UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LOS CONTROLES DE SEGURIDAD EN LOS ORDENADORES DE LOS CUBÍCULOS EN UACE.

PINEDA ARGUDO PAUL ANDREI
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LOS CONTROLES DE SEGURIDAD EN LOS ORDENADORES DE LOS CUBÍCULOS EN UACE.

PINEDA ARGUDO PAUL ANDREI
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE LOS CONTROLES DE SEGURIDAD EN LOS ORDENADORES DE LOS CUBÍCULOS EN UACE.

PINEDA ARGUDO PAUL ANDREI
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 01 DE FEBRERO DE 2019

MACHALA
01 de febrero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Análisis de los controles de seguridad en los ordenadores de los cubículos en UACE., 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

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
ESPECIALISTA 2

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 3

Fecha de impresión: viernes 01 de febrero de 2019 - 11:31

URKUND

Urkund Analysis Result

Analysed Document:	PINEDA ARGUDO PAUL ANDREI_PT-011018.pdf (D47129833)
Submitted:	1/22/2019 10:20:00 PM
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

El que suscribe, PINEDA ARGUDO PAUL ANDREI, en calidad de autor del siguiente trabajo escrito titulado Análisis de los controles de seguridad en los ordenadores de los cubículos en UACE., 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, 01 de febrero de 2019

PINEDA ARGUDO PAUL ANDREI
0703918516

DEDICATORIA

En el presente trabajo investigativo titulado “ANÁLISIS DE LOS CONTROLES DE SEGURIDAD EN LOS ORDENADORES DE LOS CUBÍCULOS EN UACE”, lo dedico a Dios supremo creador y hacedor de las cosas, por ser mi mayor motivador.

A mis padres Numan y Maria, hermanos y familiares por ser el apoyo incondicional para continuar y culminar mis metas.

A los docentes de la UACE que con su esfuerzo y dedicación supieron guiarme en el sendero del aprendizaje

Pineda Argudo Paul Andrei.

AGRADECIMIENTO

- A Dios, por darme fortaleza y sabiduría para culminar el presente trabajo de investigación

- A mi familia, por brindarme su apoyo incondicional durante todo el ciclo estudiantil para cumplir meta, llegar a ser profesional en Contabilidad y Auditoría.

- Al Ing. Jorge Gonzales, docente tutor, por brindarme sus conocimientos académicos necesarios para mi formación profesional y por orientarme en el desarrollo del presente trabajo practico de investigación.

Pineda Argudo Paul Andrei.

RESUMEN

La docencia es una labor compleja, que exige responsabilidades éticas, morales y técnicas con la sociedad; en el proceso de formación profesional con el afán de renovar saberes en las diversas ciencias, contribuyendo al progreso de las naciones a la vez que se deroga, la tarea de solucionar las problemáticas sociales. La transferencia tecnología con fines académicos requiere herramientas tanto pedagógicas como didácticas, de las cuales destaca el ordenador, mismo que facilite elaborar clases, comunicación, acceder al sistema virtual para interactuar dinámicamente en el procedimiento de aprendizaje. El presente escrito analiza el estado de los computadores usados en los cubículos, de la Unidad Académica de Ciencias Empresariales, perteneciente a la Universidad Técnica de Machala; se estudian los controles físicos/lógicos que aseguran la integridad de la información, flujo de datos y que medios o mecanismos resguardan a este activo, se aborda la temática a través de la auditoría informática, a la vez se realiza una revisión a nivel contextual para determinar el estado de la UTMACH en relación a otras instituciones de educación superior. El objetivo del trabajo, es identificar las vulnerabilidades presentes en los ordenadores, proponiendo medidas de seguridad que respondan eficientemente ante posibles ataques, enmarcados en las tendencias contemporáneas.

Palabras Clave: ordenadores, cubículos, auditoría informática, controles.

