UTMACH

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE CIENCIAS DE LA EDUCACIÓN MENCIÓN DOCENCIA EN INFORMÁTICA

ACTUALIZACIÓN TECNOLÓGICA Y MEDIDAS DE SEGURIDAD DEL CENTRO DE CÓMPUTO DE LA ESCUELA FISCAL MIXTA ALEJANDRO CAMPOVERDE ANDRADE

CUENCA CUMBICOS RONALD DANILO
LICENCIADO EN CIENCIAS DE LA EDUCACIÓN

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE CIENCIAS DE LA EDUCACIÓN MENCIÓN DOCENCIA EN INFORMÁTICA

ACTUALIZACIÓN TECNOLÓGICA Y MEDIDAS DE SEGURIDAD DEL CENTRO DE CÓMPUTO DE LA ESCUELA FISCAL MIXTA ALEJANDRO CAMPOVERDE ANDRADE

CUENCA CUMBICOS RONALD DANILO
LICENCIADO EN CIENCIAS DE LA EDUCACIÓN

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE CIENCIAS DE LA EDUCACIÓN MENCIÓN DOCENCIA EN INFORMÁTICA

EXAMEN COMPLEXIVO

ACTUALIZACIÓN TECNOLÓGICA Y MEDIDAS DE SEGURIDAD DEL CENTRO DE CÓMPUTO DE LA ESCUELA FISCAL MIXTA ALEJANDRO CAMPOVERDE ANDRADE

CUENCA CUMBICOS RONALD DANILO
LICENCIADO EN CIENCIAS DE LA EDUCACIÓN

VELEZ TORRES EISER OSWALDO

MACHALA, 20 DE AGOSTO DE 2018

MACHALA
20 de agosto de 2018

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Actualización tecnológica y medidas de seguridad del centro de cómputo de la Escuela Fiscal Mixta Alejandro Campoverde Andrade, 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.

VELEZ TORRES EISER OSWALDO
0701046179
TUTOR - ESPECIALISTA 1

ENCALADA CUENCA JULIO ANTONIO
0702797432
ESPECIALISTA 2

VALAREZO CASTRO JORGE WASHINGTON
0703594705
ESPECIALISTA 3

Fecha de impresión: miércoles 22 de agosto de 2018 - 10:13

URKUND

Urkund Analysis Result

Analysed Document:	URKUND actualizacion tecnologica medidas seguridad centro computo ronald cuenca.docx (D40698090)
Submitted:	8/2/2018 2:06:00 AM
Submitted By:	rdcuenca_est@utmachala.edu.ec
Significance:	5 %

Sources included in the report:

ARCE CAMPOVERDE JUAN CARLOS.pdf (D21152599)

Instances where selected sources appear:

3

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

El que suscribe, CUENCA CUMBICOS RONALD DANILO, en calidad de autor del siguiente trabajo escrito titulado Actualización tecnológica y medidas de seguridad del centro de cómputo de la Escuela Fiscal Mixta Alejandro Campoverde Andrade, 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.

El autor 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.

El autor 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, 20 de agosto de 2018

CUENCA CUMBICOS RONALD DANILO
0705320273

RESUMEN

La tecnología se ha convertido en parte diaria del ser humano que simplifican las actividades personales y laborales, donde la computadora es un recursos didáctico aliado para el desarrollo académico y educativo del individuo. La difusión de la informática en las aulas educativas hace posible su uso pedagógico a través de los centros de cómputo existentes en las instituciones educativas. En la actualidad no se concibe una educación carente de la materia de informática, siendo necesario que las autoridades educativas otorguen un presupuesto adecuado para el mantenimiento y actualización de los centros informáticos. En la Escuela Fiscal Mixta Alejandro Campoverde Andrade del cantón Pasaje, se ha palpado la falta de seguridad en los equipos de cómputo, además de carecer de la actualización informática dando lugar a que el centro de cómputo sea vulnerable a daños informáticos y físicos por su inadecuado control. El objetivo general es describir los procesos para la actualización tecnológica y medidas de seguridad del centro de cómputo de la Escuela Fiscal Mixta Alejandro Campoverde Andrade del cantón Pasaje. El método utilizado fue el descriptivo tipo transversal usándose la técnica de la bibliografía para acceder a revistas científicas, libros, internet que den las pautas para la elaboración del presente trabajo. Como alternativa de solución se hizo un inventario de activos recomendándose la elaboración de políticas para la actualización y seguridad del centro de cómputo institucional para mantener los recursos tecnológicos en perfecto estado para el uso diario por parte de los estudiantes.

