UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE COMPUTO DE LA BIBLIOTECA DE LA UACE-UTMACH.

CARRILLO GUILLEN KATHERINE STEFANY
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE COMPUTO DE LA BIBLIOTECA DE LA UACE-UTMACH.

CARRILLO GUILLEN KATHERINE STEFANY
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE COMPUTO DE LA BIBLIOTECA DE LA UACE-UTMACH.

CARRILLO GUILLEN KATHERINE STEFANY
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

ORDÓÑEZ BRICEÑO KARLA FERNANDA

MACHALA, 09 DE JULIO DE 2018

MACHALA
09 de julio de 2018

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE COMPUTO DE LA BIBLIOTECA DE LA UACE-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.

ORDONEZ BRICEÑO KARLA FERNANDA
0705031003
TUTOR - ESPECIALISTA 1

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

PARRA OCHOA EUDORO BENITO
0701063406
ESPECIALISTA 3

Fecha de impresión: martes 25 de septiembre de 2018 - 10:50

URKUND

Urkund Analysis Result

Analysed Document:	CARRILLO GUILLEN KATHERINE STEFANY_PT-010518.pdf (D40253727)
Submitted:	6/19/2018 3:13:00 AM
Submitted By:	kcarrillo_est@utmachala.edu.ec
Significance:	1 %

Sources included in the report:

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000100013

Instances where selected sources appear:

1

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

La que suscribe, CARRILLO GUILLEN KATHERINE STEFANY, en calidad de autora del siguiente trabajo escrito titulado EVALUACIÓN DEL RIESGO INFORMÁTICO EN EL CENTRO DE COMPUTO DE LA BIBLIOTECA DE LA UACE-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.

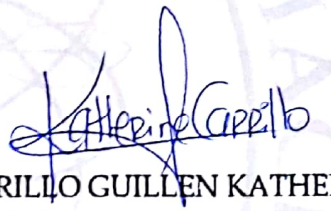
La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

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, 09 de julio de 2018



CARRILLO GUILLEN KATHERINE STEFANY
0705303907

RESUMEN

La documentación presente realiza una evaluación del riesgo informático en la biblioteca de la Unidad Académica de Ciencias Empresariales de la UTMACH desde el enfoque de la auditoria informática, pretende medir el estado de la problemática por medio de la observación y análisis empleando una matriz de evaluación; se ejecuta una interpretación de la temática a nivel macro, meso y micro basándose en recopilación de competencias teóricas a través de artículos científicos que sumados a la indagación de campo facultan la compresión del riesgo informático (físico y lógico) que se encuentra el centro de cómputo estudiado, para identificar las vulnerabilidades, fortalezas, debilidades siendo analizadas desde el punto de vista objetivo acorde a las exigencias tanto locales como nacionales en contraste con estandarizaciones internaciones o políticas reglamentadas; con la finalidad de proponer los controles de seguridad necesarios al garantizar la integridad de los activos informáticos.

Palabras Clave: Evaluación, riesgo, autoría, controles, informática.

ABSTRACT

The present documentation carries out an evaluation of the computer science risk in the library of the Academic Unit of Business Sciences of the UTMACH from the approach of the computer audit, aims to measure the state of the problem by means of observation and analysis using an evaluation matrix; an interpretation of the subject is carried out at the macro, meso and micro level, based on the compilation of theoretical competences through scientific articles that, added to the investigation of the field, enable the compression of the computer (physical and logical) risk found in the computing center studied, to identify vulnerabilities, strengths, weaknesses being analyzed from the objective point of view according to local and national requirements in contrast to international standardizations or regulated policies; with the purpose of proposing the necessary security controls to guarantee the integrity of the computer assets.

Keywords: Evaluation, risk, authorship, controls, computing.

ÍNDICE DE CONTENIDOS

RESUMEN II
ABSTRACT III
ÍNDICE DE ILUSTRACIONES V
ÍNDICE DE CUADROS V
1. INTRODUCCIÓN 6
2. FUNDAMENTACIÓN TEÓRICA 7
2.1 Servicios y tipos de Auditoria Informática 7
2.2 Riesgo Informático 7
2.3 Seguridad Informática 8
2.4 Estándar ISO 27002 9
2.5 Proceso de evaluación de riesgos 10
3. METODOLOGÍA 10
4.1 Estudio preliminar centro de computo 11
4.1.1 Problemas latentes 13
4.1.2 Objetivos Especificas de la Auditoría 14
4.1.3 Inventario de computadoras 14
4.2 Que se va a evaluar (seguridad física y lógica) 15
4.3 Guía de Evaluación 16
4.4 Matriz de riesgo 16
4.5 Fotos 17
4.5 Matriz FODA 18
4.7 Resultados 19
5. CONCLUSIONES Y RECOMENDACIONES 20
6. REFERENCIAS BIBLIOGRÁFICAS 22

