UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA EL CENTRO DE COMPUTACIÓN DE LA ESCUELA LICEO JOSÉ MARÍA MORA

CORREA CAÑAR EVELYN JULEYSI
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA EL CENTRO DE COMPUTACIÓN DE LA ESCUELA LICEO JOSÉ MARÍA MORA

CORREA CAÑAR EVELYN JULEYSI
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA EL CENTRO DE COMPUTACIÓN DE LA ESCUELA LICEO JOSÉ MARÍA MORA

CORREA CAÑAR EVELYN JULEYSI
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

ORDÓÑEZ BRICEÑO KARLA FERNANDA

MACHALA, 04 DE FEBRERO DE 2019

MACHALA
04 de febrero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA EL CENTRO DE COMPUTACIÓN DE LA ESCUELA LICEO JOSÉ MARÍA MORA, 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

GONZALEZ SANCHEZ JORGE LUIS
0703333898
ESPECIALISTA 2

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 3

Fecha de impresión: lunes 04 de febrero de 2019 - 07:49

URKUND

Urkund Analysis Result

Analysed Document: CORREA CANAR EVELYN JULEYSI_PT-011018.pdf (D47131341)
Submitted: 1/22/2019 11:08:00 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

La que suscribe, CORREA CAÑAR EVELYN JULEYSI, en calidad de autora del siguiente trabajo escrito titulado PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA EL CENTRO DE COMPUTACIÓN DE LA ESCUELA LICEO JOSÉ MARÍA MORA, 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, 04 de febrero de 2019

CORREA CAÑAR EVELYN JULEYSI
0750194730

RESUMEN

Un sistema de control interno se ha caracterizado por ser una herramienta que ayuda a salvaguardar los sistemas informáticos que se manejan dentro del ámbito profesional o empresarial, de tal forma que diseña un esquema de protección ante las vulnerabilidades, para que las operaciones se ejecuten de manera eficiente y eficaz, logrando cumplir con sus objetivos propuestos. Por ello, la presente investigación se fundamenta en proponer un Sistema de Control Interno Informático, para el centro de cómputo de la Escuela Religiosa Liceo José María Mora del cantón El Guabo, debido a que está expuesta a riesgos informáticos que impiden el desarrollo de sus funciones. El objetivo propuesto es de determinar los factores que conlleva un sistema de control interno, mediante la determinación de políticas, normas, procedimientos y controles como los preventivos, detectivos y correctivos, con el propósito de llevar una correcta administración de los recursos informáticos y brindarle mayor seguridad. Asimismo se utilizará la metodología de carácter descriptivo, donde se comenzará con investigaciones bibliográficas de artículos científicos, para detallar a criterio propio los pasos de aplicación del sistema mencionado, refiriéndose primero el entorno del lugar, segundo la configuración del sistema informático, tercero establecer políticas, normas y procedimientos y por último definir controles.

Palabras claves: Control interno, controles preventivos, controles detectivos, controles correctivos, y recursos informáticos.

ABSTRACT

An internal control system has been characterized as a tool that helps to safeguard the computer systems that are handled within the professional or business environment, in such a way that it designs a protection scheme against vulnerabilities, so that operations are executed in a efficient and effective, achieving compliance with its proposed objectives. Therefore, this research is based on proposing a computerized internal control for the computer center of the Religious School Liceo José María Mora of El Guabo Canton, because it is exposed to IT risks that hinder the development of their duties. The proposed objective is to determine the factors that lead to an internal control system, through the determination of policies, rules, procedures and controls such as preventive, detectives and corrective, with the purpose of carrying out a correct administration of computer resources and provide greater security. The methodology descriptive, which will begin with bibliographic research of scientific articles, to detail its sole discretion steps of applying the system mentioned, referring to the setting of the place, second configuration of the computer system, third policies set first will also be used, standards and procedures and finally define controls.

Keywords: Internal control, preventive controls, detective controls, corrective controls, and computer resources.