PALABRAS CLAVES: Seguridad equipos de cómputo, actualización informática, sistema de gestión, computadora como recurso didáctico, inventario de activos.

ABSTRACT

Technology has become a daily part of the human being that simplifies personal and work activities, where the computer is an educational resource allied to the academic and educational development of the individual. The dissemination of information technology in educational classrooms makes it possible to use it pedagogically through existing computer centers in educational institutions. At present an education lacking in the subject of computer science is not conceived, being necessary that the educational authorities grant an adequate budget for the maintenance and updating of the computer centers. In the Mixed Fiscal School Alejandro Campoverde Andrade of the Pasaje canton, the lack of security in the computer equipment has been felt, in addition to lacking the computer update, resulting in the computer center being vulnerable to computer and physical damage due to its inadequate control. The general objective is to describe the processes for the technological update and security measures of the computer center of the Mixed Fiscal School Alejandro Campoverde Andrade of the Pasaje canton. The method used was the descriptive transversal type using the bibliography technique to access scientific journals, books, internet that give the guidelines for the elaboration of this work. As an alternative solution, an inventory of assets was made, recommending the development of policies for the updating and security of the institutional computing center to keep technological resources in perfect condition for daily use by students.

KEY WORDS: Security computer equipment, computer update, management system, computer as a teaching resource, inventory of assets.

ÍNDICE

RESUMEN 1

ABSTRACT 2

1. INTRODUCCIÓN 5

2. MARCO TEÓRICO 7

2.1. Seguridad en equipos de cómputo 7

2.2. Sistema de gestión de seguridad de la información 9

2.3. Administración de un Sistema de Gestión de Seguridad de la información 10

2.4. Seguridad en un centro de cómputo 11

2.5. La computadora como recurso didáctico 11

2.6. Evaluación del nivel tecnológico y medidas de seguridad en el Centro de cómputo de la Escuela Fiscal Mixta Alejandro Campoverde Andrade 13

3. CONCLUSIONES 15

BIBLIOGRAFÍA 16

ÍNDICE DE TABLAS

Tabla Nº 1: Aspectos para la formación integral del estudiante en el centro de cómputo ... 12

Tabla Nº 2: Inventario de activos ... 13

Tabla Nº 3: Vulnerabilidades, riesgos y amenazas del centro de cómputo ... 14

1. INTRODUCCIÓN

El desarrollo tecnológico se ha convertido en un aliado para el progreso educativo. La informativa educativa consiste en el uso de tecnologías para educar a los alumnos de instituciones educativas, para los diversos niveles, planes de estudio, y para el desempeño personal de las empresas e instituciones que lo requieran. La difusión de la informática en las aulas educativas hace posible su uso pedagógico a través de los centros de cómputo existentes en las instituciones educativas.

Los centros de cómputo en las unidades educativas han permitido optimizar el proceso de enseñanza-aprendizaje de los estudiantes. Dando lugar que el Estado realice cuantiosas inversiones para que las instituciones educativas fiscales cuenten con centros o laboratorios de cómputo para acercar a los estudiantes a la práctica informática, optimizando sus actividades académicas.

Bennet, Maton y Kervin (2008) citado por Calderón, Padilla y Fornaguera (2013) señala que la importancia de los centros de cómputo es que los estudiantes tienen un acercamiento directo con la tecnología accediendo a información pertinente a su ambiente académico, formando personas que estén preparadas para afrontar el futuro de nuestra sociedad.

Hoy en día no se concibe una educación carente de la materia de informática, siendo necesario que las autoridades educativas otorguen un presupuesto adecuado para el mantenimiento y actualización de los centros informáticos. Sin embargo esta situación suele tornarse complicada en las instituciones fiscales.