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Elementos cruciales en la seguridad informática 8
Ilustración 2. Diseño para la gestión de calidad en auditoria informática 9
Ilustración 3. Evaluación de riesgos 10
Ilustración 4. Estado de las instalaciones de datos 12
Ilustración 5. Control de ordenadores estudiantes en biblioteca de UACE 12
Ilustración 6. Regulador de energía del ordenador principal (UPS) 17
Ilustración 7. Ordenadores encargados (derecha) y estudiantes (izquierda) 18

ÍNDICE DE CUADROS

Cuadro 1. Especificaciones de las computadoras del centro de computo de biblioteca UACE 13
Cuadro 2. Inventario computadoras Biblioteca UACE 14
Cuadro 3. Matriz de Evaluación de seguridades 15
Cuadro 4. Guía de Evaluación 16
Cuadro 5. Matriz de riesgo relación causa-efecto 16
Cuadro 6. Matriz F.O.D.A (Fortalezas, oportunidades, debilidades y amenazas) 18
Cuadro 7. Matriz de resultados detallando relación causa-efecto 20

1. INTRODUCCIÓN

La vida cotidiana atraviesa un proceso de transformación en el cual toda las esferas sociales del hombre son gestionadas directa o indirectamente por las TIC´s, a tal punto que la sociedad basa sus funcionalidades en la recopilación, transmisión y almacenamiento de grandes cantidades de información a través de quipos informáticos; propiciando la necesidad de mantener una planificación de protección, mantenimiento, operación y evaluación tanto del punto de vista técnico como legal mediante la aplicación de políticas locales o estándares internacionales de calidad en cuanto a sistemas computacionales. (González., 2007)

En el marco académico las nuevas tecnologías integran percepciones pseudo practicas gracias al uso de ordenadores como fuente de consulta, simulación e inclusive como ayudante personas más que como una herramienta educativa; la auditoria informática es la conjunto de saberes orientados a valorar las medidas de seguridad en sus sistemas, su incidencia a nivel institucional, personal e interdepartamental para evaluar si los activos informáticos salvaguardan la integridad de los datos componen el entorno empresarial. (Santiso, Koller, & Bisaro, 2016)

Desde el punto de vista macro hoy en día se postula una nueva visión de desarrollo empresarial derivada de la gestión del conocimiento como enfoque para sintonizar el recursos humano e informático en una introspección tecnológica que asista los procesos gerenciales en el cumplimiento de objetivos estratégicos para convertirse en una entidad de avanzada, esto linealiza la relevancia de los sistemas informáticos que ya no son vistos como meros complementos sino como un pilar de potencialidades intrínsecamente correlacionadas a las capacidades cognitivas e intuitivas de los dirigentes institucionales. (Baryolo, Sentí, Camejo, & Rodríguez, 2012)

El objetivo del presente estudio es identificar las vulnerabilidades (físicas y lógicas) latentes en el centro de computo de la Unidad Académica de Ciencias Empresariales y proponer las medidas de seguridad a implementar para garantizar la seguridad de los activos informáticos. Es necesario efectuar conjugar las perspectivas teórica-prácticas mediante una matriz de evaluación que relaciona los puntos a analizar, sus indicadores (procesos de seguridad física y lógica), que herramientas se usan, su accionar personal en quienes facultan los ordenadores para determinar fortalezas, debilidades y connatos de la infraestructura informática con la finalidad de proponer controles que solucionen dichos percances. (PADILLA, CAÑAR, CEDILLO, MARQUEZ, & CUEVA, 2017)

2. FUNDAMENTACIÓN TEÓRICA

Los conceptos que inciden que sustentan los criterios aplicados afines a los saberes de administración de empresas y riesgo informático son:

2.1 Servicios y tipos de Auditoria Informática

Seguridad interna: Se compara en base a normativas el nivel de seguridad de las redes locales y corporativas internas.

Seguridad perimetral: Se indaga acerca de los márgenes la red local o corporativa en función de su conexión con redes públicas.

Test de intrusión: Se mide la resistencia a la intrusión intentando acceder al sistema empleando diversos niveles de acoso.

Análisis forense: Se ejecuta de luego de los incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados, en el caso de presentarse la inoperatividad del sistema, se denomina análisis post mórtem.

Código de aplicaciones: Analiza el código sin importar el lenguaje, un ejemplo concreto y frecuente se realiza con los sitios web, mediante el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, Cross Site Scripting (XSS), etc.

Los principales tipos de auditoria son:

Explotación: Consiste en procesar la materia prima (Datos) para convertirlos en procesos de seguridad mediante controles de seguridad.

Sistemas: Radica en analizar los componentes de las redes internas y externas, líneas o instalaciones informáticas en general.

Comunicaciones: Le compete auditar los sistemas de intercomunicaciones y conexionado en la arquitectura informática.

Proyectos: Conlleva un análisis de todos los componentes de la elaboración de un proyecto desde identificar la línea base hasta el lenguaje de programación.

Seguridad: Se refiere a todos los enfoques relacionados a la seguridad física y lógica que protege la integridad de los activos informáticos. (GUSTAVO, 2017)

2.2 Riesgo Informático

Es una gama de procesos que buscan garantizar la confiabilidad de un sistema informático en función de las vulnerabilidades, debilidades y amenazas del sistema analizadas respecto

a la probabilidad de ocurrencia e impacto de las mismas sobre los activos del mismo. (Maya, 2013)

Vulnerabilidades: Son todas las condiciones que permiten materializarse a una amenaza como hackers, suplantar de identidad, fallos en programación, software malicioso, errores humanos o factores latentes que podrían causar incidentes.