ABSTRACT

Teaching is a complex task that demands ethical, moral and technical responsibilities with society; in the process of professional training with the desire to renew knowledge in the various sciences, contributing to the progress of nations while repealing, the task of solving social problems. The transfer of technology for academic purposes requires both pedagogical and didactic tools, of which the computer stands out, which facilitates the elaboration of classes, communication, access to the virtual system to interact dynamically in the learning process. This paper analyzes the state of the computers used in the cubicles, of the Academic Unit of Business Sciences, belonging to the Technical University of Machala; the physical / logical controls that assure the integrity of the information, the flow of data and which means or mechanisms protect this asset are studied, the subject is addressed through the computer audit, while a contextual level review is carried out. determine the status of the UTMACH in relation to other institutions of higher education. The objective of the work is to identify the vulnerabilities present in the computers, proposing security measures that respond efficiently to possible attacks, framed in contemporary trends.

Keywords: computers, cubicles, computer audit, controls.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

INTRODUCCIÓN

El rol de las universidades en la era contemporánea, también denominada *sociedad del conocimiento* es formar profesionales versátiles, capaces e íntegros que solventen de forma eficaz los problemas latentes las áreas correspondientes a su zona de influencia. Las exigencias actuales demandan el uso de las Tecnologías de la Información y Comunicación a través de sistemas informáticos para optimizar los procesos de enseñanza-aprendizaje, revolucionando el desempeño en la relación estudiante-docente gestando diversos servicios académicos/administrativos mediante ordenadores (Muñoz-Repiso, 2007).

Las NTIC´s dentro de las funciones pedagógicas potencian la didáctica en las clases, dinamizan la producción del conocimiento, ayudan a facilitar una enseñanza *horizontal* donde alumno/docente participan activamente en cumplir las competencias estipuladas en el syllabus. El implementar sistemas informáticos dentro de una institución de educación superior implica un cambio progresivo en procedimientos administrativos, académicos, estructura organizacional, desempeño docente, comunicación e interrelaciones personales; así como evaluar las ventajas-desventajas que caracterizan a los sistemas sofisticados en virtud de sus vulnerabilidades/amenazas, donde la auditoría informática es la encargada de emitir un informe bajo un juicio crítico e índole técnica para garantizar la fidelidad y seguridad de los datos, gracias a que la información es un activo indispensable en el desarrollo de cualquier entidad sin importar su función o naturaleza (Martinot, 2017).

En la Universidad Técnica de Machala los docentes deben brindar tutorías académicas, al reforzar los contenidos de las temáticas impartidas en clases, aclarar dudas sobre tareas o tutorar al estudiante en actividades curriculares; para ello cuentan con un ordenador de uso profesional, en el cual se realizan labores afines a la cátedra. No obstante, gestionar datos entre un grupo de personas trae consigo riesgos como hurto de información, filtrar documentos, manipulación de datos, modificar o cambiar calificaciones e irrupciones al sistema mediante la plataforma docente, debido a que desde sus computadoras acceden a la base de datos de la unidad académica (X. A. Vila, 2014); bajo tal preámbulo el presente trabajo delinea una evaluación de los controles físicos y lógicos que deben implementarse para mantener la integridad de la información en los ordenadores de los cubículos, analizar el grado de seguridad que impera en la unidad académica de ciencias empresariales e inferir propuestas sobre las medidas más eficientes desde la perspectiva de la auditoría informática.

2. DESARROLLO

2.1. FUNDAMENTACIÓN TEÓRICA

En esta sección se definen las concepciones y terminologías que describen al desarrollo del proyecto, se basa en la caracterización de criterios desde el punto de vista del autor, en favor de la argumentación epistemológica del estudio.

2.1.1 Auditoría Informática:

Es una disciplina, que integra una herramienta gerencial al evaluar la infraestructura de sistemas, coordinar aspectos financieros y tecnológicos a favor del cumplimiento de los objetivos institucionales; en lo relacionado a sistemas informáticos consiste en fiscalizar la seguridad de los activos computacionales, analizar las vulnerabilidades/amanezcas para establecer controles que garanticen la calidad de datos y mejora continua de la cadena de valor en todos los procesos externos e internos de la organización (Caycedo-Casas, 2017).