Se ha obtenido la autorización de la Escuela Fiscal Mixta Alejandro Campoverde Andrade del cantón Pasaje, para realizar el presente trabajo de titulación, como resultado de la cual se pudo observar que los laboratorios cuentan con software sin licencias, versiones desactualizadas, programas antivirus gratuitos que impiden ejercer un mayor control, ausencia de políticas de mantenimiento y uso del centro de cómputo afectando a su seguridad, provocando que las computadoras se encuentren en mal estado impidiendo un uso adecuado de los recursos tecnológicos por parte de los estudiantes. Como lo señala Vega y Vinasco (2014) el incremento del uso del internet

reflejado en el mayor acceso de usuarios requiere de herramientas para proteger sus datos de ataques informáticos.

Objetivo general

Describir los procesos para la actualización tecnológica y medidas de seguridad del centro de cómputo de la Escuela Fiscal Mixta Alejandro Campoverde Andrade del cantón Pasaje.

Objetivos específicos

- Establecer los activos informáticos que posee la institución educativa.
- Identificar las vulnerabilidades y riesgos del centro de cómputo.
- Elaborar medidas de seguridad para el centro de cómputo de la unidad educativa.
- Determinar la situación actual de los equipos informáticos.

Metodología

El método utilizado fue el descriptivo tipo transversal usándose la técnica de la bibliografía para acceder a revistas científicas, libros, internet que den las pautas para la elaboración del presente trabajo.

Alternativa de solución

La Escuela Fiscal Mixta Alejandro Campoverde Andrade se elaboraron políticas para la actualización y seguridad del centro de cómputo institucional para lo que fue necesario establecer los factores críticos para elaborar una propuesta ajustada a sus necesidades informáticas para mantener los recursos tecnológicos en perfecto estado para el uso diario por parte de los estudiantes.

2. MARCO TEÓRICO

2.1. Seguridad en equipos de cómputo

La información es el medio por el cual se obtiene conocimiento de un determinado tópico, esta misma se expone diariamente a cambios dada las actualizaciones que existen a diario de lo sucedido en el mundo, las tecnologías protagonistas son las de información y comunicación, por este motivo, tomará al menos unos años hasta que toda la humanidad se comunique en la red por medio de la tecnología celular, siendo este el medio de comunicación con menor brecha digital (Ramírez, 2013). Según García y Vidal (2016) el número de equipos computacional se ha incrementado de forma significativo en las empresas e instituciones incrementándose las amenazas informáticas. De esta manera se demuestra que la información es tan valiosa en cada institución o persona que la posea al punto que debe de ser protegida de cualquier daño.

Los mayores ataques informáticos, según Miranda, Valdés, Pérez, Portelles y Sánchez (2016) , se dan por la fragilidad del software, malware, dispositivos móviles, personal institucional, piratas informáticos (hackers) provocando el 69% de los problemas de seguridad. La difusión de los virus es más rápida debido al acceso al internet, donde el objetivo del virus no solo es dañar al sistema sino obtener datos privados como contraseñas, claves de tarjetas de crédito (Quiroz, 2017). Ante esta realidad la ISO 17799:2005 (Organización Internacional de Normalización) para las cuales, la información es un activo muy importante y directamente le asigna un valor; por lo tanto, las organizaciones deben de proteger este activo (Alexander, 2012). Existen diferentes activos de información los cuales se clasifican de la siguiente forma:

- Activos de información como datos, manual de usuario.
- Documentación tales como contratos.
- Software informático evidenciado en aplicaciones, sistema operativo.
- Activos tecnológicos como computadoras, equipos, accesorios informáticos.
- Personal interno y externo.
- Imagen y posicionamiento de la empresa.
- Servicios comunicacionales.

En el momento en el que un programa posee la característica de duplicarse a sí mismo e infectar a una computadora, este se convierte en un virus, este se propaga de manera rápida e irrumpe en la computadora sin ningún permiso o consentimiento del usuario. Mata y Guevara (2010) indican que este virus puede contaminar a otras computadoras transmitiendo el archivo infectado, es tan sencilla su propagación que solo es necesario ejecutar, abrir o copiar el documento para que la computadora se infecte, de esta manera el virus toma ventaja de los servicios de la red y la transmisión de información vía USB.