ÍNDICE

RESUMEN **1**

ABSTRACT **2**

ÍNDICE **3**

INTRODUCCIÓN **4**

1. FUNDAMENTACIÓN TEÓRICA **5**

1.1 Control interno 5

1.2 Control Interno informático 5

1.3 Clasificación de las actividades de control interno 6

1.4. Seguridad de la información 6

2. DESARROLLO **7**

3. CONCLUSIONES **16**

BIBLIOGRAFÍA **17**

ANEXOS **19**

ÍNDICE DE TABLAS

Tabla 1. Fases del proceso de controles de seguridad informática. 8

Tabla 2. Controles preventivos, detectivos y correctivos. 13

ÍNDICE DE ANEXOS

Anexo A. Características de las computadoras del laboratorio de computación de la Institución Educativa. 20

INTRODUCCIÓN

En los últimos años, el uso de la informática ha generado un crecimiento mundial en las actividades profesionales de cada individuo, de tal forma que se ha convertido en un componente fundamental, para el desarrollo económico y social de un país. Además, cabe recalcar que juega un papel importante dentro de los fines académicos, debido a que facilita el desarrollo de las actividades, mediante la exploración y construcción de conocimientos que permiten desarrollar la formación intelectual (Fombona, Vázquez, & Reis, 2016).

Sin embargo, varias de las organizaciones educativas presentan dificultades en el desarrollo de sus actividades, por motivos de que carecen de controles, de tal modo que son endebles a los riesgos informáticos, como la pérdida de información, fallas técnicas, entre otros. En este sentido Huapaya (2017) confirma, que esto se debe por no emplear adecuadamente las normas y procedimientos que se instauraron en las políticas internas como también a la desactualización de las mismas. Como en el caso de la escuela Religiosa Liceo José María Mora, sus actividades no están acorde a lo planificado en el programa académico que se distribuyó al centro de cómputo.

Por ello, el presente trabajo se enfoca en determinar los factores que conlleva un sistema de control interno, mediante la determinación de políticas, normas, procedimientos y controles como los preventivos, detectivos y correctivos, con el propósito de llevar una correcta administración de los recursos informáticos y brindarle mayor seguridad. Paralelamente a esto, es importante concretar que los controles que se implemente, deben estar acorde a las funciones que desarrolle la institución, para así garantizar un desempeño eficiente.

La pesquisa aplicada es de carácter descriptiva, porque detalla el objeto de estudio mediantes pasos, teniendo en cuenta dos teorías que se detallaron en el apartado de metodología; los cuales sirven como base para desarrollar la propuesta del sistema de control interno informático, estableciendo los siguientes pasos: primero el entorno del lugar, segundo la configuración del sistema informático, tercero establecer políticas, normas y procedimientos y por último definir controles que permitirán proteger a los equipos informáticos y a las tecnologías de información de la institución.

1. FUNDAMENTACIÓN TEÓRICA

1.1 Control interno

El control interno, es aquel sistema de carácter preventivo que busca salvaguardar los recursos que conlleva una entidad, de tal modo que brinde seguridad a sus funciones y a su vez confiabilidad en los datos, con el único propósito de que se logren los objetivos planteados (Portal, 2016). Asimismo cabe recalcar que el propósito de este sistema se fundamenta en niveles como lo establece Quinaluisa, Ponce, Muñoz, Ortega, & Pérez, (2018) indicando a la "Eficacia y eficiencia de las operaciones, fiabilidad de la información y el cumplimiento de las leyes y normas" (pág. 269).

1.2 Control Interno informático

Desde el punto de vista de Estupiñán, (2015) indica que los controles internos se encuentran englobados con la informática, debido a que estan incorporados en todos los niveles organizacionales, de tal forma que se plantean medidas automatizadas para las operaciones; orientandolas a planear, direccionar y organizar el grado de cumplimiento de los sistemas informáticos, a fin de evitar eventos no deseados.