Amenazas: Es el resultado de la existencia de una vulnerabilidad y riesgos latentes en los procesos informáticos ya sea de índole personal, física, lógica, errores e inclusive desastres naturales que podrían dañar los activos.

Debilidades: Es la falta de fortaleza en un determinado aspecto, se catalogan de acuerdo a la gravedad que presenta para el sistema, un ejemplo es la falta de presupuesto, desconocimiento de leyes o tipología de ataques o la mala distribución del personal, también la existencia de vulnerabilidades en la configuración u operación del sistema.

2.3 Seguridad Informática

Es el conjunto de estudios que garantizan que la totalidad de los recursos informáticos sean usados como se decidió y de manera adecuada en base a la ley, que la modificación, almacenamiento, aporte, borrado e integración de datos sea realizada estrictamente por las personas autorizadas para dichos fines. La ilustración 1 esquematiza la definición planteada.

Ilustración 1. Elementos cruciales en la seguridad informática

Fuente: Elaboración Propia

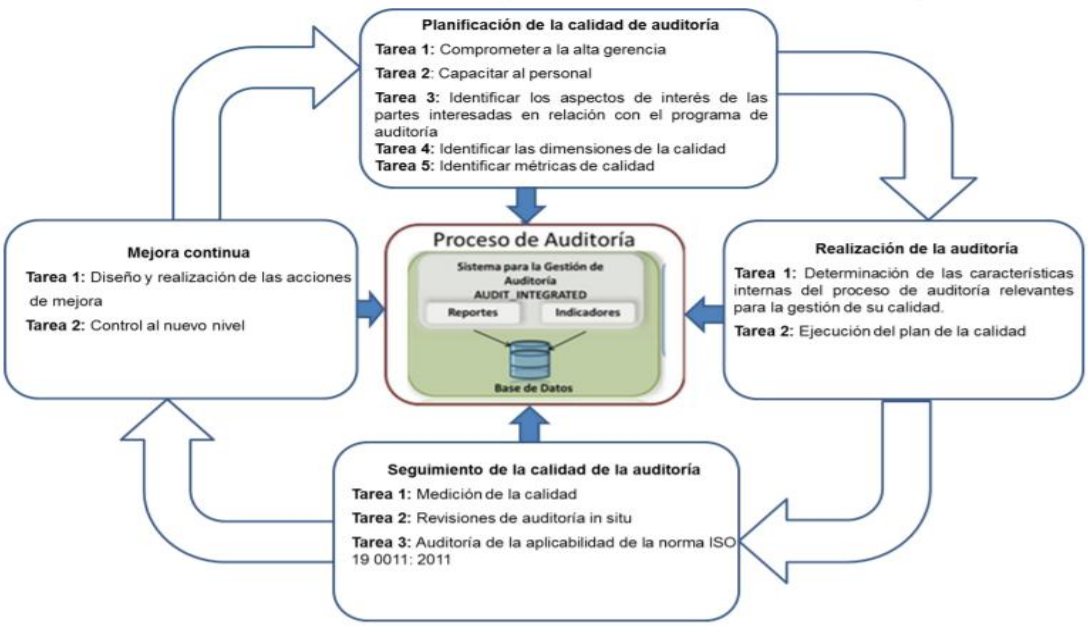
Controles Físicos: Son las medidas de seguridad aplicadas a los recursos físicos tanto personal como identificaciones (contraseñas, distintivos) o restricciones temporales como a los equipos resguardo y vigilancia. (GUSTAVO, 2017)

Controles Lógicos: Son los medios de seguridad aplicados a los datos impidiendo su libre acceso a personal no autorizado o barreras que resguarden su uso.

Gestión de activos: Es la planificación de controles (inventarios, propiedad, devolución), actividades estructuras al uso y manejo de recursos (hardware-software) de manera eficiente en los procedimientos institucionales. (Melo, 2008)

El riesgo informático en las instituciones formula una política de gestión de calidad centrada en los procesos de auditoria que derivan en una mejora continua de los pasivos-activos que resguardan la información, dicho esquema se detalla en la imagen 1.