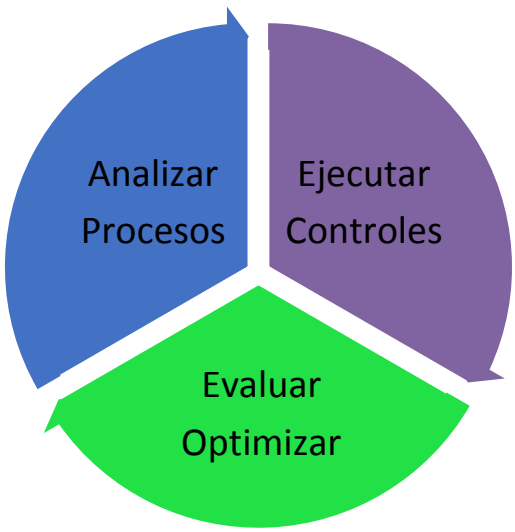

Ilustración 1 Relación entre los componentes de la auditoría informática Fuente: Elaboración Propia

2.1.2 Ordenador:

Es un sistema que permite tratar, organizar, computar, procesar y presentar información a través de periféricos de entrada/salida; es una máquina que opera mediante programas gestionados de manera lógica e interactúa con el usuario (interfaz hombre-máquina), su principal utilidad radica en la conectividad vía internet.

La aptitud de los docentes frente al computador es positiva, gracias a que notan mejor coordinación en tareas, potencian sus competencias pedagógicas, intensifica colaboración y el uso de software permiten simular condiciones semejantes a la realidad, además dan una pauta clara en el desarrollo de destrezas frente al uso adecuado de las herramientas tecnológicas (Vinas-Forcade, 2015).

Es necesario que cada estudiante y docente cuente con ordenador, se le otorgue las características óptimas para la enseñanza, los factores más destacables en las instituciones academias referente al uso de computador se resumen en el *cuadro 1.*

Ítems	N	Media	Desviación estándar
Acceso a Internet en mi casa.	101	4.45	.818
Las computadoras del centro educativo se encuentran en óptimas condiciones.	101	4.66	.803
Cada estudiante tiene acceso a una computadora en el laboratorio de informática.	101	3.10	1.513
El centro educativo dispone de suficientes computadoras con acceso a Internet.	101	1.93	1.227
El centro educativo posee red WiFi abierta para los docentes.	101	1.73	1.094
El centro educativo posee red WiFi abierta para los alumnos.	101	2.50	1.647
Tengo acceso a nuevos programas educativos para implementar en el aula.	101	1.72	1.176
Los programas de las computadoras del centro educativo están actualizados.	101	3.25	1.513
Las computadoras reciben mantenimiento de manera periódica.	101	2.69	1.528
El centro educativo facilita la capacitación docente en el área de cómputo.	101	2.71	1.486
El centro educativo cuenta con un soporte técnico para apoyar a los docentes.	101	2.67	1.530

Cuadro 1 Opinión docente sobre uso de ordenadores en las escuelas Fuente: (Gutiérrez, Escaño, & Guerrero, 2017)

2.1.3 Vulnerabilidad/Amenazas:

Son debilidades o aperturas que facilitan ataques potenciales, están directamente ligadas a las amenazas que son agentes internos/externos capaces de dañar o atacar aprovechando una oportunidad; en conjunto integran el riesgo que es la probabilidad de ser vulnerados; las afectaciones dependen de la exposición al peligro y de la respuesta del sistema en base a sus defensas (Yánez, Barahona, Naranjo, Fassler, & García, 2018).

Las recomendaciones más comunes para evitar ataques en computadores son:

- Mantener siempre al día todos los softwares
- Poner en práctica un firewall, sabiendo sobre sus aplicaciones y prestaciones
- No descargar ni instalar cualquier programa de internet, sin las garantías propuestas por sus desarrolladores

- Mantener un buen antivirus como seguridad AVG o Avast
- Realizar mantenimientos periódicos y realizar copias de seguridad (Tecnología & Informática, 2018)

2.1.4 Controles:

Son las medidas, regulaciones, normativas y herramientas que permiten responder a ciberataques, minimizar los daños derivados de acciones mal intencionadas, manteniendo un orden en los activos informáticos, son de carácter físico (al personal/equipos) y lógicos

(Configuraciones/software).