Por lo tanto, se llega a establecer que un control interno informático debe conllevar los siguientes aspectos:

- Ser apropiado y efectivo,
- Acorde a las necesidades del ente económico
- Contener normas y procedimientos
- Llevar registros y manejo de información

Además Mancilla & Saavedra, (2015) mencionan que el control interno informático recurren en el análisis, desarrollo e implementación de sistemas que surgen en la operación, procedimientos de datos, procesamiento de información y la difusión de resultados, de tal forma que se cree un ambiente de autocontrol con normas de seguridad.

Otro punto importante de las medidas de control, es que se pueden generar bajos dos aspectos, tanto manuales como automáticos, en el primer caso se realiza por el responsable del área, sin manejar instrumentos computacionales; en cambio los automáticos, se refieren al software en cuanto a su composición ya sea por medio de programas de aplicación, métodos de comunicación e información, gestión de datos, etc.

1.3 Clasificación de las actividades de control interno

Los controles preventivos, son aquellos mecanismos que permiten pronosticar un suceso no deseado antes de que se acontezca; es decir, se enfocan únicamente en reducir o restringir la posibilidad de ocurrencia del riesgo ante su origen y agente generador (Orjuela, 2016).

En lo que respecta a los controles detectivos, tienen la función de identificar los hechos o anomalías en el momento en que se materialicen, de tal forma que se neutralice su origen; por lo que González, Myer, & Muñoz, (2017) indican que en términos de seguridad física, se refiere a la protección que tiene el sistema para detectar y contrarrestar la amenaza presentada, antes de que ocasiones daños definitivos.

Por último, los controles correctivos están destinados a generar medidas de control que permitan la reconfiguración de los recursos afectados (Acosta, 2018). Además el surgimiento de este control, es porque los dos controles anteriormente mencionados fueron vulnerables a riesgos. Sin embargo, Morón, Reyes, & Urbina, (2015) señalan que unos correctos controles, ocasionan la disminución o eliminación de cualquier tipo de amenaza, consiguiendo que se evite pérdidas.

1.4. Seguridad de la información

Por la existencia de las Tecnologías de Información y Comunicación (TIC), se ha generado la existencia de controles informáticos, de tal modo que integre una planificación, diseño e instauración de sistemas de información que permitan procesar, almacenar y sintetizar información relevante de manera segura (Castañeda, 2014).

Por esa razón, nacen medidas de seguridad de la información, las cuales deben cumplir con los aspectos de disponibilidad, integridad y confidencialidad.

Asimismo, busca proteger a los activos de información de una empresa, asegurando de que los controles establecidos vayan en relación a los elementos de la información, equipos (software y hardware) y usuarios que hacen uso de las herramientas tecnológicas (ISOTools Excellence, 2015).

También es importante destacar que las TIC han generado un aporte positivo en los centros educativos debido a que han impulsado a mejorar el proceso de enseñanza y aprendizaje (Del Moral, Villalustre, & Neira, 2014). En lo que respecta a la seguridad informática, Quiroz & Macías (2017) reflejan que el propósito es reducir los riesgos al máximo, el cual debe enfocarse a disposiciones organizacionales técnicas, legales, administrativas, y gerenciales. Donde Gil V & Gil J, (2017) hacen referencia que salvaguardar los recursos informáticos permitirá que la entidad logre alcanzar sus objetivos.

2. DESARROLLO

2.1 Metodología

El diseño de esta investigación es de tipo descriptiva, debido a que conlleva a observar y detallar el comportamiento que tiene el objeto de estudio, basándose en la metodología que señalan los siguientes autores. Según Chávez & Vargas, (2016) afirman que para realizar una propuesta del sistema informático para el control interno, es necesario tener claro la descripción del sistema informático; es decir, conocer las características que lo conforman, y el área de ubicación; tomando en cuenta los siguientes aspectos: seguridad, administración, operaciones y los reportes.

Sin embargo, Miranda, Valdés, Pérez, Portelles, & Sánchez, (2016) indican que lo mejor es aplicar una gestión automatizada de controles de seguridad informática, mediante fases como la planificación, implementación y operación y la medición; las cuales se detallarán en la siguiente tabla:

Tabla 1. Fases del proceso de controles de seguridad informática.