Según Estrada, Alba y Martín (2012) las amenazas son los riegos que toda organización corre a la hora de mantener a salvo los activos de la misma. Caiza y Bolaños (2014) indican que es necesario que las empresas o instituciones evalúen los riesgos elaborando políticas de control para proteger la información. Cualquier tipo de acción que no esté previamente autorizada y además vulnere la integridad, confidencialidad y disponibilidad de la información obtenida por la organización es considerada una amenaza.

Basándose en (Guachi, 2012), el software es el equipamiento interno y lógico de una computadora que consta de un conjunto de programas que hacen posible la ejecución de una acción o tarea específica dentro de la computadora. Muy al contrario, el hardware es el conjunto de elementos físicos y externos que componen un ordenador. Asimismo, es de importante relevancia saber que las computadoras realizas tareas que fueron previamente ordenadas.

A partir de las portaciones de Díaz, Pérez y Proenza (2014), se extrae que toda organización o identidad está en la obligación de poseer una estrategia diseñada en la que se reguarde la información de cualquier tipo de amenaza, así mismo esta debe poseer un respaldo que garantice la continuidad, restablecimiento, y la recuperación en caso de que exista algún tipo de violación a la seguridad de información. A su vez la seguridad informática implica el reguardo de las tecnologías de información.

Con el motivo de mantener a salvo la información informática se implanta un SGSI (Sistema de Gestión de Seguridad de la Información) que asegura el reguardo de los datos ante la pérdida de:

- Confidencialidad de los datos la cual garantiza que, a la información solo tengan acceso personas autorizadas.
- Protección de datos: Resguarda la información de manera integra
- Disponibilidad del sistema: Asegura que la persona tenga acceso a la información siempre que sea necesario

Es necesario adquirir una mentalidad de prevención creando algunos hábitos al momento de acceder a internet, como lo son:

- No ingresar a sitios desconocidos o de poca confianza
- No descargar archivos ejecutables, adquirir software de organizaciones con prestigio.
- No permitir la instalación automática de software.
- No permitir el acceso a juegos o sitios para adultos por internet.
- Supervisar que los sitios web tengan certificado de seguridad.
- Evitar abrir correos electrónicos de dudosa procedencia.
- Configurar cortafuegos o firewalls para impedir la vulnerabilidad del computador.

En el momento de usar dispositivos de almacenamiento USB:

- Utilizar la memoria externa o pendrive en equipos confiables.
- Utilizar antivirus cada vez que se acceda al dispositivo de almacenamiento.
- Reiniciar el computador para que el virus sea eliminado de la memoria interna.
- Asigrar atributos de lectura y escritura al dispositivo de almacenamiento.

Las probabilidades de conseguir seguridad total son muy bajas ya que existen constantes amenazas que aparecen a diario, por este motivo la mayoría de las organizaciones prefieren adquirir cortafuegos o firewall y de esta forma bloquean el acceso sin consentimiento a las redes, además se aplica un SGSI que respalde y proteja la información de forma eficiente.

2.2.Sistema de gestión de seguridad de la información

El Sistema de Gestión de Seguridad de la Información (ISMS) son políticas de administración de la información. Este término es comúnmente usado por la ISO/IEC

27001, sin embargo, no es la única normativa que hace uso de este término. Un ISMS representa el diseño, implantación, mantenimiento de un conjunto de procesos que una organización utiliza para llevar eficientemente la accesibilidad hacia la información, de esta manera se pretende asegurar la confidencialidad, integridad y disponibilidad hacia los activos, y así mismo minimizando a la vez cualquier tipo de riesgo que corra la información.

Según Yánez y Yánez (2012) la ISO está conformada por 150 países y 350.000 organizaciones, ya sean estas públicas o privadas, a nivel mundial, conformando a su vez otros organismos como lo son el Instituto Argentino de Normalización y Certificación (IRAM); Instituto Nacional de Normas (ANSI), Instituto Ecuatoriano de Normalización (INEN), etc. Estos trabajan a nivel de comités Técnicos, además poseen más de 19.000 estándares publicados a partir de su fundación en 1947, y su publicación en el año 1951.