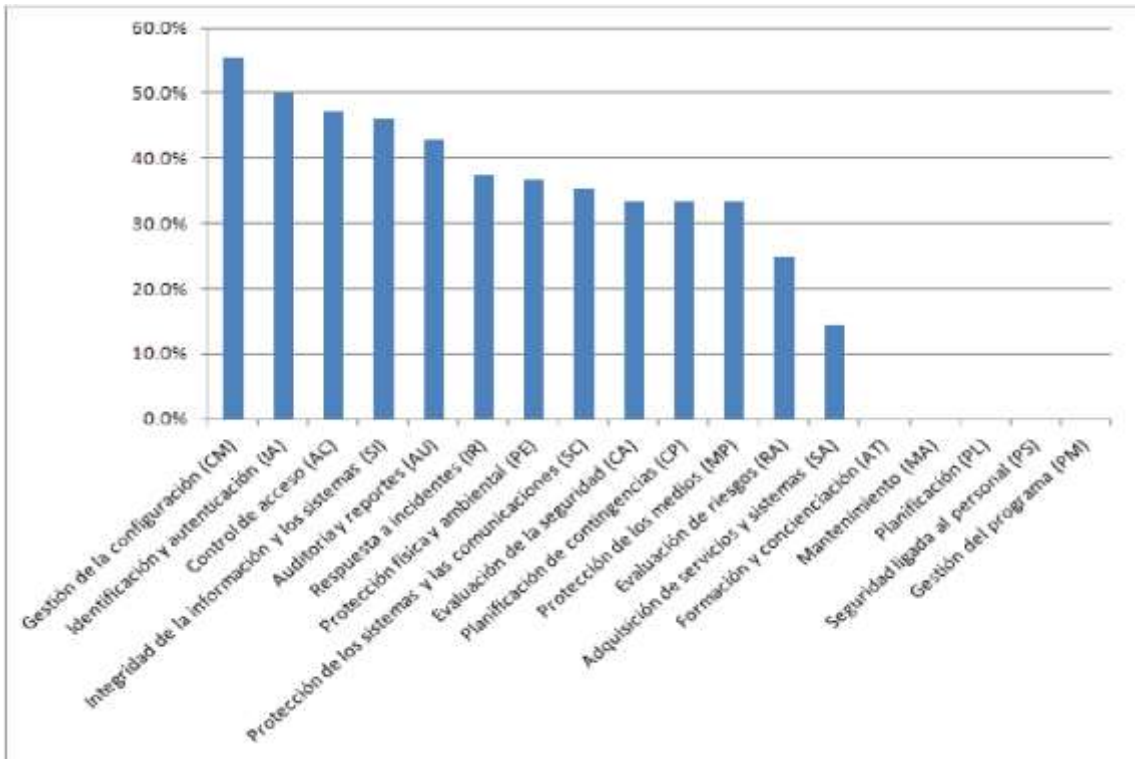

Ilustración 2 Medidas de seguridad automatizables en ambientes institucionales Fuente: (Perurena, García, & Rubier, 2013)

2.1.5 Seguridad de sistemas:

Se refiere a la convergencia de dos conceptos, la seguridad informática que presta las técnicas, mecanismos, algoritmos, configuraciones y controles que garantizan la integridad del sistema, su calidad, confiabilidad; mientras que la seguridad de la información es la ausencia de riesgos sobre los datos, sus procesos, guardado e inferencias que pongan en peligro el contenido de la institución.

Por lo tanto, es un proceso dinámico encargado de validar la seguridad de los entornos y activos informáticos, mediante controles e inferir sobre las políticas de uso en recursos tangibles e intangibles.

2.2. MARCO CONTEXTUAL

En este apartado, se aborda la temática a nivel macro, meso y micro identificando las tendencias actuales, procesos afines, referencias en países desarrollados o universidades de renombre e investigaciones, que describan el estado en el campo de estudio alrededor de la auditoría informática en ordenadores de uso docente.

A nivel general en las Instituciones de Educación Superior, se establecen políticas de seguridad física, lógica, inventarios, controles de software e imponen responsabilidades gradualmente, acorde a los riesgos o falencias, además se prevén ataques o miden amenazas al denotar vulnerabilidades, también se protege a la red de forma tangible e intangible, se toma prestado servicios virtuales solventado en plataformas Cloud Computing y en servidores propios respaldos por copias de seguridad/antivirus corporativos (ANUIES, 2011).