Fase 1: planificación	Fase 2: implementación y operación	Fase 3: medición
• Caracterización del sistema de información • Listado de activos informáticos • Reporte de evaluación de riesgos • Políticas de seguridad • Listado de controles	• Manual de procedimientos	• Plan de acciones correctivas • Plan de seguridad informática

Fuente: Miranda et al, (2016)

Por lo consiguiente, las fases propuestas por los autores anteriormente mencionados, servirán como referencia para resolver el problema identificado, de los estudiantes de la Escuela Religiosa Liceo José María Mora del cantón El Guabo, que constantemente están realizando actividades que no están acorde a lo planificado en el programa de las asignaturas que se imparten en ese centro de cómputo, lo que impide que el proceso de enseñanza- aprendizaje se dé con normalidad y de forma adecuada.

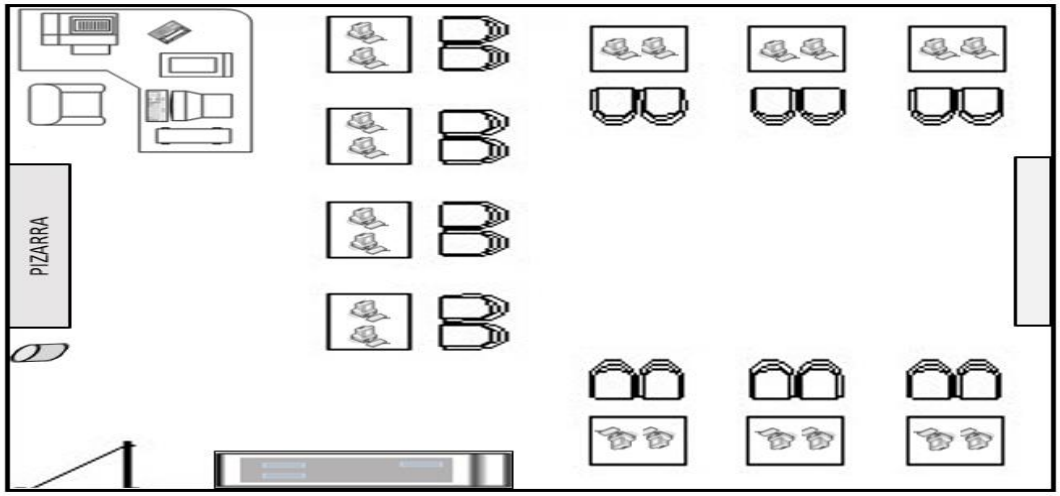
Por ello, se establece en proponer un sistema de control interno informático, el cual se determinarán pasos, a partir de ciertos lineamientos que se expusieron anteriormente en la metodología.

2.2 Propuesta de un Sistema de Control Interno Informático

1. Entorno del lugar

En esta etapa, se hace hincapié a la ubicación del centro de computación, donde se mostrará a continuación un esquema gráfico de la distribución física de las instalaciones.

Figura 1. Instalaciones del centro de computación de la Escuela Religiosa Liceo José María Mora.



Elaborado por: Autor

El laboratorio de computación, se encuentra situado en la parte alta de la institución académica, el cual está asignada por un solo responsable como es el Ingeniero en Sistemas Federico Daniel Jaramillo Maza; el cual cumple con las funciones de instructor académico, de administrar la sala, dar soporte y procesamientos a los recursos informáticos que se encuentre en el mismo.

Cabe señalar que esta área, es solo para fines académicos de instrucción primaria, el cual tiene un abastecimiento de 20 personas por curso; donde se imparten conocimientos básicos del paquete de ofimática como es Microsoft Office Word, Excel y Power Point.

2. Configuración del sistema informático

En lo que respecta a los equipos informáticos, estos se encuentran interconectados entre sí; es decir, con redes de área local y la estructura de equipamiento cuenta con un suministro eléctrico de línea independiente del resto de la instalación para evitar interferencias. Además cuenta con una iluminación de 450 lúmenes de distancia del suelo, lo que significa que es la apropiada para el laboratorio y a s vez cuenta con un aire acondicionado. En lo que respecta al sistema operativo cuenta con Windows 7 Ultimate Copyright 2009 Microsoft Corporation, donde sus características específicas se detallan en el anexo 1.

