UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORIA DE SEGURIDAD INFORMÁTICA EN LOS LABORATORIOS DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH

REYES MATAMOROS GABRIELA LILIBET
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORIA DE SEGURIDAD INFORMÁTICA EN LOS LABORATORIOS DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH

REYES MATAMOROS GABRIELA LILIBET
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

AUDITORIA DE SEGURIDAD INFORMÁTICA EN LOS LABORATORIOS DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH

REYES MATAMOROS GABRIELA LILIBET
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

ORDÓÑEZ BRICEÑO KARLA FERNANDA

MACHALA, 18 DE JULIO DE 2018

MACHALA
18 de julio de 2018

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado AUDITORIA DE SEGURIDAD INFORMÁTICA EN LOS LABORATORIOS DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
TUTOR - ESPECIALISTA 1

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

PARRA OCHOA EUDORO BENITO
0701063406
ESPECIALISTA 3

Fecha de impresión: jueves 05 de julio de 2018 - 17:20

Urkund Analysis Result

Analysed Document:	REYES MATAMOROS GABRIELA LILIBET_PT-010518.pdf (D40268693)
Submitted:	6/20/2018 12:19:00 AM
Submitted By:	titulacion_sv1@utmachala.edu.ec
Significance:	3 %

Sources included in the report:

Tesis completa 1.docx (D10509854)
1486076859_557__Taller%252BGrupal%252B2%252Bactualizado.docx (D25470599)

Instances where selected sources appear:

2

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

La que suscribe, REYES MATAMOROS GABRIELA LILIBET, en calidad de autora del siguiente trabajo escrito titulado AUDITORIA DE SEGURIDAD INFORMÁTICA EN LOS LABORATORIOS DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

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

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 18 de julio de 2018

REYES MATAMOROS GABRIELA LILIBET
0705833648

DEDICATORIA

El presente trabajo se lo dedico a Mi Dios, pues él es quien guía cada paso que doy y me ha acompañado a lo largo de mi vida, sosteniéndome y ayudándome a levantarme para cumplir con todos mis objetivos, a mis padres por hacer de mí una persona de bien con muchas aspiraciones en la vida e inculcarme valores y principios fundamentales para mi crecimiento personal y profesional, por apoyarme en todo momento y motivarme a culminar mis estudios y alcanzar mis sueños.

AGRADECIMIENTO

Mi agradecimiento infinito principalmente a Dios porque él es el motor por el cual gira mi vida, a mis docentes por haberme impartido sus valiosos conocimientos a través de mis años de estudio académico en la Universidad Técnica de Machala, y finalmente a mi valiente madre que ha sido mi inspiración en todo momento para vencer los obstáculos que se me han presentado, es para ella mi gratitud, respeto y amor.

ÍNDICE

AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LOS LABORATORIOS DE LA UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES DE LA UTMACH

RESUMEN

Las Instituciones Educativas de tercer nivel en el Ecuador, se encuentran en constante innovación siendo una de las principales la utilización de las tecnologías y el internet, apareciendo así nuevas metodologías para poder establecer la utilización de las TICs, estas innovaciones traen consigo amenazas tanto físicas, como virtuales donde existen individuos que buscan robar información, por ejemplo, números de cuentas bancarias, dinero, direcciones, etc., además también se llegan a detectar problemas en el manejo de los activos electrónicos generando pérdidas o daños provocados por realizar de manera errada los procesos que se necesitan para mantener los equipos de la manera adecuada, logrando establecer laboratorios educativos con la calidad esperada.

Por lo cual, la implementación de controles de seguridad es considerado importante porque mediante ellos se puede evitar el robo de información, las máquinas se encuentran en buen estado, la utilización es la correcta, etc. Por lo cual, la presente una investigación establecerá una auditoría informática basada en la utilización de los laboratorios de la Unidad Académica de Ciencias Empresariales, para lograr detectar las vulnerabilidades que posee y de esa manera poder determinar los controles adecuados para mejorar la calidad que posee, proporcionando a los estudiantes laboratorios que logren tener seguridad, siendo adecuados para fines estudiantiles.

Palabras Claves

Seguridad Informática; Auditoria; Gestión; Tecnología; Laboratorios.

ABSTRACT

The Third Level Educational Institutions in Ecuador are in constant innovation, one of the main ones being the use of technologies and the Internet, thus appearing new methodologies to be able to establish the use of ICTs, these innovations bring with them both physical threats, as virtual where there are individuals who seek to steal information, for example, bank account numbers, money, addresses, etc., in addition to detecting problems in the management of electronic assets generating losses or damages caused by wrongly performing the processes that are needed to maintain the equipment in the proper way, managing to establish educational laboratories with the expected quality. Therefore, the implementation of security controls is considered important because they can prevent theft of information, the machines are in good condition, the use is correct, etc. Therefore, the present research will establish a computer audit based on the use of the laboratories of the Academic Unit of Business Sciences, to detect the vulnerabilities that it has and in that way to be able to determine the adequate controls to improve the quality that it has, providing students with laboratories that achieve safety, being suitable for student purposes.

Keywords

Information security; Audit; Management; Technology; Laboratories

INTRODUCCIÓN.-

En la actualidad vivimos sumergidos en el mundo de las tendencias tecnológicas donde el uso de sistemas computacionales en empresas, instituciones del estado e instituciones educativas es indispensable para su fortalecimiento, de forma, que no existe quien no esté relacionado o tenga necesidad de relacionarse con estos sistemas (Escorcia & Jaimes de Triviño, 2015).

En el sector educativo, se ha visto la necesidad de implementar sistemas computacionales y demás herramientas tecnológicas, señala; (Colorado & Navarro, 2012) "En el ámbito educativo se realizan innovaciones con el fin de incorporar nuevos procesos en los métodos de enseñanzas y aprendizajes, donde las herramientas tecnológicas se convierte en una ayuda para el docente el cual permitirá conocer la diversidad de estos recursos tecnológicos que implementándolos como fundamentos pedagógicos.