A nivel nacional se realizan indagaciones de auditoría informática, en los sistemas que solventan las necesidades universitarias, denotando que la revisión debe ser externa e interna, entre los puntos a evaluar se destaca:

- Ingreso de datos usuario
- Registro docente
- Administración de usuario
- Administración de roles y niveles
- Generar reportes e informes
- Analizar y optimizar procesos académicos
- Auditar periódicamente

La mayor vulnerabilidad apreciada, es que nunca se había auditado los sistemas por lo que se carecían de medios para interpretar e inferir un estado, además se desconocía el estado de los equipos o si han sido revisados por un profesional. (Jordán, 2016).

A nivel micro, se tienen la Política General de Seguridad de la Información de la Universidad Técnica de Machala; en el inciso 5.5 Equipos informáticos se dictan las siguientes consideraciones:

La UTMACH otorga al personal docente y administrativo computadores de escritorio y portátiles, así como equipos informáticos para el desenvolvimiento de las actividades académicas, con el fin de proteger la integridad física/darles buen uso (UTMACH, 2015), se debe cumplir con lo siguiente:

a) Cuando un departamento requiera un equipo, debe gestionar su compra previo informe técnico de la Dirección de TIC.
b) El departamento de bodega debe notificar a las direcciones de TIC el ingreso de todo equipo informático y actualizar inventario.
c) El computador es para uso exclusivo de actividades institucionales acorde a la función del servidor para su puesto.
d) Una vez terminada la jornada de trabajo, funcionario deberá apagar los equipos y guardarlos con las seguridades necesarias para evitar pérdidas o daños.
e) En caso de presentar algún problema el ordenador, el servidor deberá solicitar ayuda a través del Sistema Help-Desk y dependiendo de su oficina se escalará al técnico de Administración Central.
f) En caso de falla o mal funcionamiento del equipo en garantía, el usuario debe solicitar un informe técnico a la Dirección de TIC.
g) Con el fin de precautelar la información, el usuario debe asignar contraseña para encendido y protector de pantalla, la misma que dará a conocer a su jefe inmediato quien la usará en caso de emergencia institucional.
h) El funcionario a cargo del computador, es dueño de los datos almacenados y por tanto tiene la responsabilidad de efectuar los respaldos correspondientes con el propósito de garantizar la continuidad de los procesos.
i) Todas las estaciones de trabajo deberán usar fondo de escritorio y proyectos de pantalla institucional, el mismo que se activa después de diez minutos de inactividad.
j) El software instalado en los computadores, deberá ser el estrictamente necesario para llevar a cabo las funciones de cada usuario.
k) Cuando por alguna necesidad el usuario se retire de su puesto de trabajo debe dejar bloqueado su computador a fin de evitar que personas ajenas a sus funciones ingresen a la información.
l) El funcionario a cargo de un ordenador, cuando se ausente temporalmente deberá entregar el equipo a su jefe inmediato para su custodia.
m) Solo personal autorizado puede realizar administración remota a equipos tecnológicos de la UTMACH.
n) No está permitido:
    - Hacer cambios en la configuración del computador, sin el aviso de la dirección de TIC.

- Instalar o desinstalar software o componentes de software, configurar o cualquier cambio que afecte a las propiedades iniciales del equipo.
- La instalación de programas que traten de evadir las medidas de seguridad u otros aplicativos de entretenimiento o de uso personal, que no tengan que ver con el desenvolvimiento institucional.
- Conectar a la red de la UTMACH equipos informáticos sin previo visto bueno de la dirección de TIC.

2.3. MARCO METODOLÓGICO

Comprende la recopilación, de los procesos que permiten la elaboración del trabajo, siendo una triangulación entre obtención de información, tratamiento e interpretación de los estados citados.

2.3.1 Investigación Documentada:

Es la indagación en fuentes bibliográficas con el rigor académicos competente a trabajos de grado, tales como artículos de revistas científicas, proyectos de titulación, informes institucionales, PDFs de escritos o cualquier medio documentado que facilite la abstracción de información y argumentar los criterios descritos en el presente trabajo.