3. **Establecer políticas, normas y procedimientos de seguridad**

Una vez reconocida el área y las características del centro de computación, se procede a detallar las políticas, normas y procedimientos que deben conllevar dicha institución académica para el correcto funcionamiento del sistema de control interno.

Políticas

- Los responsables de cada área, deben garantizar la seguridad de los recursos informáticos y de la información que se genera en su departamento.
- Es responsabilidad de los trabajadores, informar cualquier tipo de riesgo o daño que se presente en las instalaciones de la escuela.
- Ningún usuario podrá mover o reubicar los equipos de cómputo, siempre y cuando no tenga la debida autorización del director encargado de la escuela.
- Cada área deberá llevar un registro de inventario de los aparatos electrónicos que contiene.
- Los trabajadores que dispongan del manejo de un ordenador, deben revisar que esté en óptimas condiciones e informar cualquier falencia.
- Las peticiones de información por parte de sujetos internos o externos deben estar notificadas mediante un oficio dirigido hacia el rector/a de la institución académica.
- La unidad educativa garantizará la seguridad de la información de todos los empleados y estudiantes.

Normas

Las siguientes normas son para aplicarlas en el laboratorio de computación, de tal forma que se cumpla con lo establecido en el sistema de control interno.

- El laboratorio debe mantenerse en un entorno limpio y sin humedad.
- El ingreso de los estudiantes al centro de cómputo será únicamente con la persona encargada, de tal forma como está establecido en el horario de clases.
- El docente responsable debe encargarse de que los estudiantes conozcan las instrucciones de uso de los ordenadores, con el fin de evitar riesgos por mal uso.

- Se prohíbe el ingreso de alimentos y bebidas al laboratorio por seguridad de los equipos.
- Revisar constantemente que los cables de conexión, estén en buen estado y no sean pisados o aplastados por otros objetos.
- Llevar inventariado los recursos informáticos de forma que se detalle el estado en que se encuentran.
- Realizar mantenimientos a los ordenadores en un lapso de cada 6 meses.
- Supervisar el funcionamiento del sistema operativo para prevenir fallas.
- Examinar que la configuración de los programas estén acorde a las características del software.
- Revisar cada año que el programa de antivirus este actualizado y su función sea la correcta**.**
- Llevar un registro de todos los cambios, fallas o actualizaciones que se han generado en los ordenadores.
- Almacenarse por duplicado los programas y archivos que están en los ordenadores.
- Ejercer medidas de control a los usuarios para constatar qué tipo de actividades o información operan.
- Los usuarios deben responsabilizarse de todos los dispositivos que utilicen dentro del centro de computación.
- Solo el docente a cargo debe encargarse de la actualización del software en un lapso de cada 5 años.
- El docente, es responsable de la información que se maneje en el centro de cómputo, en el cual después de 3 años serán eliminados para precautelar la seguridad del laboratorio.

Procedimientos

1. Procedimiento para el ingreso a los laboratorios por parte del docente y estudiantes.

- El docente, primero debe registrar su hora de entrada en la huella biométrica
- Procede a solicitar al conserje abrir el laboratorio de computación.

- El responsable debe revisar el horario de clase para saber a qué curso le corresponde impartir clases.
- Luego el encargado, de ir a ver a los alumnos al curso para posteriormente llevarlos al laboratorio de computación.
- El docente debe tomar la respectiva lista de asistencia y llenar un formato de manera manual, donde indicará los siguientes campos:
    - Parte superior (encabezado): Logo y nombre de la institución, nombre del docente, fecha y el curso con su respectivo paralelo.
    - Cuerpo: Número de estudiante, nombres y apellidos, número de computadora y observaciones.
    - Parte inferior (Final): Firma del encargado del área con su número de cédula.