Mesquida, Mas, Amengual y Cabestrero (2010) comentan que la ISO 27001, una norma internacional posee y nos facilita un patrón para crear, implementar, operar, supervisar, mantener y optimizar el sistema de gestión (SGSI). Recientemente, en el año 2013, esta norma fue publicada dando a conocer la revisión más reciente y cambiando el nombre de esta norma dando lugar al siguiente: ISO/IEC 27001:2013.

2.3.Administración de un Sistema de Gestión de Seguridad de la información

Solarte (2015) et al. apunta que es necesaria la existencia de algunos factores y circunstancias que aseguren el éxito, de manera que estos sean: apoyo total e incondicional ofrecido por la dirección general, que sean compatibles los controles con la cultura organizacional, noción de los protocolos de seguridad, conocimiento de la organización de los riesgos, medios de comunicación con los trabajadores para expresar y analizar los aspectos de seguridad, alcance de las políticas y métodos de seguridad, además de los mecanismos que controlan la seguridad de la información, políticas, control y procedimiento para la administración del riesgo

2.4.Seguridad en un centro de cómputo

Llamamos seguridad a un conjunto de metodologías, documentos y programas y dispositivos con el objetivo de obstaculizar la entrada sin autorización a los recursos de cómputo, dando acceso único a quienes sean los usuarios del sistema evitando la intrusión de cualquier virus. Es necesario que se vigilen estas propiedades en particular:

Privacidad. – Solo aquellos que tienen derecho y autoridad deberán ver y manipular la información. Difundir o divulgar información confidencial es un ataque a la privacidad.

Integridad.- La información deberá ser veraz y no modificable ante cualquier tipo de alteración o amenaza no deseada. La alteración de los datos resultantes en cualquier identidad representa un ataque a la integridad.

Disponibilidad.- La información debe de ser accesible en el momento que el usuario requiera de su uso.

Es necesario que se posea una visión amplia que comprenda una cantidad específica de aspectos que tengan relación entre si metodológicamente. Existen dos áreas de gran calibre que se integran en el enfoque:

- Aspectos administrativos
    - Contar con políticas de seguridad dentro del centro de cómputo.
    - Poseer seguridad física y contra incendios.
    - Tener asignadas las responsabilidades en el personal.
    - Seguros
- Aspectos técnicos

2.5. La computadora como recurso didáctico

Con el fin de atender aquellos que no poseen los recursos necesarios al alcance, se solicita las mejores herramientas y elementos para promover el desarrollo educativo de manera equitativa, las computadoras funcionan como un material educativo innovador y de calidad, el mismo que carece en el día a día de los estudiantes dadas las posibilidades

y el entorno en el que se desarrollan. Para De Llano y Adrían (2003) estos dispositivos permiten practicar una educación más dinámica, ya que aporta recursos multimedia y de esta manera romper con el prototipo del libro como única fuente de aprendizaje y conectando con el aula. Amaro y Rodríguez (2016) dicen que el uso del internet debe contar con niveles de seguridad para proteger la información personal ingresada por el usuario

El uso de la informática debe de ser asimilada como un proceso de formación con criterio, que capacite al alumno de manera integral. La capacitación informática debe alcanzar otros objetivos además de ser solo un usuario más de la tecnología, logrando habilidades de tipo cognitivo, ético, social y actitudinal, tal como se lo indica en la tabla 1:

Tabla Nº 1: Aspectos para la formación integral del estudiante en el centro de cómputo

Aspectos	**Descripción**
Cognitivo:	Comprensión de la tecnología y critica analítica de la misma.
Aplicado:	Usar los medios de la informática y tecnología para crear y expresar ideas a través de la misma.
Ético:	Poseer opinión propia dentro de la tecnología infiriendo una crítica sobre el uso de la tecnología..
Social:	Comprender cuales son los impactos tecnológicos en la sociedad y que maneras estas pueden favorecer o perjudicar.
Actitudinal:	Crear una mentalidad abierta en la que se sepa que se posee control sobre la tecnología acercando al usuario a la misma sin miedo alguno.
FUENTE: De Llano y Adrián (2003)	

Podemos observar que en la Tabla nº 1 que esta información supera a las ideologías tradicionales de la tecnología, la implementación de clases de informática en institutos colegios y centros educativos en general hará del ciudadano un individuo con las capacidades necesarias para desarrollarse tecnológicamente y dentro de la sociedad se logrará un avance.