Ilustración 2. Diseño para la gestión de calidad en auditoria informática



Fuente: (Dalilis, Rosario, & Luis, 2016)

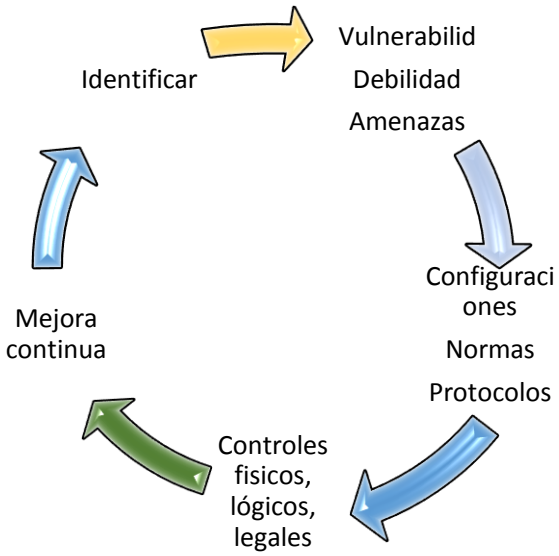
2.4 Estándar ISO 27002

La norma ISO 27002:2013 establece un conjunto de actividades y directrices bien definidas para la implementación de la seguridad informática, a fin de proteger los activos informáticos, generando confianza tanto al cliente interno como al cliente externo, de esta manera se empieza a implementar los procesos de seguimiento en cada una de las áreas, estableciendo e identificando cada uno de los potenciales riesgos que se pueden presentar en la empresa. (ISO, 2013)

2.5 Proceso de evaluación de riesgos

Son un conglomerado complejo de gestiones que planifican la estructuración de una estrategia completa de seguridad contrastando las potencialidades y falencias de un sistema informático; en la *ilustración 3* se observa dicho proceso.

Ilustración 3. Evaluación de riesgos



Fuente: Elaboración propia

3. METODOLOGÍA

Los métodos empleados en la obtención y tratamiento de la información son los siguientes:

Investigación Documentada: Es necesario recopilar postulaciones conceptuales en ponencias a nivel macro en bases de datos indexadas para realizar la argumentación teórica del proyecto.

Método Descriptivo-Observacional: Se requiere efectuar una investigación de campo al concatenar los criterios teórico-prácticos desde el punto de vista epistemológico, por tal motivo se recurre a la matriz de evaluación como instrumento de medida y a las observaciones realizadas en el centro de computo estudiado que en conjunto permiten describir e interpretar los resultados que solucionan a la problemática planteada.

Análisis Deductivo: El desarrollo de la temática se induce progresivamente al inferir el estado del centro de cómputo a partir de la autoría informática partiendo desde las apreciaciones generales al caso particular de la biblioteca de UACE determinando los controles de seguridad a proponer.

4. DESARROLLO

La evaluación del riesgo informático es un proceso interpretativo donde se debe involucrar todo el personal, realizar toda una variedad de gestiones, aplicaciones tecnológicas, tomar medidas físicas-lógicas e integrar configuraciones o técnicas especiales de programación al elaborar un plan estratégico de seguridad en el cual todos los actuantes colaboran en su manejo (activos-sistemas informáticos) y socialización a la vez que se retroalimenta de forma continua, bajo los lineamiento de planificar, hacer, verificar y actuar. (Solarte, Rosero, & Ruano, 2015)

La auditoría informática comprende una serie de etapas sistematizadas desde el diagnostico, evaluación, análisis y estudio del entorno informático (hardware, redes, bases de datos, instalaciones, softwares,…) sobre estándares internacionales derogados como modelo de referencia en este caso ISO 27001, desde la perspectiva institucional constituye un proceso empresarial en el cual se mide el nivel de funcionalidad de los sistemas informáticos en base a una evaluación que identifica fortalezas y debilidades para proponer una configuración adecuada a las necesidades de protección examinando los controles que conlleven un mejor desempeño/rendimiento en los sistemas al mismo tiempo que asisten en la toma de decisiones gerenciales haciendo de soporte en el crecimiento externo e interno de la entidad capitalista. (MOJICA & LISBOA, 2011)

4.1 Estudio preliminar centro de computo

Se realiza una visita previa donde se constata el estado de las computadoras, como se encuentran las conexiones, disposiciones de puertos de red, tomacorrientes, la información sobre funcionamiento u observaciones se obtienen mediante una entrevista con los encargados; quienes destacan los siguientes puntos:

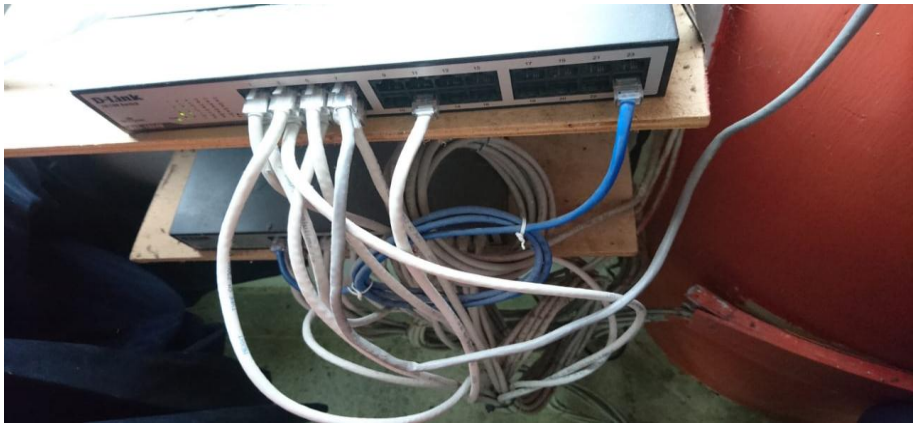
Ordenadores: Son un total de 18 máquinas, las cuales cuentan con acceso a internet, Windows 10, programas básicos, 16 son de uso para estudiantes y 2 ordenadores host que regulan a los demás son de uso para los encargados.