2. Procedimiento para realizar mantenimiento físico a los ordenadores.

- Para realizar el respectivo mantenimiento no se debe portar joyas.
- Debe asesorarse que el ordenador este desconectado.
- Utilizar las herramientas necesarias y de manera organizada.
- Mantener ordenadamente cada pieza desarmada.
- Se procede a realizar el respectivo mantenimiento del ordenador.
- Luego debe revisar que estén en buen estado los conectores internos.
- Finalmente armar cada pieza del ordenador.
- Cuando se termine de realizar el mantenimiento, tiene que llenarse un formulario donde indique los siguientes aspectos:
    - Datos del equipo: Marca, procesador y modelo
    - Características del hardware
    - Detalle del mantenimiento: Fecha, número de computadoras, detalles del mantenimiento, observaciones
    - Firma del responsable del área.

3. Procedimiento para solicitar nuevos hardware o software.

- Realizar un comunicado mediante un oficio a la máxima autoridad del plantel educativo indicando el requerimiento de nuevo computador.

- Debe considerarse el presupuesto destinado para el área informática del laboratorio.
- Revisar que los recursos informáticos contengan características adaptables al sistema operativo.
- Para constancia de la petición de un nuevo hardware o software debe llenar un formulario que contenga los siguientes campos:
    - Datos generales: Fecha, identificación del responsable
    - Detalles específicos: Cantidad, descripción, marca, estado (gama alta, gama media y baja) y las observaciones.
    - Firma del personal encargado.
- El responsable del área se encargará de adquirir el respectivo hardware o software.

4. Procedimiento para la instalación del software.

- Llenar un formulario estableciendo los requisitos técnicos del software, en el cual se detalla el sistema operativo que necesita la computadora, el procesador, la memoria RAM, disco duro.
- El docente tiene que verificar que dicho software esté en óptimas condiciones.
- Procederá analizar las políticas de seguridad del sistema operativo.
- Finalmente, ejercer la instalación del respectivo software.

4. Definir controles preventivos, detectivos y correctivos

Tabla 2. Controles preventivos, detectivos y correctivos.

Detalle	Controles preventivos	Controles detectivos	Controles correctivos
Normas	• Socializar las normas con los estudiantes.	• Seguimiento a la normativa para constatar su cumplimiento.	• Modificación de las políticas según a las necesidades de la institución.

Ingreso de alimentos	• Colocar afiches de prohibición de alimentos en la sala de computación. • Controlar en el ingreso al laboratorio, que ningún alumno ingrese comida o bebidas.	• El docente realice supervisiones en el laboratorio durante la ejecución de la clase.	• Establecer sanciones en el promedio de conducta con una disminución de 3 puntos por razones de que los alumnos ingresen alimentos y bebidas.
Protección de los ordenadores	• Instalación de alarmas • Detectores de humo • Protectores de voltaje • Extintores manuales de incendios • Mantenimiento de los sistemas informáticos.	• Sensores de temperatura • Supervisar las instalaciones del laboratorio • Implementar el programa McAfee Security Scan Plus para diagnosticar el estado del ordenador.	• Realizar seguimientos y controles al uso de los recursos. • Ejecutar plan de contingencia ante los riesgos fortuitos.
Protección de las aplicaciones y programas	• Implementar un antivirus como Avast Free Antivirus.	• El programa indique alertas de amenazas en las computadoras • Detecte errores en el funcionamiento aplicaciones y programas.	• Se emitan reportes automáticos de lo que ocasiono la ejecución de ese error y solucionarlo.

Seguridad de la información	• Crear dos cuentas de usuario, una de administrador (docente) y la otra de invitado (estudiantes).	• Diseñar un programa de monitoreo mediante un experto informático, donde establezca una configuración que detecte cuando un usuario sin autorización, esté accediendo a los archivos restringidos.	• Restaurar los datos de información de los ficheros dañados o perdidos.
Ingreso del docente a las instalaciones del laboratorio	• Tener una puerta con cerradura adecuada a manera que solo el responsable pueda acceder al laboratorio.	• El conserje inspeccione que el laboratorio se encuentre con la persona responsable.	• Sancionar al docente responsable con el 5% de descuento del salario que recibe, en caso que esté ausente en su jornada de trabajo.