Por esta razón, los centros de educación superior del sector público del Ecuador en la actualidad están enfrentando un entorno mucho más exigente que los obliga a tener una gestión eficaz para captar y mantener a los estudiantes por la imagen pública que proyecta la institución como ente formador de profesionales competentes que se insertan en el mercado laboral (Moreira, Tachong, & Pico, 2016). Las tecnológicas se ven en un diseño constante de mejoras donde se une lo tecnológico y pedagógico, para lograr la adaptación y aceptación que se desea tener en el ámbito educativo (Gros & Ingrid , 2013).

Al incluir las tecnologías de la información en el sector educativo o cualquier otro, se crea con ello la necesidad de fijar estándares de seguridad electrónica. Vivimos en tiempos donde los sistemas tecnológicos son muy avanzados y a la vez de fácil acceso, las redes institucionales locales y regionales llegan a ser inmensas, además el uso de servidores y computadores personales tienen cada vez mayor capacidad de proceso y acceso a otros computadores cuya interconexión se extiende mundialmente (Voutssas, 2010).

Por consiguiente, la presente investigación encuentra apropiado aplicar una auditoría interna a los sistemas computacionales de los laboratorios de la Unidad Académica de Ciencias Empresariales (UACE) de la Universidad Técnica de Machala (UTMACH), con el fin de establecer controles físicos e informáticos que contribuyan a la seguridad, cuidado y mejoramiento de estos espacios.

FUNDAMENTACIÓN TEÓRICA.-

Son muchas las definiciones que se podría tomar en consideración, a continuación se detallará aquellas que se consideran más importantes para la investigación.

Seguridad Informática

En todo tipo de organización, empresas, instituciones educativas utilizan para la creación, procesamiento, transmisión y almacenamiento de su información las ventajas de las tecnologías de la información y las comunicaciones, debido a eso el número de amenazas se incrementa provocando que se busque la integridad y confiabilidad de dicha información con sistemas de seguridad informática (Miranda, Valdes, Perez, Portelles, & Sanchez, 2016).

Según Ávila & Suárez (2013) , la seguridad informática tiene como principal objetivo la protección de los recursos tecnológicos como los equipos de cómputo, servidores, Router, cables, etc. y, también de la información que se posee dentro de los mismos, desarrollando métodos y procedimiento que ayuden a reforzar o mantener un sistema seguro.

Es importante destacar que este tipo de seguridad no es un estado que se alcanza en un determinado momento o tiempo y que permanece estático, sino que debe ser considerado como un proceso continuo que siempre debe ser gestionado (Montesino, Baluja, & Porven, 2013).

Gestión de Seguridad

Es un proceso de mejora continua donde se mantiene un nivel aceptable de riesgo percibido, el cual es provocado por la vulnerabilidad que poseen los diferentes sistemas de cómputo donde las dos principales que se tiene son la mala programación que bloquean el funcionamiento permitiendo acceder a información confidencial, y la mala utilización provocando daños físicos a las máquinas (Carrasco, 2013).

Auditoría

La auditoría es una herramienta utilizada para diagnosticar, controlar, verificar y establecer las acciones o los procesos que poseen las empresas, con el fin de poder cumplir con los objetivos estratégicos planteados (Santamaria, Cardenas, & Vega, 2016).

En la actualidad la auditoría considerada tradicional, se la une con la informática para el mejoramiento de los procesos, naciendo la necesidad de incorporar personas especializadas en el ámbito informático en las auditorías, formando equipos capaces de adentrarse en las auditorías informáticas y que sirvan de apoyo a las auditorías financieras (Martinez, Briseida, & Liuba, 2013).

Auditoría informática

Es la revisión técnica, periódica o esporádica de los sistemas informáticos que se poseen dentro de las instituciones, estos sean hardware, software, instalaciones y personal, con la finalidad de analizar y evaluar, si la planeación se lleva como lo esperado, para medir la eficacia, la seguridad y la adecuación que los componen (Alvarez, 2016).

Donde el objetivo principal de las auditorías informáticas, es el control el cual define el resultado o propósito que se desea obtener por la implementación de procesos establecidos en los sistemas informativos de las instituciones (Gomez , 2014).

Auditoría a la gestión informática

Su aplicación se enfoca exclusivamente a la revisión de las funciones y actividades de tipo administrativo que se realizan dentro de un centro de cómputo, tales como la planeación, organización, dirección y control de dicho centro. Estas auditorías se vuelven cada día más exigentes porque mediante la globalización, los sistemas de información con el tiempo se están sustituyendo casi en su totalidad por la tecnología, donde se poseen inmensas y cada vez más complejas redes institucionales locales o regionales (Quiroz & Macías, 2017).

Auditoría de la seguridad de los sistemas computacionales

Es la revisión exhaustiva que se realiza a todo lo relacionado con la seguridad de un sistema de cómputo, sus áreas y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, las bases de datos, redes, instalaciones y usuarios del sistema (Muñoz Razo, 2002).

DESARROLLO.-

Desde que las diversas entidades de negocio de una empresa se fueron apoyando conjuntamente en la informática, conocer acerca de las herramientas informáticas que la tecnología nos ofrece ha tomado un valor indispensable cuando el objetivo principal es la adquisición de nuevos conocimientos que permitan a las personas avanzar en los procesos tecnológicos.

Hoy por hoy hasta la empresa más pequeña cuenta con computadoras que almacenan información importante, poseer éstos equipos se ha convertido en una necesidad y a su vez en una gran ventaja que facilita el desarrollo de las acciones diarias. Por ende, todo lugar donde se realice alguna actividad en específica se encontraran oficinas, centros de cómputo o cualquier espacio donde exista una o varias computadoras que guardan la información, sistemas o plataformas que faciliten y agilicen el desarrollo de sus actividades.