2.3.2 Estudio de caso:

Es un proceso del razonamiento empírico, que alude a un tema en específico dentro de su contexto real; su fortaleza radica en la facultad de relacionar los límites del problema a partir de un análisis profundo entre sus variables cualitativas, mayormente se utiliza en investigaciones educativas o de índole social, por su capacidad de enfocarse a un caso en particular (Pulido Polo, 2015).

2.3.3 Análisis sintético:

Es un proceso lógico, que converge dos facultades complementarias el análisis que establece relaciones en función de las características e infiere la comprensión del caso sintetizando los resultados obtenidos, para efectuar una descomposición mental de las fases del fenómeno objetando sus propiedades, este método es versátil en investigaciones que requieren reflejar el estado real de un problema en forma concreta (Rodríguez Jiménez & Pérez Jacinto, 2017).

2.4. DESARROLLO:

Se evalúa los controles actuales que resguardan la seguridad en los ordenadores, luego se proponen medidas de vanguardia para mejorar el desempeño tanto del docente como computador, a la vez que se refuerza la integridad de datos desde la perspectiva de la auditoría informática. En el *cuadro 2* se resumen las características de los ordenadores en los cubículos de tutorías.

HARDWARE	
Unidad Central de Procesamiento (CPU)	Intel Core I3 de 2.93 Ghz Memoria ram 2 Gb Disco duro 320 Gb
Dispositivos de entrada	Teclado QBEX Mouse QBEX Puertos USB Puerto VGA
Periféricos de salida	Monitor Resolución 800 x 600
Conexionado	Cable PS/2 y cable minidin (Teclado y Mouse) Cable serial (Modem externo- Scanner) Cable monitor. Cable par trenzado (Conexión a una red) Cable HDMI (Monitor, Pantalla, y Proyector) Cable Energía eléctrica
PROGRAMAS	
Sistema Operativo	Windows 10 Premium
Paquete integrado de prestaciones de oficina	*Microsoft Office:* Microsoft Word (Procesador de texto) Microsoft Excel (Hoja de cálculo) Microsoft PowerPoint (Diapositivas) Microsoft Access (Programa de bases de datos) Microsoft Outlook (Correo electrónico y cuentas)
Software	Antivirus Norton Internet Security Nero 7 Ultra Edition Windows Internet Explorer 7 Skype VLC Media Player Google Chrome Adobe Reader X 10.0.0 (2010) Adobe Flash Player 9.0.283.0 A (2010)

Cuadro 2 Características físicas y lógicas de los ordenadores docentes Fuente: Elaboración Propia

Los controles físicos y lógicos implementados actualmente en los ordenadores/cubículos docentes, se describen en el *cuadro 3.*

CONTROLES FÍSICOS (Docente)	
Acceso a ordenador con cuenta	Ingresar sistema por cuenta/contraseña
Autentificación	Asignación de cubículos y distributivo por horarios
Identificación	Marcar ingreso a la UACE
Vigilancia	Conserjes y personal actúan de veedores
Sanciones y medidas al personal	Política General de Seguridad de la Información de la Universidad Técnica de Machala
CONTROLES LÓGICOS Y CONFIGURACIONES	
Antivirus	Norton Internet Security
Protocolos de red a internet (Docente)	Reconocimiento de IP
Configuraciones de la red de ordenadores UTMACH	Medidas de protección en el servidor y controles implementados por la Dirección de TIC
Autentificación	Login/password en sistema docente (EVA, SIUTMACH, Correo institucional)
Copias de respaldo	En google drive (Gmail) o realizadas por el docente

Cuadro 3 Controles físicos y lógicos implementados en cubículos de UACE Fuente: Elaboración Propia

En relación a los controles, se diagnostican las vulnerabilidades que pueden representar un riesgo para los ordenadores