Elaborado por: El autor

Todo este diseño de controles, ayudará a que la institución académica mejore el desarrollo de sus actividades, lo cual permitirá un manejo sincronizado con la malla curricular establecida, logrando cumplir sus objetivos propuestos.

3. CONCLUSIONES

Del presente trabajo investigativo se concluye, que la aplicación de un sistema de control interno en la Escuela Religiosa Liceo José María Mora del cantón El Guabo, permitirá llevar una correcta administración de los sistemas informáticos, de tal modo que le ayudará a brindar un mejor desarrollo de sus actividades. Por esa razón, se establecieron cuatros pasos puntuales para desarrollar dicho sistema de control, el cual conllevo describir la entorno del centro de computación como las instalaciones físicas, ubicación y responsable del área, al segundo paso configuración del sistema informático, donde se detalló minuciosamente las características del hardware y software, posteriormente se establecieron las políticas, normas y procedimientos; y por último los controles preventivos, detectivos y correctivos.

En lo que respecta a las políticas, normas, y procedimientos, es importante tener claro que para la formulación de las mismas, deben estar acordes a las operaciones que se manejan en el centro de cómputo para que así evitar riesgos. Además estas normas van dirigidas hacia el responsable del área, donde él se encargará de ejercer el cumplimiento de cada una de ellas, para mantener la seguridad de la información y de los recursos informáticos.

Otro punto importante son los controles preventivos, detectivos y correctivos, donde se determinaron bajo el concepto de la norma, teniendo como enfoque a la protección física y lógica de las computadoras, seguridad de la información como también del docente responsable. Cada punto detallado tiene como fin salvaguardar los recursos informáticos mediante el seguimiento, instauración de programas como Avast Free Antivirus, McAfee Security Scan Plus y la creación de un programa de monitoreo por medio de un experto informático, que ayuden a detectar el acceso de usuarios sin autorización hacia los archivos restringidos.

BIBLIOGRAFÍA

Acosta, D. (2018). Categorización funcional de los diferentes tipos de controles de seguridad y su aplicabilidad en la estrategia de protección corporativa. *Revista SIC: ciberseguridad, seguridad de la información y privacidad, 27*(130), 122-124. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6474305

Castañeda, L. (2014). Los sistemas de control interno en las Mipymes y su impacto en la efectividad empresarial. *En Contexto*(2), 129-146. Obtenido de http://ojs.tdea.edu.co/index.php/encontexto/article/view/139

Chávez, J., & Vargas, L. (2016). Propuesta de un sistema de control interno para el área de caja en la empresa "Exclusividades Cielito", de la ciudad de Yurimaguas, 2016. *Accounting, 1*(2), 17-39. Obtenido de https://revistas.upeu.edu.pe/index.php/ri_apfb/article/view/887/855

Estupiñán, R. (2015). *Control interno y fraudes: análisis de informe COSO I, II y III con base en los ciclos transaccionales.* (Tercera ed.). Bogotá, Colombia: Ecoe Ediciones.

Fombona, J., Vázquez, E., & Reis, J. (2016). Los problemas de los recursos informáticos en el contexto universitario. *Revista Iberoamericana de Ciencia, Tecnología y Sociedad, 11*(32), 145-163. Obtenido de https://www.redalyc.org/articulo.oa?id=92445928009

Gil V, V., & Gil J, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia et Technica Año XXII, 22*(2), 193-197. doi:http://dx.doi.org/10.22517/23447214.11371

González, J., Myer, R., & Muñoz, W. (2017). La evaluación de los riesgos antrópicos en la seguridad corporativa: del Análisis Modal de Fallos y Efectos (AMFE) a un modelo de evaluación integral del riesgo. *Revista Científica General José María Córdova, 15*(19), 269-289. doi:http://dx.doi.org/10.21830/19006586.81