Al tratar la auditoría de sistemas computacionales Muñoz Razo (2002), en su libro, incluye de manera acertada la evaluación del hardware, software, gestión informática, información, diseño de sistemas, bases de datos, seguridad, redes de cómputo y otros conceptos o recursos especializados de los sistemas computacionales.

La Unidad Académica de Ciencias Empresariales cuenta con 4 laboratorios de cómputo para un total de 3000 estudiantes, el ingreso a los laboratorios es permitido en el momento que el docente o estudiante encargado solicite el permiso correspondiente mediante previa solicitud de autorización al responsable del cuidado de los laboratorios y sistemas computacionales de ésta unidad académica.

Los laboratorios son de uso exclusivo para el desarrollo de actividades educativas, y siempre estarán bajo supervisión del encargado o docente responsable del grupo. Se ha cuestionado mucho el hecho que los alumnos deban estar bajo supervisión para poder hacer uso de los equipos en los laboratorios de cómputo, sin duda esto se debe al mal uso y poco cuidado que le dan al mismo.

- **AUDITORÍA**

1º PLANEACIÓN

Por este motivo de aquí parte la importancia de llevar un control acerca de la seguridad informática de los laboratorios de cómputo de la UACE mediante la ejecución de una auditoría interna, la cual mediante visita preliminar a los laboratorios se logró obtener lo siguiente:

Análisis de la Problemática

- Vulnerabilidad de la seguridad informática de los laboratorios de la UACE, riesgo de pérdida, daño, alteración o hurto de los sistemas computacionales.

El origen de la auditoría se da por la continua presencia de contrariedades en los laboratorios de ésta unidad académica, que a pesar de la existencia de políticas de seguridad persisten, generando daños de los recursos tangibles e intangibles propiedad de la universidad, ocasionando retraso de las actividades y gasto económico que podría evitarse. Los 4 laboratorios cuentan con una sola persona encargada de su gestión y administración informática, cada uno tiene entre 25 a 27 computadores y permite una capacidad máxima de 32 personas por sala.

Se implementa un cuestionario (encuesta) direccionado a los alumnos, docentes y demás personal responsable, con el fin de evaluar el recurso humano que hace uso de los laboratorios y con ello obtener los resultados favorables o No favorables de la auditoría **(Ver Anexo A).**

Mediante un inventario se obtiene información real y exacta de los computadores existentes en los 4 laboratorios de cómputo.

LABORATORIO	N° DE COMPUTADORES	FUNCIONAN	NO FUNCIONAN	CAPACIDAD
Laboratorio # 1	25	25	0	32 personas
Laboratorio # 2	27	27	0	32 personas
Laboratorio # 3	27	27	0	32 personas
Laboratorio # 4	25	25	0	32 personas
TOTAL	104	104	-	128 personas

- **Cuadro elaborado por el autor en base a la información recopilada.**

Se establece la visita a los laboratorios para conocer el estado de los equipos de cómputo y poder verificar los programas que poseen en cada uno de ellos. Verificando aleatoriamente el estado en que se encuentran los equipos, CPU, monitores, mouse, teclado, regulador, puertos de conexión salida del CPU, conexiones eléctricas, cables de internet, sillas, escritorios, entre otros. **(Ver Anexo B).**

OBJETIVOS DE LA INVESTIGACIÒN

Objetivo General:

Realizar una auditoría para identificar las vulnerabilidades de los sistemas computacionales de la UACE y establecer políticas que contribuyan al buen funcionamiento y uso de estos sistemas de cómputo mediante el buen manejo de sus usuarios.

Objetivos Específicos:

- Determinar las posibles vulnerabilidades y riesgos de los aspectos tangibles dentro de los laboratorios que afecten a los sistemas computacionales de la UACE.
- Analizar las políticas de seguridad informáticas establecidas y validar su correcto funcionamiento.
- Evaluar el factor humano del área de sistemas y medir sus resultados.

GUÍA DE EVALUACIÓN

En el siguiente cuadro se detalla los puntos generales de evaluación con sus respectivos puntos de evaluación específico, los cuales están conectados directamente con los objetivos de la auditoría, también se expone las herramientas utilizadas para la ejecución.

Matriz de Evaluación de Puntos Generales

Punto general de evaluación	Definición	Puntos específicos de evaluación	Objetivos	Planes	Herramientas
Riesgos físicos	Riesgo derivado de los aspectos tangibles de la empresa como es el acceso del personal al equipo de cómputo, periféricos y componentes, así como lo relacionado con las instalaciones, mobiliario, equipos, construcciones y demás elementos palpables del centro de informática de la empresa	¿Las computadoras, equipos y demás accesorios se encuentran en condiciones óptimas para su uso continuo?	Determinar las posibles vulnerabilidades y riesgos de los aspectos tangibles dentro de los laboratorios que afecten a los sistemas computacionales de la UACE.	Inspeccionar las salas de computación	Observación directa
		¿El espacio asignado para la implementación y ejecución de los sistemas informáticos, se conserva en buen estado, y a su vez, está libre de insectos o polvo que dañe los equipos?		Realizar inventario	Inventario
				Verificar estado de los equipos	Experimentación
Riesgos operativos-Lógicos	Riesgos derivados del funcionamiento operativo (lógico) del sistema, en cuanto al comportamiento de sus lenguajes y programas, así como en los niveles de accesos, privilegios	¿La Facultad de Ciencias empresariales cuenta con antivirus y licencia propia?	Analizar las políticas de seguridad informáticas establecidas y validar su correcto funcionamiento.	Estudiar y analizar las políticas de seguridad informáticas ya establecidas.	Entrevista
		¿Existen restricciones para acceder libremente			