2.6.Evaluación del nivel tecnológico y medidas de seguridad en el Centro de cómputo de la Escuela Fiscal Mixta Alejandro Campoverde Andrade

Para evaluar el nivel tecnológico y medidas de seguridad en el centro de cómputo de la Escuela Fiscal Mixta Alejandro Campoverde Andrade se deben de determinar los activos más importantes con la intensión de establecer las vulnerabilidades, amenazas y riesgos dentro de la institución.

Tabla Nº 2: Inventario de activos

TIPO DE ACTIVO	NOMBRE DE ACTIVO
Activo de Información	Información de los usuarios, referencias de los proveedores, manuales de usuario, inventario de activos informáticos.
Software y Licencias	Licencia del sistema operativo, programas y aplicaciones informáticas con licencia, programas antivirus actualizados, y demás licencias con que deben de contar los programas informáticos.
Instalación de red eléctrica	Instalaciones eléctricas para computadores, sistema de conexión a tierra para evitar descargas de voltaje que pongan en riesgo los equipos de computación.
Servicios de terceros	Acceso a internet, mantenimiento de los equipos informáticos, compra y actualizaciones de los programas informáticos.
Personal	Talento humano a cargo del centro de cómputo, estudiantes y docentes que tienen acceso al sitio.
FUENTE: Solarte, Enríquez y Benavides (2015)	

En la tabla 2 se ha realizado el inventario de los activos dentro de la institución educativa para determinar su situación para determinar si el software posee licencias, se cuenta con antivirus actualizados, instalaciones eléctricas adecuadas con conexiones a tierra para evitar la sobrecarga de voltaje que ponga en riesgo a los equipos computacionales, determinar los servicios a terceros como son los proveedores de internet, empresas de mantenimiento tecnológico, determinar la situación del personal del área de informática, si cuentan con conocimientos actualizados.

En la tabla 3 se realizó el análisis sobre las vulnerabilidades, amenazas y riesgos potenciales que se palparon en el centro de cómputo de la Escuela Fiscal Mixta Alejandro Campoverde Andrade, para que en lo posterior se tomen las medidas correctivas para actualizar e incrementar los niveles de seguridad en los equipos informáticos.

Tabla Nº 3: Vulnerabilidades, riesgos y amenazas del centro de cómputo

Hardware		
Vulnerabilidad	**Amenazas**	**Riesgos potenciales**
Ausencia de equipos UPS para soportar apagones.	Cortes por fallas eléctricas internas o externas a la institución educativa.	Pérdida de datos, deterioro de hardware y software por apagado incorrecto.
Software		
Software sin licencia	Presencia de virus informáticos, troyanos, gusanos, malware, spyware.	Lentitud en los programas informáticos, daños al sistema operativo, ocultamiento de la información.
Software desactualizado	Acceso a información privada y sensible, uso de equipo como plataforma de ataque a otros sistemas.	Acceso no autorizado de usuarios que tienen acceso al robo de información privada, daños a equipos.
Seguridad física		
Ausencia de control para el acceso de personal no autorizado al centro informático de la institución educativa.	Acceso a equipos informáticos sin control, poniendo en riesgo el ingreso de virus, malware, spyware.	Pérdida de información, pérdida de equipos y/o accesorios informáticos, daño de equipos.
Seguridad lógica		
Ausencia de control en el acceso al centro informático.	Se suplanta identidad del usuario.	Robo de información, alteración, destrucción de datos, robo de claves de acceso.
Redes de comunicaciones		
Inseguridad en motores de búsqueda utilizados como Google, Bing, Firefox.	Acceso sin autorización desde sitios remotos.	Motores de búsqueda vulnerables para la pérdida de archivos y daños de la información.
Ausencia de políticas de seguridad en el centro de cómputo	Ataques al computador.	Borrado, destrucción, daño de información privada.
FUENTE: Solarte, Enríquez y Benavides (2015) ELABORACIÓN: El autor		

3. CONCLUSIONES

- La Escuela Fiscal Mixta Alejandro Campoverde Andrade posee entre los activos informáticos software y licencias, redes eléctricas, servicios a terceros, personal del centro de cómputo, los que están a disposición de los estudiantes para impartir las clases de informática.

