante en el ordenador, además de enviar mensajes si esto fuera necesario, se puede argumentar que el sistema es muy básico y poco adecuado si se tiene como finalidad realizar mejoras en el área. Además, manifestó que al momento de ingresar a los ordenadores se refleja un formulario el cual deberá ser llenado por el usuario con la finalidad de llevar un control, pero sin embargo al momento de realizar este proceso, el formulario no se visualizó.

3.2.4. Evaluación y uso de las instalaciones de la biblioteca.

- El hardware del centro de cómputo se encuentra desgastado por el uso, lo cual puede ocasionar incomodidades al usuario. Cabe recalcar también que de los 20 ordenadores que posee la biblioteca solo están disponible 13.
- Las instalaciones eléctricas se encuentran funcionando, sin embargo, también se evidencio que ciertos tomacorrientes se encuentran desgastados llegando a ser inseguros.
- La iluminación con la que cuenta la biblioteca es deficiente, existen bombillas en mal estado ocasionando que el área se vea oscura.
- La biblioteca cuenta con dos aires acondicionados, los cuales se encuentran operando correctamente.
- El inmobiliario de la biblioteca se encuentra en buen estado.

A continuación, se desarrolló la ejecución de la matriz de evaluación de las actividades.

Tabla 3. *Matriz de evaluación de las actividades a auditar*.

Actividades evaluadas y ponderadas	**Ponderación por actividad**	**Calificación de ponderación**
1. Mantenimiento de los ordenadores	**20%**	**20%**
Mantenimientos preventivos	10%	10%
Actualizaciones de software	10%	10%

2. Difusión de las políticas de la biblioteca	**5%**	**2%**
Socialización de las políticas para la utilización de los ordenadores o solicitar libros	5%	2%
3. Software de Controles para acceso a los ordenadores	**25%**	**14%**
Evaluación del sistema Control Ciber	10%	5%
Restricción a ciertas páginas web	10%	6%
Monitoreo del uso del ordenador por parte de la encargada del dpto.	5%	3%
4. Evaluación y uso de las instalaciones de la biblioteca	**50%**	**40%**
Operatividad del hardware	10%	6,5%
Funcionalidad de las instalaciones eléctricas	10%	8%
Funcionalidad de la iluminación	10%	5%
Funcionalidad del sistema de climatización	10%	10%
Inmobiliario	10%	10%
Total, factor a ponderar	**100%**	**76%**

Fuente: *El Autor, 2019*

Como se aprecia en la tabla 2, se realizó la evaluación de las actividades, en ella se puede determinar e indicar que dentro de cada actividad se está evaluando puntos específicos de hardware, software y humano, se consideró las políticas propuestas por el autor para realizar la ponderación de cada parámetro indicado. Cabe mencionar que, posterior a la evaluación realizada en el centro de cómputo de la biblioteca de la UACE, obtuvo una calificación de 76/100.

Tabla 4. Calificación.

Bueno	70-100
Regular	55-69
Malo	1-54

Fuente: *El Autor, 2019*

Se puede visualizar el rango de las calificaciones por cada variable. Dentro de los parámetros que se reflejan en la tabla 4, se estableció que la calificación es buena.

3.2.5 Matriz de riesgo del centro de cómputo de la biblioteca de la UACE

Para el caso de la evolución de matriz de riesgo del centro de cómputo de la biblioteca de la UACE, se hizo uso de la entrevista. El autor Pulido (2015) define a la entrevista,

como la herramienta o instrumento asimétrico que, permite la recolección de información cualitativa a través de preguntas y respuesta.

Para el caso de la investigación, esta permitió evaluar parámetros de riesgo del centro de cómputo de la biblioteca de la UACE, mismo que se encuentran expuestos a continuación:

Tabla 5. *Criterios de evaluación del impacto y probabilidad.*

PROBABILIDAD	
4	Alto (A)
3	Medio Alto (MA)
2	Medio Bajo (MB)
1	Bajo (B)

IMPACTO	
1	Insignificante (I)
2	Manejable (M)
3	Requiere Atención (RA)
4	Crítico (C)

Fuente: *El Autor, 2019*

Se puede observar que los niveles utilizados para la evaluación de las actividades a auditar en la matriz de riesgos, teniendo presente los enunciados indicados en el punto 3.2 Políticas, los cuales serán necesarios para ejecutar la evaluación.