Huapaya, J. (2017). *Repositorio académico USMP*. Obtenido de El control interno en la gestión adminitrativa de las instituciones educativas privadas de educación básica regular en el distrito de Lince, 2016:

http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/3174/3/huapaya_fjj.pdf

ISOTools Excellence. (21 de Mayo de 2015). *ISO 27001: ¿ Qué significa la seguridad de la información?* Obtenido de ISOTools Excellence: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

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. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2227-18992016000200002

Morón, A., Reyes, M., & Urbina, Á. (2015). Gestión de riesgos en la empresa R.C. Agelvis, C.A. *Multiciencias, 15*(4), 417-427. Obtenido de http://www.redalyc.org/articulo.oa?id=90448465008

Orjuela, M. (2016). Elaboración de SAGRLAFT para las empresas vigiladas por la Superintendencia de Sociedades, obligadas a reportar a la UIAF. *Apuntes contables*(18), 9-29. Obtenido de https://revistas.uexternado.edu.co/index.php/contad/article/view/4663

Portal, J. (2016). Control interno e integridad: elementos necesarios para la gobernanza pública. *El Cotidiano*(198), 7-13. Obtenido de http://www.redalyc.org/articulo.oa?id=32546809002

Quinaluisa, N., Ponce, V., Muñoz, S., Ortega, X., & Pérez, J. (2018). El control interno y sus herramientas de aplicación entre COSO y COCO. *Cofin Habana, 12*(1), 268-283. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2073-60612018000100018

Quiroz, S., & Macías, D. (2017). Seguridad en informática: consideraciones. *Dominino de las Ciencias, 3*(1), 676-688. doi:http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.5.agos.676-688

ANEXOS

Anexo A. Características de las computadoras del laboratorio de computación de la Institución Educativa.

ESPECIFICACIONES DE LA COMPUTADORAS	
HARDWARE	
Número de computadoras	• 20 computadoras (Estudiantes) • 1 computadora (Docente)
PC	• Disco Duro 16 GB • Unidad de CD-ROM o DVD-ROM • Memoria RAM 2 GB • Procesador Intel Core i3-2100 • Adaptador de vídeo y monitor con una resolución Súper VGA (800 x 600) o mayor. UPS- Forza FX 1500
Periféricos de entrada	• Teclado Genius- Interfaz del dispositivo USB, Diseño de teclado QWERTY • Mouse Genius- Tipo de Mouse Óptico, Diseño estándar, Interfaz USB, Resolución (dpi) 800 /1200
Router	• Router inalámbrico N 300Mbps TL-WR841ND • Velocidad inalámbrica de 300 Mbps y Control de ancho de banda basado en IP, fácil Encriptado de la seguridad inalámbrica al presionar el botón QSS.
Cables	• Cable PS/2 y cable mini din (Teclado y Mouse) • Cable serial (Modem externo- Escáner) Cable monitor. • Cable par trenzado (Conexión a una red) • Cable HDMI (Monitor, Pantalla, y Proyector) • Cable Energía eléctrica
SOFTWARE	
Sistema operativo	Windows 7 Ultimate Copyright 2009 Microsoft Corporation

Programas	
Paquete Ofimática	Microsoft Office 2007- Versión Service Pack 3 (2011) Incluye los siguientes componentes: • Microsoft Word (Procesador de texto) • Microsoft Excel (Planilla de cálculo/hoja de cálculo) • Microsoft PowerPoint (Programa de presentaciones de diapositivas) • Microsoft Access (Programa de bases de datos) • Microsoft Publisher (Editor para crear varios tipos de publicaciones como tarjetas, pancartas, etc.) • Microsoft Project (Gestor de proyectos) • Microsoft Outlook (Agenda y cliente de correo electrónico y cuentas software)
Otros Programas	• Adobe Reader XI. versión 11.0.13 (2015) • Adobe Acrobat XI versión 11.0.12 (2015) • Adobe Flash Player versión 18.0.0.324 (2015) • Software antivirus ZoneAlarm • Nero Classic (2015) • VLC Media Player • Windows Internet Explorer • Skype • USB Disk Security • Google Chrome • FireFox • Navegador Opera • Papelera reciclaje