	y limitaciones en el manejo de sus archivos, bases de datos, formas de procesamiento de información y en sí de todos aquellos aspectos que de alguna manera van a influir en el buen funcionamiento del sistema computacional.	a ciertas páginas desde el navegador?			
		¿Se realiza mantenimiento preventivo a los computadores?			
		¿Existe un registro por equipo de los mantenimientos realizados?			
Riesgos del personal informático	Riesgos derivados de la actuación del factor humano del área de sistemas, ya sea del personal, de los usuarios, los asesores o consultores y de los desarrolladores o proveedores de sistemas de la empresa.	¿La persona responsable de los laboratorios cuenta con los conocimientos y preparación adecuada en sistemas informáticos?	Evaluar el factor humano del área de sistemas y medir sus resultados.	Evaluar a la persona encargada de la gestión informática	Encuesta
		¿Los alumnos son conscientes de las políticas establecidas por la UACE?		Evaluar a los alumnos que hacen uso de los laboratorios	
		¿Los docentes de la UACE se sienten comprometidos con el cuidado y buen manejo de los laboratorios?		Evaluar a los docentes responsables	

Elaborado por: Gabriela Reyes

La UACE ya cuenta las políticas establecidas para el uso de los laboratorios y computadoras, las cuales se encuentran colocadas en la entrada de cada laboratorio con el fin de que los usuarios las recuerden y pongan en práctica, uno de los objetivos de ésta auditoría verificar la ejecución de estas políticas **(Ver Anexo C)**.

MÉTODOS

La investigación dirigida a los laboratorios de la Unidad Académica de Ciencias Empresariales, se basa en dos técnicas de investigación las cuales son:

1) **Observación:** Mediante este método se logra la recolección de información que consiste en contemplar sistemática y detenidamente el comportamiento del objeto o fenómeno a

investigar, donde se relaciona directamente el investigador con el campo de estudio (Pulido Polo, 2015).

2) **Técnica de la Encuesta**: Se basa en la utilización de un cuestionario, para lograr conocer situaciones o problemas que se dan dentro de las organizaciones, empresas, o instituciones públicas, donde se obtienen datos para poder analizarlos y lograr tomar decisiones, desarrollar hipótesis o resolver problemas (Sanchez, 2012).

   Para poder realizar la encuesta se determina la población total de estudiantes de la carrera de administración de empresa de 3000, de los cuales se les deberá sacar la muestra, la cual se realizará mediante un cálculo aritmético donde se tomada diferentes consideraciones la cuales se medirá el nivel de confianza y el valor del error que es permitido, se realizará la fórmula sacando un total de 173 estudiantes a los que se les realizó la encuesta.

2º EJECUCIÓN

DESARROLLO DE HERRAMIENTAS

1) Encuesta.-

Mediante una encuesta realizada a 173 estudiantes, evaluamos parámetros importantes inmersos en los laboratorios de la UACE, donde se obtiene una calificación favorable en cuanto a todo lo derivado de los aspectos tangibles (hardware) e intangibles (software), cuidado y control de los equipos, personal responsable y docentes, mientras que con una calificación de “Suficiente” se califica al entorno de los laboratorios, su orden, cuidado e higiene, es decir que éste parámetro apenas alcanza una calificación mínima necesaria para satisfacer lo que se califica.

Por otro lado en el cumplimiento de las políticas de seguridad ya establecidas por el departamento correspondiente de la UACE por parte de los alumnos y cuidado de los sistemas informáticos mediante la aplicación de restricciones de acceso se obtiene una calificación de “Regular” y “Deficiente” correspondientemente, donde sólo el 29.8% estas conscientes de las políticas, y de la misma forma se obtiene una insatisfacción por la atención prestada dentro de los laboratorios por el encargado (**Ver Anexo D**).

2) Observación.-

Los equipos cuentan con programas básicos como son el Microsoft office, esto se evidencio mediante el inventario donde en el software de las computadoras se pudo verificar que no contaban con mayores programas que Word, Excel, Power Point, etc. (**Ver Anexo E**).

El estado de las máquinas era el adecuado porque el encargado realiza una revisión periódica, lo que permite prevenir en ciertos puntos, fallas que intervengan en el uso de las computadoras por lo estudiantes, dando mayor efectividad, pero aún así se detectaron riesgos que deben ser evaluados para poder disminuirlos mediante la aplicación de controles.

MATRIZ DE RESULTADOS

MATRIZ DE RESULTADOS PARA LA AUDITORÍA DE LOS SISTEMAS COMPUTACIONALES A LOS LABORATORIOS DE LA UACE

Punto específico evaluado	Excelente	Bueno	Suficiente	Regular	Deficiente
Condiciones de las computadoras, equipos y demás accesorios tangibles de los laboratorios de la UACE		X			
Entorno del espacio asignado incluyendo su cuidado e higiene para la implementación de los sistemas computacionales			X		
Cuidado de los programas y archivos del computador					X
Cuidado de los sistemas informáticos mediante la restricción de acceso a páginas no educativas o necesarias					X
Seguimiento y control de los mantenimientos realizados a cada computador		X			
Personal altamente calificado		X			
Alumnos conscientes de las políticas establecidas para el cuidado y uso de los laboratorios				X	
Docentes comprometidos con el cumplimiento de las normas establecidas		X			

Elaborado por: Gabriela Reyes

MATRIZ DE RIESGO

Matriz Análisis de Riesgo

CONSECUENCIAS

PROBABILIDAD	Insignificante 1	Menor 2	Moderada 3	Mayor 4	Catastrófica 5
HACKERS 1	BAJO	BAJO	BAJO	MODERADO	MODERADO
INCENDIO 2	BAJO	BAJO	MODERADO	MODERADO	MODERADO
VIRUS 4	MODERADO	ALTO	ALTO	ALTO	EXTREMO
FALLA DEL SERVIDOR 5	BAJO	BAJO	MODERADO	MODERADO	MODERADO

Con la siguiente matriz se determina, cuál de los riesgos encontrados afectan con mayor significancia a los laboratorios siendo que las computadoras por estar en dominio de los estudiantes se ven expuestas a un nivel alto a los malware y los virus, esto provocado por el uso indebido de las mismas, por el bajo de información inadecuado, la descarga de programas sin licencias, etc., que puede llegar a provocar en las máquinas fallas por la gran cantidad de virus que llegan a tener.