Normas: Dentro de biblioteca se aplican normativas de control, no hacer ruido, dedicarse exclusivamente a actividades académicas, no instalar programas ni descargar aplicaciones de redes sociales.

Estado de instalaciones: Las conexiones a tomacorrientes de las máquinas son empotradas mientras que las debajo de las mesas son sobrepuestas por medio de canaletas que permiten conectar laptops a los usuarios de la biblioteca; en cuento a redes se transmite datos por cable UPT blindado protegido con canaletas plásticas, no obstante, debido a los

años se observa un deterioro regular en las instalaciones, en la *ilustración 4* se denota las conexiones de datos en la biblioteca de UACE.

Ilustración 4. Estado de las instalaciones de datos



Fuente: Autor

Aplicación de Controles: Se implementan una serie de políticas y regulaciones, tanto a estudiantes como a los computadores, está restringida acceso a páginas web pornográficas, redes sociales, sitios no seguros, los ordenadores cuentan con Frizzin que congela el estado de la máquina no permite ni modificar ni agregar información, no se debe ingresar comidas ni bebidas, además de ser registrados todos los usuarios llevando un control de quienes la usan en un tiempo estandarizado de 1 hora por estudiante. La navegación/tiempo de uso de los ordenadores se gestiona mediante un software de control de *ciber*, como se aprecia en la *ilustración 5.*

Ilustración 5. Control de ordenadores estudiantes en biblioteca de UACE

Control de Ciber 1.585

Opciones Impresiones Cajero Socios Cupones Ultimos Venta Directa Ayuda

Ord.	Inicio	Contador	Estado	Dto.	Parar a:	Extras	Nota	Mensaje	CD	PRI
1	03:06:12 pm	1:57:30	Contando							1
2	04:29:46 pm	0:33:56	Contando							2
3	04:30:33 pm	0:33:9	Contando							3
4	03:22:50 pm	1:40:52	Contando							4
5	03:23:03 pm	1:38:28	Sin usar							5
6	04:57:57 pm	0:5:45	Contando							6
7	03:36:31 pm	1:27:11	Contando							7
8			Sin usar							8
9			Sin usar							9
10	04:28:38 pm	0:35:4	Contando							10
11	04:52:13 pm	0:11:29	Contando							11
12			Sin usar							12
13	04:47:37 pm	0:16:5	Contando							13
14	04:43:58 pm	0:19:44	Contando							14
15			Sin usar							15
16			Sin usar							16
17			Sin usar							17
18			Sin usar							18
19			Sin usar							19
20			Sin usar							20

Fuente: (Cunalata, 2018)

4.1.1 Problemas latentes

La biblioteca de la UACE se sitúa en la parte baja del edificio principal frente al patio de comidas, esto la hace susceptible a eventos de inundación; cuenta con un área de aproximadamente 200m2 con interconexión de ordenadores, acceso a internet, horario de atención de 9 a 12 am y 15 a 20 pm; se observa que el sistema operativo es Windows aunque sin licencia, además de estar desactualizado, no se cuenta con un plan de acción en tanto a seguridad informática ni se lleva un registro de mantenimiento u operación del sistema. Las reglas de comportamiento y uso de ordenadores se socializan con las autoridades-estudiantes para emplear adecuadamente los recursos informáticos tanto digitales como físicos; en el *cuadro 1* se observa el levantamiento de las máquinas del centro de compto estudiado.

Cuadro 1. Especificaciones de las computadoras del centro de computo de biblioteca UACE

HARDWARE	
Número de ordenadores	18 todos operan correctamente
CPU	Intel Core I3 de 2.93 Ghz Memoria ram 2 Gb Disco duro 320 Gb
Periféricos de entrada	Teclado QBEX Mouse QBEX Puerts USB Puerto VGA
Periféricos de salida	Monitor Resolución 800 x 600
Conexionado	Cable PS/2 y cable mini din (Teclado y Mouse) Cable serial (Modem externo- Escáner) Cable monitor. Cable par trenzado (Conexión a una red) Cable HDMI (Monitor, Pantalla, y Proyector) Cable Energía eléctrica
SOFTWARE	
Sistema Operativo	Windows 10
Paquete Ofimático	*Paquete Office:* Microsoft Word (Procesador de texto) Microsoft Excel (Planilla de cálculo/hoja de cálculo) Microsoft PowerPoint (Programa de presentaciones de diapositivas) Microsoft Access (Programa de bases de datos) Microsoft Publisher (Editor para crear varios tipos de publicaciones como tarjetas, pancartas, etc.) Microsoft Project (Gestor de proyectos) Microsoft Outlook (Agenda y cliente de correo electrónico y cuentas software)
Otros Programas	Google Crome

	Adobe Reader X 10.0.0 (2010) Adobe Flash Player 9.0.283.0 A (2010) Antivirus Norton Internet Security Nero 7 Ultra Edition Windows Internet Explorer 7 Skype VLC Media Player

Fuente: (Cunalata, 2018)

Las características físicas y lógicas de los ordenadores expresan un riesgo derivado de la desactualización de sistema operativo, falta de un licencia corporativa, poca capacidad de respuesta en la máquina acosada debido a sus bajas prestaciones.