- El centro de cómputo de la institución educativa posee una serie de vulnerabilidades que provocan amenazas y riesgos potenciales en los equipos e instalaciones tales como software sin licencia, falta de actualización del sistema operativo, antivirus desactualizados, reducido control al acceso de los equipos, vulnerabilidad en los navegadores, ausencia de políticas de seguridad, situación que provoca que ciertos equipos no estén aptos para su uso, impidiendo que las clases puedan ser desarrolladas de manera eficiente y oportuna perjudicando el desarrollo del proceso de enseñanza-aprendizaje.

- La institución educativa debe de diseñar políticas para garantizar la protección de los bienes informáticos, adquiriendo las licencias para el uso del software, ejerciendo mayor control en los estudiantes para que utilicen los equipos solamente para las tareas asignadas, evitando ingresar a sitios web de dudosa procedencia que dan lugar a la presencia de virus informáticos que dañan o vulneran los equipos informáticos de la entidad escolar.

BIBLIOGRAFÍA

Alexander, A. (2012). *Análisis y evaluación del riesgo de información: Un caso de la banca. Aplicación del ISO 27001:2005.* Lima: Pontificia Universidad Católica del Perú.

Amaro, J. A., & Rodríguez, C. R. (2016). Seguridad en internet. *Paakat: Revista de Tecnología y Sociedad*(11), 1-10.

Caiza, M., & Bolaños, F. (2014). Las implementaciones de las normas de seguridad de la información: estudio de caso la Sociedad de Lucha Contra el Cáncer del Ecuador. *Revista electrónica de Computación, Informática, Biomédica y Electrónica*(3), 2-22.

Calderón, M. d., Padilla, M., & Fornaguera, J. (2013). Introducción de tecnologías en el aula de dos preescolares públicos costarricenses: estrategias de autogestión, alcances y limitaciones. *Actualidades Investigativas en Educación, 13*(2), 1-23.

De Llano, J., & Adrían, M. (2003). *La informática educativa en la Escuela.* Caracas: Federación Internacional de Fe y Alegria.

Díaz, Y., Pérez, Y., & Proenza, D. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. *Ciencias Holguín, 20*(2), 1-14.

Estrada, Y., Alba, W., & Martín, A. (2012). Fundamentos para implementar y certificar un Sistema de Gestión de la Seguridad Informática bajo la Norma ISO/IEC 27001. *Serie Científica de la Universidad de las Ciencias Informáticas, 5*(10), 15-23.

García, G., & Vidal, M. J. (2016). La informática y la seguridad. Un tema de importancia para el directivo. *INFODIR*(22), 47-58.

Guachi, T. (2012). *Norma de seguridad informática iso 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa de Ahorro y Crédito San Francisco Ltda.* Ambato: Universidad Técnica de Ambato.

Mata, I., & Guevara, O. (2010). Virus informáticos. Todo un caso, pero no perdido. *Ciencia UAT, 4*(4), 56-61.

Mesquida, A., Mas, A., Amengual, E., & Cabestrero, I. (2010). Sistema de gestión integrado según norma ISO 9001, ISO/IEC 2000 e ISO/IEC 27001. *1856-8327, 6*(3), 25-34.

Miranda, M., Valdés, O., Pérez, I., Portelles, R., & Sánchez, R. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas, 10*(2), 14-26.

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

Ramírez, J. L. (2013). Humanización del aprendizaje en la era de la información: una arista andragógica. *Revista Electrónica "Actualidades Investigativas en Educación, 13*(3), 1-18.

Solarte, F., Enríquez, E., & Benavides, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la normas ISO/IEC 27001. *Revista Tecnológica ESPOL, 28*(5), 492-507.

Vega, O. A., & Vinasco, R. E. (2014). Captcha: ¿Una solución para la seguridad informática o problema para la accesibilidad/usabilidad web? *Revista e-Ciencias de la Información, 4*(2), 1-14.

Yánez, J., & Yánez, R. (2012). Auditorías, mejora contínua y normas ISO: Factores claves para la evolución de las organizaciones. *Ingeniería Industrial. Actualidad y Nuevas Tendencias, 3*(9), 83-92.