VULNERABILIDADES	
FÍSICAS	**LÓGICAS**
Poca vigilancia a estudiantes /docentes	Antivirus desactualizados/falta de antivirus de red
Conductas inadecuadas por personal o alumnos	Autentificación poco segura
Equipos desactualizados	Filtración de información a través de la red
Poca inversión en renovación de equipos informáticos	Ataques remotos o acceso no autorizado al sistema
No se realiza auditoria de sistemas en forma periódica	Ataques al servidor/suplantación de IP/configuración de seguridad incorrecta/robo de contraseñas o datos
	Falencias en red de ordenadores y acceso a internet

Cuadro 4 Vulnerabilidades latentes en los ordenadores docentes Fuente: Elaboración Propia

Análisis:

Los computadores docentes, no son máquinas aisladas forman parte del sistema informático de la UTMACH, evidentemente conjugan una red, por lo tanto, las vulnerabilidades también deben evaluarse desde la perspectiva del servidor, redes de acceso a internet, e interacciones entre usuario/sistema.

La falta de renovación de equipos computacionales, sistemas informáticos online, servicios web, a partir de las prestaciones Cloud Computing o bondades de la red; acarrea riesgos como accesos remotos, ataques vía internet, hackers, entre otras amenazas que pueden dañar potencialmente a los ordenadores e impactar a la información que gestionan los docentes.

Aunque, no se ha realizado auditoría con anterioridad, ni evaluado la seguridad computacional; es imperiosos un análisis escalonado desde los ordenadores hasta los servicios virtuales, para estar a la vanguardia de las tendencias globales, que a la vez que mejoran las prestaciones didácticas, incrementan la confianza en los estudiantes y docentes al usar los equipos informáticos.

La mayor debilidad del sistema, radica en el poco control físico hacia el personal, como todas las seguridades lógicas son programables e inminentemente objetivas, la falencia se da desde la parte humana, y más por ser de uso personal; por lo cual se proponen medidas de seguridad acorde a la revisión literaria citada, a través del *cuadro 5.*

CONTROLES DE SEGURIDAD FÍSICOS	
Vigilancia	Implementar video vigilancia por cámaras interconectadas a la dirección de TIC
Autentificación	Usar contraseñas cifradas mediante reconocimiento biométrico
Acceso al ordenador	Regular las sesiones con software semejantes a los cyber
Identificación	Portar credenciales y marcar horarios de uso de los ordenadores
Respuesta ante riesgos informáticos	Capacitar periódicamente al personal/recibir asesoría profesional
Políticas de seguridad	Imponen sanciones económicas o penalizaciones más graves por parte de la dirección de TIC
MEDIDAS DE SEGURIDAD LÓGICAS	
Antivirus	Actualización constante e implementar antivirus de red
Servidor	Encriptar datos, configurar direcciones IP con mecanismos de resguardo, tener dominios propios
Accesos remotos	Cortafuegos, autenticación cliente-servidor

	con barreras
Acceso a internet/redes de ordenadores	Emplear mecanismos de seguridad para evitar/prevenir ataques como inyección SQL, configuración de seguridad incorrecta o secuestro/suplantación de identidad e intercepción de datos
Datos e información	Copias de seguridad en la nube o respaldos en unidades de almacenamiento externas
Auditoría informática	Auditar y fiscalizar el sistema de forma regular, emitir informes e implementar mejores pertinentes para garantizar integridad de los recursos computacionales

Cuadro 5 Controles de seguridad para los ordenadores docentes Fuente: Elaboración Propia

Las medidas de seguridad, se pueden acatar de manera estratégica para estandarizar los controles en respuesta a los posibles ataques/vulnerabilidades, gracias a la implementación de normativas internacionales como la ISO 27002 y *Open Web Application Security Project* (OWASP), que garantizan una reacción dinámica ante cualquier eventualidad de índole informático, a más de dotar de una *filosofía* de mejora continua a todos los mecanismos que integran al sistema (Rubio, Sánchez, & M, 2009).