4.1.2 Objetivos Especificas de la Auditoría

- Verificar la seguridad de los recursos informáticos, estado de quipos periféricos e instalaciones en relación al cumplimiento de las metas institucionales
- Evaluar la seguridad del acceso a usuarios tanto internos como externos, así como el manejo del centro de cómputo de biblioteca
- Examinar el perfil profesional del responsable de biblioteca de UACE para confirmar sus competencias en el manejo de los activos informáticos
- Comprobar la seguridad de los recursos informáticos, así como sus equipos periféricos e instalaciones para que se verifique sobre el cumplimiento con los objetivos institucionales.
- Identificar el grado de acatamiento de políticas, planes y procesos institucionales en virtud de la protección de datos mediante buen uso de recursos tecnológicos
- Elaborar una evaluación del plan de mantenimiento mediante un análisis critico para proponer los controles físicos y lógicos en el adecuamiento de la seguridad del centro de cómputo de UACE

4.1.3 Inventario de computadoras

En el centro de computo se lleva un registro de las características principales de los ordenadores, dando un total de 18 máquinas, cuya descripción se aprecia en el *cuadro 2.*

Cuadro 2. Inventario computadoras Biblioteca UACE

CANTIDAD	DESCRIPCIÓN	MARCA	MODELO
1	COMPUTADORA DE ESCRITORIO PROCESADOR INTEL CORE I3 DE 2,93GHZ, MEMORIA RAM 2GB, DISCO DURO 320GB, TECLADO, MOUSE, MONITOR QBEX	QBEX	HW191APB
1	COMPUTADORA DE ESCRITORIO PROCESADOR INTEL CORE I3 DE 2,93GHZ, MEMORIA RAM 2GB, DISCO DURO 320GB, TECLADO, MOUSE, MONITOR QBEX	QBEX	HW191APB
1	COMPUTADORA DE ESCRITORIO PROCESADOR INTEL CORE I3 DE 2,93GHZ, MEMORIA RAM 2GB, DISCO DURO 320GB, TECLADO, MOUSE, MONITOR QBEX	QBEX	HW191APB

1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G
1	COMPUTADOR DE ESCRITORIO	ACER	VERITON M4630G

Fuente: (Cunalata, 2018)

Esto indica que los recursos informáticos necesitan ser actualizados, debido a que sus características se están quedando cortas en relación a las exigencias de los estudiantes y potencia que demandan los softwares actuales.

4.2 Que se va a evaluar (seguridad física y lógica)

Los niveles de seguridad se pueden medir en base a indicadores físicos y lógicos que identifican las falencias en el centro de computo analizado, tales criterios se resumen en el *cuadro 3.*

Cuadro 3. Matriz de Evaluación de seguridades

Seguridad Física	Seguridad Lógica	Personal
Registro de usuarios	Antivirus	Encargado de biblioteca
Identificación del personal	Configuraciones cliente-servidor	
Control biométrico de jornada laboral	Host con IP privadas hacían red externa	
Claves y códigos de acceso a privilegios	Control de ciber, restricción de accesos a web dañinas	Dirección de TIC´s

Fuente: Elaboración Propia

Se aprecia que existe un nivel bueno de seguridad desde el punto de vista físico y regular en referencia a la seguridad lógica, también se evidencia la falta de personal especializado que realice gestiones de seguridad informática (ingeniero en sistemas).

4.3 Guía de Evaluación

Se evalúa la medida en que se procede a llevar la seguridad en el centro de computo en función de lo que se posee y que se hace para resguardar los activos informáticos, esto se aprecia mediante el *cuadro 4.*

Cuadro 4. Guía de Evaluación

Puntos a evaluar	**Procedimiento**	**Estado**
Operaciones físicas y lógicas	Aplicación de controles físicos a personal	Bueno, distintivos y controles biométricos
Actividades académicas	Reguladas por encargado	Muy bueno, se registra y supervisa toda actividad
Mantenimiento de ordenadores	Limpieza, mantenimiento preventivo, predictivo	Bueno, se realiza monitoreo constante de los equipos
Documentación de políticas/reglamentaciones	Regulación de actividades internas, medida de aplicación	Regular, no existen políticas especializadas entorno al riesgo
Infraestructura Informática	Estado de equipo informático	Bueno, a pesar de la desactualización de equipos, estos operan correctamente
Instalaciones eléctricas-datos	Mantenimiento y mejora de instalaciones	Regular, se observa vetustez en el cableado
Defensa contra ataques externos	Aplicar protocolos de control, Firewall, IP	Regular, no se ha detectado intrusiones al sistema, pero se carece de plan de acción o medidas de respuesta

Fuente: Elaboración propia

4.4 Matriz de riesgo

Se identifica los riesgos en base a las vulnerabilidades-debilidades apreciadas en el centro de computo de biblioteca, dicho proceso de observa a través del *cuadro 5.*