Tabla 6. *Matriz de identificación de riesgos.*

	Actividades evaluadas	Probabilidad				Impacto				Puntaje	Nivel de riesgo
		B	MB	MA	A	I	M	RA	C		
A	**Mantenimiento de los ordenadores**										
A1	Mantenimientos preventivos	1				1				**1**	Bajo
A2	Actualizaciones de software	1				1				**1**	Bajo
B	**Difusión de las políticas de la biblioteca**										
B3	Socialización de las políticas para la utilización de los ordenadores o solicitar libros		1					3		**3**	Medio
C	**Software de Controles para acceso a los ordenadores**										
C4	Evaluación del sistema Control Ciber				4			3		**12**	Alto
C5	Restricción a ciertas páginas web		2					3		**6**	Medio

C6	Monitoreo del uso del ordenador por parte de la encargada del dpto.			3		3	**9**	Alto
D	**Evaluación y uso de las instalaciones de la biblioteca**							
D7	Operatividad del hardware			3		3	**9**	Alto
D8	Funcionalidad de las instalaciones eléctricas		2		2		**4**	Medio
D9	Funcionalidad de la iluminación		2			3	**6**	Medio
D10	Funcionalidad del sistema de climatización	1			2		**2**	Bajo
D11	Inmobiliario	1		1			**1**	Bajo

Fuente: *El Autor, 2019*

Los procesos evaluados son específicos de la Biblioteca de la UACE, los cuales fueron sometidos a una matriz de riesgo, cabe recalcar que cada actividad tiene un código asignado. La calificación y el nivel de riesgo que obtuvo cada ítem es criterio de autor, partiendo de la entrevista realizada al personal encargado y de los elementos que se pudo observar en la visita preliminar que se realizó. Siendo la *Actividad A* la que obtuvo un nivel de *Riesgo Bajo* mientras que la *Actividad C* obtuvo el nivel de *Riesgo Alto*.

Tabla 7. *Ponderación del nivel de riesgo.*

RIESGO	VALORES
Alto	7 - 16
Medio	3 – 6
Bajo	1 -2

Fuente: *El Autor, 2019*

Se propone la ponderación de los tres niveles de riesgo que se evaluaron en la matriz.

Tabla 8. *Evaluación del nivel de riesgo.*

PROBABILIDAD					
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	**2**	**3**	**4**
			IMPACTO		

Fuente: *El Autor, 2019*

Riesgo = Probabilidad x Impacto

Se puede observar que la tabla utilizada para la matriz de riesgo fue de 4x4, donde se tomó en cuenta las escalas de la probabilidad por impacto que se indico en la tabla 5.

Tabla 9. *Evaluación de la matriz de riesgos.*

PROBABILIDAD					
	4			C4	
	3			C6 - D7	
	2		D8	C5 - D9	
	1	A1 -A2 - D11	D10	B3	
		1	**2**	**3**	**4**
			IMPACTO		

Fuente: *El Autor, 2019*

Se puede observar que los riesgos de color verde *(A1, A2, D11, D10)* son aceptables, con lo que se puede indicar que dentro de estas actividades no se tiene mayor problema. Mientras que los riesgos de color amarillo *(D8, B3, C5, D9)* tiene un mayor impacto en el área de la biblioteca, donde se puede desencadenar posibles vulnerabilidades, y por último el valor rojo *(C6, D7, C4)* son las actividades donde se corre mayores riesgos.

CONCLUSIONES

- El riesgo analizado desde la perspectiva informática, se puede indicar que son aceptables las actividades evaluadas, con menor impacto fueron las actualizaciones de software y mantenimiento preventivos, donde se manifestó que cada semestre se realiza los respectivos mantenimientos de los ordenadores con la finalidad de mantenerlos en condiciones favores para los alumnos.
- Se pudo evidenciar que la biblioteca carece de una adecuada visualización de las políticas existentes en el área, por tal motivo es un tema que requiere mayor atención

siendo su nivel de riesgo medio, es por ello que si no se socializa las políticas con los alumnos y docentes estas serán desconocidas, lo cual puede ocasionar problema.