3º DICTAMEN

MATRIZ DE SITUACIONES RELEVANTES

En esta matriz se realiza la ubicación de las fortalezas, Debilidades, Amenazas y oportunidades que se le presenta a los laboratorios de la carrera de Administración de Empresas.

FORTALEZAS	OPORTUNIDAD
-Equipos de Computación en buen estado -Buena Gestión Administrativa -Docentes Responsables en el cuidado de los laboratorios.	-Constantes Innovaciones en las Tecnologías -Mejoramiento Continuo de las Estrategias Informáticas.
DEBILIDADES	**AMENAZAS DEL EXTERIOR**
-Personal en Encargado -Poca adecuación en su ubicación -Poca programación -Falta de Restricciones a páginas o sitios web no educativos.	-Estudiantes con poco conocimiento del correcto manejo de las máquinas. -Incremento en el número de programas maliciosos de la web. (VIRUS). - Fácil acceso a la información para los hackers.

Elaborado por: Gabriela Reyes

Se determina los siguientes factores como son las debilidades, porque a pesar de que el personal encargado realiza su labor, no proporciona ayuda a los estudiantes cuando se suscitan problemas de la manera adecuada, por lo cual se debe buscar realizar capacitaciones o actualización de conocimiento, las áreas de los laboratorios deben ser mejoradas en lo físico y lo virtual a pro de las innovaciones que se dan día con día en el ámbito educativo.

Las fortalezas que poseen los laboratorios de la carrera de ciencias empresariales es el interés constante por mantener los equipos en buen estado, una de las amenazas que poseen los laboratorios llegan a ser considerados el alumnado que posee falencias en el correcto manejo y políticas de los mismo, dando como oportunidades las innovaciones que pueden llegar a establecer un espacio estudiantil cada vez más automatizado y de grandes expectativas.

RESULTADOS ENCONTRADOS

Se ha examinado los sistemas computacionales de la Unidad Académica de Ciencias Empresariales que comprende básicamente en cuatro centros de cómputo destinados a laboratorios para uso de los estudiantes y docentes. Toda la información obtenida ha sido gracias a colaboración del personal encargado de ésta área y herramientas utilizadas para la

recolección de información. Tengo la responsabilidad de expresar una opinión sobre la seguridad de éstos sistemas computacionales basados en mi auditoría.

La auditoría fue realizada en base a la metodología del catedrático Carlos Muñoz Razo, en su libro "AUDITORÍA EN SISTEMAS COMPUTACIONALES", mediante a evaluación se determinó parámetros relevantes de analizar con el objeto de obtener una seguridad razonable acerca de sí las políticas ya determinadas para el buen funcionamiento y seguridad de los laboratorios se cumplen correctamente. Para el desarrollo de la auditoría se integraron papeles de trabajo que en caso de alguna aclaración puedan ser presentados como respaldo de todo el trabajo realizado y como base razonable para fundamentar las opiniones aquí vertidas.

SOLUCIONES

Los resultados de la auditoría indican que los sistemas computaciones de la UACE, presentan falencias en su seguridad informática, pese a obtener buenos resultados en la mayoría de los parámetros evaluados no alcanza la excelencia que requiere una institución de educación superior. Mediante la auditoría se plantea las siguientes soluciones:

- Replantear las políticas de seguridad de manera más específica.
- Concientizar a los usuarios del cumplimento de las políticas de seguridad.
- Capacitar al personal encargado en gestión administrativa de los sistemas informáticos.
- Aplicar estándares de seguridad para el ingreso los computadores y accesos a los programas.
- Aplicar restricciones a páginas que no sean útiles para el desarrollo educativo.

Por ende, además se determina la aplicación de un control de seguridad informática mediante la aplicación de un plan el cual, es considerado como un documento de trabajo y como tal será accesible a todo el personal de la Universidad Técnica de Machala, este plan se ajustará siempre a un sistema de seguridad que debe ser aplicado por los laboratorios para lograr la excelencia, el plan siempre se mantendrá actualizado. Se determina la estructura del Plan, revisar (**Anexo F)**.

CONCLUSIONES

- En conclusión, elaborar una auditoría informática es fundamental para toda identidad para de esa manera proteger tanto la integridad física de las máquinas, como la confiabilidad que se posee en la información, en el sistema educativo universitario se deben poseer laboratorios o centros de cómputo que cuenten con todas las herramientas necesarias para poder desarrollar las clases de la manera adecuada, por ende se realizó una auditoría informática a los laboratorios de la Unidad Académica de Ciencias Empresariales considerando varios aspectos relevantes a tomar en consideración, buscando lograr con ella eliminar las vulnerabilidades y de la misma forma desarrollar un plan para lograr la estructura idónea para los alumnos.
- La auditoría informática permite conocer todos los aspectos más relevantes dentro del sistema que se aplica, un claro ejemplo es en las políticas que poseen los laboratorios de ciencias empresariales, donde mediante la tabulación de las encuestas realizadas a los alumnos se determinó que no poseen un conocimiento de las mismas, siendo necesario el mejoramiento del sistema. Con la aplicación de la auditoría también se logra la disminución de los riesgos informáticos, los cuales ayudan a materializar las amenazas que se presentan y se reduce el impacto todo esto sin costos elevados o grandes estructuras de personal.
- Siendo así, mediante la aplicación de los sistemas de seguridad se logra la unión de los recursos humanos con los técnicos, siempre con el respaldo de las medidas administrativas garantizando que los controles permitan mantenerse al riesgo en niveles bajos, llegando hacer asumible por la institución pública.