Cuadro 5. Matriz de riesgo relación causa-efecto

Descripción del riesgo	**Responsables de la aparición del riesgo**
Pérdida o daño de información	Virus, código malicioso o malware

Suplantar identidad de estudiantes/docentes	Hackers
Daño del equipo informático	Mal uso de los estudiantes, falta de mantenimiento, desastres naturales
Acceso remoto a la red	Hackeo, atentados corporativos
Pérdida de información institucional	Falta de sistema de respaldo general
Fallos o errores en la configuración de plataforma/programación de la red	Falta de personal capacitado

Fuente: Elaboración propia

En base a los riesgos se deduce que se tiene un nivel medio de seguridad frente a un alto nivel de riesgo, esto se debe al desequilibrio como institución que no ha derogado esfuerzos en pulir su sistema informático, la falta de personal especializado que gestione medidas de seguridad deriva en una elevada vulnerabilidad por fallos de personal, en contraste con hackeos virus, no se ha tenido percances significativos.

4.5 Fotos

El respaldo de haber efectuado la investigación de campo, además de evidenciar el estado físico de a infraestructura informática se detallan en las ilustraciones 6 Y 7.

Ilustración 6. Regulador de energía del ordenador principal (UPS)

Fuente: Elaboración Propia

Ilustración 7. Ordenadores encargados (derecha) y estudiantes (izquierda)

Fuente: Elaboración Propia

Se destaca que los ordenadores cuentan con regulador de energía que los protege en caso de corte inesperado de energía, no obstante, no todas las máquinas lo poseen ni su cableado se encuentra distribuido de la mejor manera, esto se atribuye a que la biblioteca no ha tenido mejoras sustanciales desde su inauguración.

4.5 Matriz FODA

El análisis interno/externo se resumen en el *cuadro 6.*

Cuadro 6. Matriz F.O.D.A (Fortalezas, oportunidades, debilidades y amenazas)

	FORTALEZAS: Asistencia a actividades académicas Fuente de consulta e investigación Área amplia y cómoda	*DEBILIDADES:* Falta de personal especializado Poco presupuesto Deterioro de infraestructura Políticas administrativas deficientes Falta de plan de seguridad informática
OPORTUNIDADES: Mejora de sus prestaciones Nuevas Tecnologías Potenciación de recursos informáticos	Aplicar configuraciones novedosas a red externa e interna Motivar investigaciones en seguridad informática	Gestionar inversión en optimizar recursos informáticos Cambio en la percepción de la relevancia en activos informáticos
AMENAZAS:	Elevar la eficiencia de	Automatizar un sistema de

Desastres naturales Fallos en sistema eléctrico Ataques de hackers	servicios Cloud Computing Implementar sistema de respaldo virtual	monitoreo de riesgo Mejorar la resistencia de la red, Firewall o comprar soluciones de seguridad

Fuente: Elaboración propia

Una de las debilidades más destacas es la falta de un reglamento local/nacional que regule la comercialización y penalizaciones en los servicios Cloud Computing en base a que la mayoría de aplicaciones, plataformas, almacenamiento e integración de datos son gestado en la nube, esto conlleva crear un grado de cultura que establezca la seguridad informática como una medida para el crecimiento tecnológico del Ecuador. (GONZALEZ SANCHEZ, 2016)

En el rango de las oportunidades se aconseja evaluar la posibilidad de aplicar modelos de operación, como la metodología *SUMA* (Sistema Ultra Micro Analítico) aporta estuches diagnóstico, equipos de medición y software, ofreciendo este último los procedimientos y como aprender el uso de la tecnología, soportado en Strips Reader Software SRS v 9.0 (registrado en el CEDMED) y consiste en una herramienta destinada al análisis, cálculo e interpretación de resultados para los diferentes estuches diagnósticos que pueden ser orientados a las necesidades, tendencias o exigencias de la Universidad Técnica de Machala, de forma particular ajustados a los requerimientos de sus unidades académicas. (Pías, Álvarez, Díaz, & Yero, 2014)

Se destaca el potencial investigativo que posee el centro de computo como modelo para mejorar la eficiencia en los centros informáticos de las demás unidades académicas, sus debilidades no son graves ni ostentan daños significativos, pese a ello se recomienda evaluar entorno a una auditora de código y configuración de la red usada en la UTMACH.

4.7 Resultados

En general se otorga una calificación *promedio* entorno al riesgo informático presente en el centro de computo evaluado, las soluciones propuestas pueden ser mejoradas al examinarse al establecimiento desde la perspectiva de sistemas (ingeniería de software, arquitectura del ordenador) para concatenar criterios de auditoria con la finalidad de optimizar el desempeño informático de la biblioteca de UACE.

También vale recalcar que un riesgo latente es la falta de cultura en los usuarios, pese a la existencia de políticas de control es responsabilidad institucional cuidar y preservar los recursos informáticos debido a su repercusión en la formación profesional de los estudiantes.