3. CONCLUSIONES

- Los ordenadores son instrumentos versátiles en la potenciación de las competencias pedagógicas, didácticas y optimizan los procesos de enseñanza, a la vez en el alumno mejoran las destrezas permitiendo emular ambientes educativos a través del software, facultan cálculos e interacciones mediante el uso/tratamiento de información, su mayor prestación es que dinamiza a la educación globalizando el conocimiento a todos sin importar condicionantes ni barreras físicas.
- Los sistemas informáticos se centran en computadores, siendo estos una herramienta docente con muchas bondades, por contraste también presenta vulnerabilidades, cuyo eje principal es la parte física (conducta del personal/estudiantes) que pueden desencadenar en ataques, o daños a la propiedad lógica de la UTMACH.
- Los controles físicos deben ser más severas y de carácter holístico, como cámaras de vigilancia, medidas biométricas, capacitaciones a docentes/estudiantes e integrar responsabilidades a todos los implicados, para empoderarnos hacia la institución.
- Los controles lógicos, deben enfocarse de manera sistemática, realizando auditorías de forma constante, gracias a que los ordenadores forman una red, la cual interactúa vía internet, estando siempre propensa a posibles amenazas que pongan en riesgo la calidad de información o datos académicos.
- Se aconseja invertir en la renovación, actualización y potenciamiento de los sistemas informáticos, debido a que la principal debilidad es la falta de tecnificación acorde a las medidas de vanguardia, para estar a la par de los ataques más comunes en los últimos años, además la falta de mantenimiento deteriora al hardware haciendo imperiosa una evaluación periódica de los recursos computacionales (PC, redes, servidores, routers, …).

BIBLIOGRAFÍA

ANUIES. (2011). *POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR.* Veracruz: CONSEJO REGIONAL SUR-SURESTE.

Caycedo-Casas, D. A.-F. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias*, 157-173.

Gutiérrez, V. F., Escaño, D. F., & Guerrero, M. (2017). ACTITUD DE LOS DOCENTES HACIA EL USO DE LA COMPUTADORA EN LAS ESCUELAS DE REPÚBLICA DOMINICANA. *Píxel-Bit. Revista de Medios y Educación.*, 197-210.

Jordán, M. G. (2016). *AUDITORÍA INFORMÁTICA PARA LA OPTIMIZACIÓN DEL FUNCIONAMIENTO DE LOS SISTEMAS Y EQUIPOS INFORMÁTICOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL.* Ambato: UNIVERSIDAD TÉCNICA DE AMBATO.

Martinot, M. P. (2017). Uso actual de las tecnologías de información y comunicación en la educación médica. *Rev Med Hered, 28*, 258-265.

Muñoz-Repiso, A. G.-V. (2007). HERRAMIENTAS TECNOLÓGICAS PARA MEJORAR LA DOCENCIA UNIVERSITARIA. UNA REFLEXIÓN DESDE LA EXPERIENCIA Y LA INVESTIGACIÓN. *RIED, 10*(2), 125-148.

Perurena, R. M., García, W. B., & Rubier, J. P. (2013). Gestión automatizada e integrada de controles de seguridad informática. *RIELAC, Vol.XXXIV* , 40-58.

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

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

Rubio, E. A., Sánchez, J. R., & M, I. I. (2009). *Desarrollo de Políticas de Seguridad Informática e Implementación de Cuatro Dominios en Base a la Norma 27002 para el Área de Hardware en la Empresa Uniplex Systems S.A. en Guayaquil.* Guayaquil: Escuela Superior Politécnica del Litoral “ESPOL”.

Tecnología & Informática. (2018). *Vulnerabilidades informáticas*. Obtenido de https://tecnologia-informatica.com/vulnerabilidades-informaticas/

UTMACH. (2015). *Política General de Seguridad de la Información de la Universidad Técnica de Machala.* Machala: Consejo Universitario.

Vinas-Forcade, J. (2015). PLAN CEIBAL: DE LOS PIZARRONES A LAS COMPUTADORAS. *Cuadernos de Educación Año XIII – Nº 13*, 1-14.

X. A. Vila, M. J. (2014). Diseño de una e–actividad para Seguridad Informática. *Jornadas de Enseñanza Universitaria de la Informática, XVI* , 33-39.

Yánez, H. M., Barahona, A. S., Naranjo, P. M., Fassler, M. I., & García, C. D. (2018). Detección de vulnerabilidades en aplicaciones que funcionan sobre el sistema operativo Android, mediante el desarrollo de una aplicación tecnológica. *ESPACIOS*, 1-11.