BIBLIOGRAFÍA.-

-Escorcia, L., & Jaimes de Triviño, C. (2015). Tendencias de uso de las TIC en el contexto escolar a partir de las experiencias de los docentes. *Educación y Educadores*, 137-152. Obtenido de http://www.redalyc.org/articulo.oa?id=83439194008

-Colorado, B. L., & Navarro, R. E. (2012). La Usabilidad de TIC en la práctica educativa. *RED. Revista de Educación a Distancia*, 2-11. Obtenido de http://www.redalyc.org/articulo.oa?id=54723291004

-Moreira, M. C., Tachong, L., & Pico, B. R. (2016). Satisfacción de los Usuarios que reciben servicios de la Universidad Técnica Estatal de Quevedo. *Revista Científica Avances*, 192-200. Obtenido de http://www.ciget.pinar.cu/ojs/index.php/publicaciones/article/view/166/463

-Gros, B., & Ingrid , N. (2013). Mirando el futuro: Evolución de las tendencias tecno pedagógicas en Educación Superior. *Campus Virtuales. Revista Científica de Tecnología Educativa*, 131-140.

-Voutssas, J. (2010). Preservación documental digital y seguridad informática. *INVESTIGACIÓN BIBLIOTECOLÓGICA*, 127-155. Obtenido de

http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

-Miranda, M., Valdes, O., Perez, I., Portelles, R., & Sánchez, R. (2013). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas*, 14-26. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2227-18992016000200002

-Avila, A., & Suárez, D. (2013). Una Forma de Interpretar la Seguridad Informática. *Innovación, Ingeniería y Desarrollo*, 87-93. Obtenido de http://coruniamericana.edu.co/publicaciones/ojs/index.php/IID/article/view/282

-Montesino, R., Baluja, W., & Porven, J. (2013). Gestión Automatizada e integrada de Controles de Seguridad Informática. *Rielac*, 40-58. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59282013000100004

-Carrasco, A. (2013). Conceptos de Seguridad Informática y su reflejo en la Cámara de Cuentas de Andalucía. *Auditoría Pública*, 111-117. Obtenido de http://asocex.es/wp-content/uploads/PDF/Pag%20111-117%20N%2061.pdf

-Santamaria, G., Cárdenas, M., & Vega, P. (2016). La Auditoría de Gestión, una Herramienta Necesaria para la Economía. *UTCiencia Ciencia y Tecnología al servicio del pueblo*,

95-103. Obtenido de http://investigacion.utc.edu.ec/revistasutc/index.php/utciencia/article/view/46

-Martinez, Y., Briseida, B., & Liuba, L. (2013). Propuesta del Sistema de Acciones para la implementación de la Auditoría Informática. *Revista de Arquitectura e Ingeniería*, 1-13. Obtenido de http://www.redalyc.org/articulo.oa?id=193929227003

-Alvarez, V. (2016). Aplicación de un Modelo de Auditoría Continua Utilizando JD Edwards EnterpriseOne. *INVESTIGATION No.8*, 31-49. Obtenido de http://revistas.uees.edu.ec/index.php/IRR/article/view/10

-Gómez , J. F. (2014). El rol de la auditoría de sistemas de información en la evaluación del gobierno de tecnologías de información en las organizaciones. *Investigacion, Innovacion, Ingenieria*, 38-54. Obtenido de file:///C:/Users/aproaux2/Downloads/64-182-2-PB.pdf

-Quiroz, S., & Macías, D. (2017). Seguridad en Informatica: consideraciones. *Dom. Cien*, 676-688. Obtenido de https://dominiodelasciencias.com/ojs/index.php/es/article/download/663/pdf

-Muñoz, C. (2002). *Auditoria en Sistemas Computacionales.* México: Pearson Educación. Obtenido de https://cdryst.files.wordpress.com/2009/10/aussist.pdf

-Pulido Polo, M. (2015). Ceremonial y protocolo: metodos y tecnicas de investigacion cientifica. *Opción*, 1137-1156. Obtenido de http://www.redalyc.org/pdf/310/31043005061.pdf

-Sánchez, J. (2012). La encuesta, herramienta cognitiva. *Papers*, 169-192. Obtenido de https://ddd.uab.cat/pub/papers/02102862v97n1/papers_a2012v97n1p169.pdf

-Acha Iturmendi, J. J. (1994). Auditoría Informática en la empresa.

-Ampuero Chang, C. E. (2011). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA COMPAÑÍA DE SEGUROS.

-Arroyave, J. D., Herrera, J. V., & Esteban. (2007). *Propuesta de modelo para un sistema inteligente de Detección de Intrusos de Redes Informáticas.* Antioquia: Jornada Nacional de Seguridad Informática.

-Dávalos, A. F. (2013). Auditoría de Seguridad de Información. *FIDES ET RATIO*, 19-30.

-Parada, D., Flórez, A., & Gómez, U. (2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistemática de la Dinámica de Sistemas. *Información Tecnológica*, 27-38.

-Rocha , C. A. (2011). La Seguridad Informática. *Ciencia UNEMI*, 26-33.

ANEXOS

ANEXO A

ENCUESTA

UNIVERSIDAD TECNICA DE MACHALA

UNIDAD ACADEMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORIA

OBJETIVO: Realizar una auditoría para identificar las vulnerabilidades de los sistemas computacionales de la UACE y establecer políticas que contribuyan al buen funcionamiento y uso de estos sistemas de cómputo mediante el buen manejo de sus usuarios.

1. ¿Considera que los laboratorios de la UACE son apropiados para el desempeño académico?

Si	
No	

Sugerencia: _____

2. En general, considera que el funcionamiento de los equipos es:

Excelente	
Bueno	
Regular	
Malo	

3. ¿Conoce usted las políticas de seguridad establecidas para los laboratorios de cómputos de su facultad?