Cuadro 7. Matriz de resultados detallando relación causa-efecto

Causa	Efecto	Solución
Virus, malware	Daño de información o equipo	Actualizar antivirus, usar aplicaciones de control, respaldo del sistema
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: Elaboración propia

5. CONCLUSIONES Y RECOMENDACIONES

El riesgo informático latente en el centro de computo es de nivel regular, gracias a la aplicación de criterios de seguridad informática y control por pate de los encargados, el nivel de los controles físicos es bueno, los controles lógicos son regulares debido a desactualización de equipos-software.

Las vulnerabilidades como virus, hackeos/ ciberdelincuencia se pueden mitigar aplicando nuevas tecnologías en dicho ámbito, a la vez que se fortalece el centro de cómputo, sin embargo, las amenazadas no se pueden evitar haciendo necesario tener un plan de acción que vele por la seguridad de los activos informáticos, mismo que hasta el momento no se ha gestado.

El centro de computo al ser de gran potencial para los estudiantes como centro de acopio, acceso a internet y realización de tareas, debe ser mejorado a favor del desarrollo académico e informático que urge en la UTMACH.

Las documentaciones citadas se basan en el Estándar ISO 27001 que es aceptado a nivel internacional como referencia en seguridad/riesgo informático, por lo cual puede servir de modelo en el diseño de políticas de controles tanto físicos como lógicos aplicables al centro

de cómputo, además de mejorar la imagen institucional si se lograra certificar su adecuada cumplimiento.

Se recomienda motivar investigaciones que complementen la presente desde los criterios de un ingeniero en sistemas para en conjunto idealizar la elaboración de un plan de seguridad informática.

Se aconseja realizar gestiones de fondos para mejorar las instalaciones, se hace notoria el desfase de los equipos en contraste con las exigencias de hoy en día.

Se recomienda contratar personal especializado en seguridad informática para que mejore las defensas del centro de cómputo, proponga mejores soluciones e integre nuevos procesos de identificación de riesgos que no son competencia de las ciencias empresariales.

6. REFERENCIAS BIBLIOGRÁFICAS

Baryolo, M. O., Sentí, D. C., Camejo, I. R., & Rodríguez, D. C. (2012). Modelo de gestión de log para la auditoría de información de apoyo a la toma de decisiones en las organizaciones. *Acimed*, 187-200.

Dalilis, E.-R., Rosario, M.-P. M., & Luis, C.-R. (2016). La calidad de la auditoría en Sistemas de Gestión. *Ciencias Holguín*, 1-18.

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

González., R. A. (2007). LAS HABILIDADES DEL INGENIERO INFORMÁTICO LOGRADAS A TRAVÉS DE LA ENSEÑANZA DE LA FÍSICA, CON EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TICs). *Revista Pedagogía Universitaria*, VOL. XII.

GUSTAVO, I. G. (2017). *PLAN DE SEGURIDAD INFORMÁTICA BASADA EN LA NORMA ISO 27002 PARA EL CONTROL DE ACCESOS INDEBIDOS A LA RED DE UNIANDES PUYO.* Ambato: UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES-PROGRAMA DE MAESTRÍA EN INFORMÁTICA EMPRESARIA.

ISO. (2013). *International Organization for Standardization*. Obtenido de ISO/IEC 27002:2013: https://www.iso.org/standard/54533.html

Maya, R. P. (2013). El delito de acceso abusivo a sistema informático: a propósito del art. 269A del CP del 2000. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, N° 4.

Melo, A. H. (2008). EL DERECHO INFORMÁTICO Y EL DERECHO INFORMÁTICO Y DE LA INFORMACIÓN UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27001. *REVISTA DE DERECHO*, N° 29.

MOJICA, Y. G., & LISBOA, C. L. (2011). AUDITORÍA DE LAS APLICACIONES UTILIZAY CONTROL DE PROYECTOS. CASO DEDAS PARA LA PLANIFICACIÓN ESTUDIO: ORICONSULT, C.A. *Gerencia Tecnologica Informatica*, Vol 10.

PADILLA, M. V., CAÑAR, E. J., CEDILLO, D. K., MARQUEZ, K. J., & CUEVA, C. X. (2017). *AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA Y LÓGICA AL LABORATORIO DE COMPUTACIÓN DE LA ESCUELA RELIGIOSA LICEO JOSÉ MARÍA MORA DEL CANTÓN EL GUABO EN EL PERIODO LECTIVO 2017 – 2018.* Machala: UNIVERSIDAD TÉCNCIA DE MACHALA-UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES.

Pías, N. C., Álvarez, R. R., Díaz, A. R., & Yero, J. L. (2014). SISTEMA INFORMÁTICO SRS PARA EL PROCESAMIENTO DE DATOS EN LA TECNOLOGÍA SUMA. *REVISTA INVESTIGACIÓN OPERACIONAL*, 258-267.

Santiso, H., Koller, J. M., & Bisaro, M. G. (2016). Seguridad en Entornos de Educación Virtual. *Memoria Investigaciones en Ingeniería*, Núm. 14.

Solarte, F. N., Rosero, E. R., & Ruano, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE*, 492-507.