- En el tema del software que se aplica para el control del centro de cómputo, se puede indicar que es crítico, ya que es un programa básico el cual solo permite tener control de quien desea un computador, pero no accede crear una base de datos en el cual indique a qué páginas ingresan los alumnos, o que computador es el más utilizado, con que frecuencias solicitan los alumnos un computador, que carreras visitan más la biblioteca, es decir no existe un respaldo y control de actividades.
- En la parte de infraestructura, esta se encuentra en buenas condiciones y cumple con las necesidades básicas de los alumnos, en temas de iluminación, esta necesita atención, ya que se encuentran bombillas en mal estado lo cual dificulta realizar ciertas actividades de estudio de forma adecuada. Se cuentan con dos aires nuevos lo que hace que la climatización sea óptima, para finalizar se debe acotar que las instalaciones eléctricas y el hardware necesita atención, ya que son elementos que el tiempo influye en su depreciación.

BIBLIOGRAFÍA

Alcívar, F. M., Brito, M. P., & Guerrero, M. J. (Julio-Septiembre de 2016). Auditoría en las empresas. *CE Contribuciones a la Economía*. Recuperado el 20 de Julio de 2019, de http://eumed.net/ce/2016/3/auditoria.html

Arcentales , D. A., & Caycedo, X. (22 de Agosto de 2017). Auditoría informática: un enfoque efectivo. *Revista Científica Dominio de las ciencias, 3*, 157-173. Recuperado el 28 de Julio de 2019, de https://dialnet.unirioja.es/servlet/articulo?codigo=6102836

Azán, Y., Bravo, L., Rosales, W., Trujillo , D., García, A., & Pimentel , A. (20 de Febrero de 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. Recuperado el 20 de Julio de 2019, de http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2227-18992014000200004&lng=es&nrm=iso

Barinas, A., Alarcón, A. C., & Calleja, M. (ene-jun de 2014). Vulnerabilidad de ambientes virtuales de aprendizaje utilizando SQLMap, RIPS, W3AF y Nessus*1. *Ventana Informática*(30), 247-260. Recuperado el 18 de Julio de 2019, de http://revistasum.umanizales.edu.co/ojs/index.php/ventanainformatica/article/view/276/419

Espinoza, F., García , J., & Llanos, D. (19 de Marzo de 2018). Aplicación de una metodología de seguridad avanzada en redes inalámbricas. *risti: Revista Ibérica de Sistemas e Tecnologias de Informacao*(15), 24-38. Obtenido de http://www.risti.xyz/issues/ristie15.pdf

Gil, V. D., & Gil, J. C. (Junio de 2017). Seguridad informática organizacional: un modelo de simulación basada en dinámica de sistemas. *Scientia Et Technica, 22*(2), 193-197. Recuperado el Julio de 2019, de http://www.redalyc.org/articulo.oa?id=84953103011

Gómez, E., Diego, F., Aponte, G., & Betancourt, L. (2014). Metodología para la revisión bibliográfica y la gestión de información de temas científicos, a través de su estructuración y sistematización. *Dyna*, 158-163.

González, M., De Zayas , M., & López, J. (2015). Auditoría de información y auditoría de conocimiento: acercamiento a su visualización como dominios científicos. *Revista Cubana de Información en Ciencias de la Salud*, 34-52.

Hernández, A. L., & Mejía, J. (Febrero de 2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *ReCIBE. Revista Electrónica de Computación, Informática Biomédica y Electrónica*(1). Recuperado el 29 de Julio de 2019, de http://www.redalyc.org/articulo.oa?id=512251501005

Hernández, A., & Mejía, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *ReCIBE. Revista electrónica de Computación, Informática Biomédica y Electrónica*, 1-18.

Martelo, R. J., Tovar, L. C., & Maza, D. A. (Febrero de 2018). Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. *Información Tecnológica, 29*(1), 3-10. doi:10.4067/S0718-07642018000100003

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

Roque, R. V., & Juárez, C. M. (Marzo-Agosto de 2018). Concientización y capacitación para incrementar la seguridad informática en estudios universitarios. *Paakat: Revista de tecnología y sociedad, 8*(14). doi:10.18381/Pk.a8n14.318

Salgado, M. d., Osuna, N. d., Sevilla, M., & Morales, J. I. (Julio-Diciembre de 2017). La Auditoría Informática en las organizaciones. *Revista Electrónica sobre Cuerpos Académicos y Grupos de Investigación en Iberoamérica, 4*(8). Recuperado el 18 de Julio de 2019, de http://www.cagi.org.mx/index.php/CAGI/article/view/165/324