Si	
No	

¿De qué manera tuvo usted conocimiento? _____

4. ¿Qué políticas de seguridad usted aplica?, marque con una X según corresponda:

Políticas de Seguridad	Si	No
Ingresa ordenadamente al laboratorio		
Ingresa alimentos o bebidas		
Al salir de la sala deja el mobiliario en orden		
Se registra en la hoja de control		
Tiene buen comportamiento dentro del laboratorio		
Al término de clase deja el aula en el mismo orden que lo encontró		

Cambia la configuración del equipo de computación y de los programas contenidos		
Ha instalado algún software porque usted lo ha necesitado		
Cuando se presenta una anomalía o falla de los quipos, suspende de inmediato la operación de este y acude en ese mismo instante al encargado para comunicar		
Ha extraído alguna vez equipos de cómputo o elementos de laboratorio sin autorización		
Realiza juegos u otras actividades dentro del laboratorio		

5. En escala de 1 al 5 siendo el 1 la calificación más baja ¿Cómo evalúa los siguientes aspectos de los laboratorios de la UACE?

Aspectos	1	2	3	4	5
Servicio de digitalización					
Equipamiento de las salas					
Red inalámbrica					
Limpieza					
Iluminación					
Atención					

6. ¿Cuándo detecta algún problema en las máquinas de los laboratorios reporta al encargado?

Si	
No	

7. En caso de que exista algún problema, la atención que le brindan es:

Excelente	
Bueno	
Regular	
Malo	

8. Cuando se encuentra en el laboratorio ¿Con qué frecuencia el docente está en la sala?

Siempre	
Casi Siempre	
Muy poco	
Nunca	

9. ¿Cuándo ingresa a los laboratorios llena una hoja de registro?

Si	
No	

10. ¿Qué políticas de seguridad usted recomendaría para que las autoridades implementen en los laboratorios?

Firma del Encuestado

_____

ANEXO B

FOTOS VISITA PRELIMINAR

LABORATORIO 1

LABORATORIO 2

ANEXO C

POLÍTICAS DEL USO DEL LABORATORIO

DEL USO DEL LABORATORIO
·El ingreso y salida se realizará en forma ordenada en el laboratorio para evitar accidentes a los usuarios y equipos. **·Se prohíbe el ingreso de alimentos, bebidas y el uso de celulares en el laboratorio de cómputo.** **·Al ingresar, observar que los mobiliarios de aula se encuentran en orden, caso contrario informar en la hoja de control diaria.** **·El docente debe hacer registrar a los estudiantes el nombre, número de computador y firmas en la hoja de control.** **·El docente deberá mantener orden y cordura como en una sala de estudios, el estudiante deberá permanecer sentado, por lo tanto, el estudiante debe demostrar buen comportamiento dentro del mismo.** **·Las estaciones de trabajo están compuestas por cuatro sillas del mismo color, por lo tanto no deberán ser movidas a ningún otro sitio.** **·La pizarra debe quedar despejadas de escrituras, es decir limpia.** **·Al término de clase deberá quedar el aula en el mismo orden como lo encontró al ingresar.**
DEL USO DE LAS COMPUTADORAS
·Queda estrictamente prohibido cambiar la configuración del equipo de computación y de los programas contenidos en el mismo así como de instalar software que no estén autorizados. **·En caso que presenta alguna anomalía o falla de los equipos, el usuario suspenderá de inmediato la operación de este, y acudirá en ese mismo momento al encargado del laboratorio con el fin de no hacerse responsable y de ser sancionado.** **·Se prohíbe la extracción y movimientos de cualquier parte del equipo de cómputo o elementos de laboratorio (tal como son el cambio del teclado, mouse, cables de internet, etc.).** **·En caso de encontrarse al estudiante realizando juegos o cualquier otra actividad ajena a la realización de la clase será llamado la atención, en caso de que insista en el desarrollo de juego será apagado el computador.**

- **Políticas realizadas por el Departamento de Computaciòn de la UACE.**

ANEXO D
TABULACIÓN DE LAS ENCUESTAS

¿Considera que los laboratorios de la UACE son apropiados para el desempeño académico?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	125	70,2	72,3	72,3
	NO	48	27,0	27,7	100,0
	Total	173	97,2	100,0	
Perdidos	Sistema	5	2,8		
Total		178	100,0		

En general, considera que el funcionamiento de los equipos es:

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Excelente	77	43,3	44,5	44,5
	Bueno	62	34,8	35,8	80,3
	Regular	23	12,9	13,3	93,6
	Malo	11	6,2	6,4	100,0
	Total	173	97,2	100,0	
Perdidos	Sistema	5	2,8		
Total		178	100,0		

¿Conoce usted las políticas de seguridad establecidas para los laboratorios de cómputos de su facultad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	53	29,8	30,6	30,6
	NO	120	67,4	69,4	100,0
	Total	173	97,2	100,0	
Perdidos	Sistema	5	2,8		
Total		178	100,0		

Ha instalado algún software porque usted lo ha necesitado

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	100	56,2	57,8	57,8
	NO	73	41,0	42,2	100,0
	Total	173	97,2	100,0	
Perdidos	Sistema	5	2,8		
Total		178	100,0		

¿Cuándo detecta algún problema en las máquinas de los laboratorios reporta al encargado?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	141	79,2	81,5	81,5
	NO	32	18,0	18,5	100,0
	Total	173	97,2	100,0	
Perdidos	Sistema	5	2,8		
Total		178	100,0		

En caso de que exista algún problema, la atención que le brindan es:

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Bueno	10	5,6	5,8	5,8
	Regular	151	84,8	87,3	93,1
	Malo	12	6,7	6,9	100,0
	Total	173	97,2	100,0	
Perdidos	Sistema	5	2,8		
Total		178	100,0		

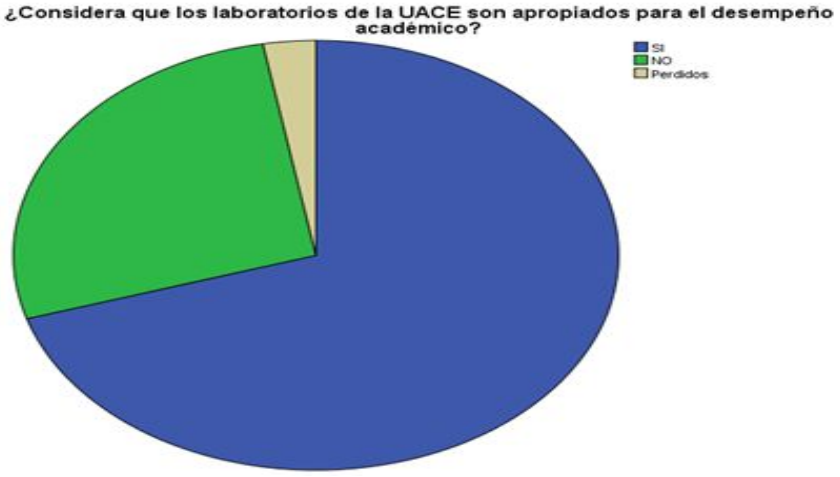
Cuando se encuentra en el laboratorio ¿Con qué frecuencia el docente está en la sala?

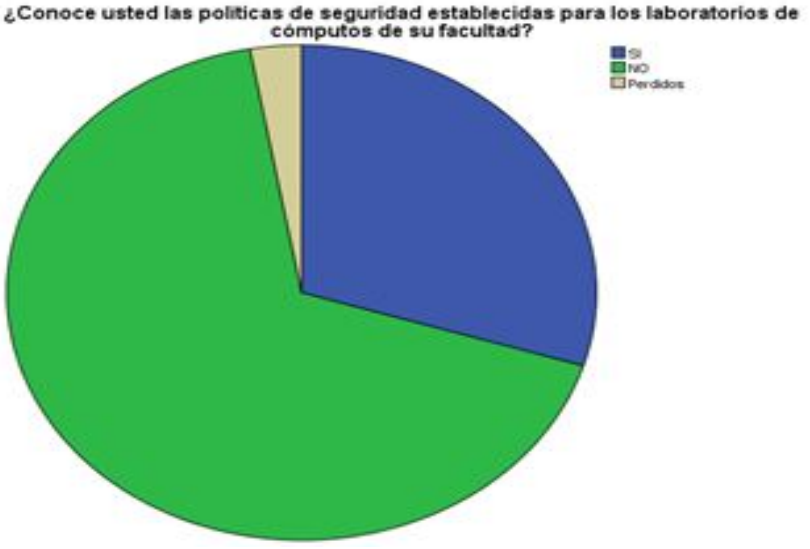
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Siempre	169	94,9	97,7	97,7
	Casi Siempre	4	2,2	2,3	100,0
	Total	173	97,2	100,0	
Perdidos	Sistema	5	2,8		
Total		178	100,0		

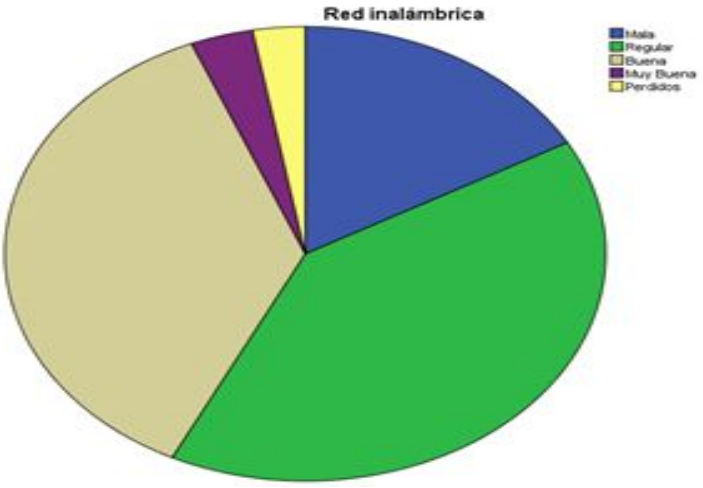
¿Cuándo ingresa a los laboratorios llena una hoja de registro?

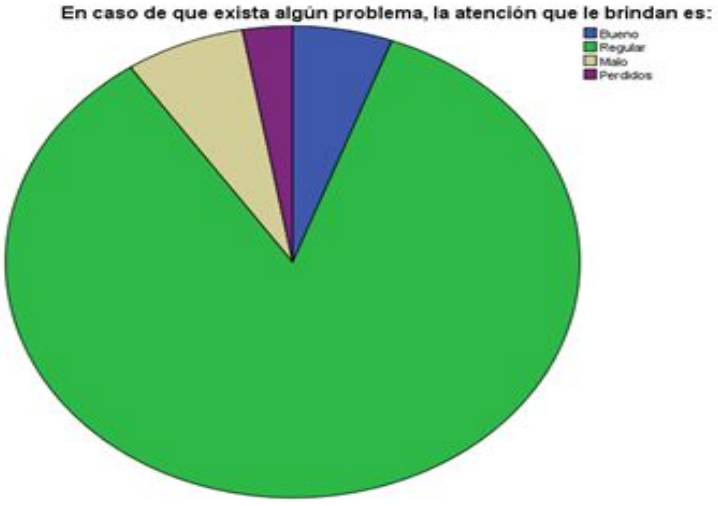
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	173	97,2	100,0	100,0
Perdidos	Sistema	5	2,8		
Total		178	100,0		

GRÁFICOS DE SECTORES









ANEXO E

FOTO DE PROGRAMAS

ANEXO F

PLAN DE SEGURIDAD INFORMÁTICA

Elaborado por: Gabriela Reyes