



# UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO  
PARA LOS LABORATORIOS DE COMPUTACIÓN DE LA UAIC DE LA  
UTMACH

JAPON ALBUJA PRISCILA ALEXANDRA  
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA  
2019



# UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES  
CARRERA DE CONTABILIDAD Y AUDITORÍA

PROPUESTA DE UN SISTEMA DE CONTROL INTERNO  
INFORMÁTICO PARA LOS LABORATORIOS DE COMPUTACIÓN  
DE LA UAIC DE LA UTMACH

JAPON ALBUJA PRISCILA ALEXANDRA  
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA  
2019



# UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES  
CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA LOS  
LABORATORIOS DE COMPUTACIÓN DE LA UAIC DE LA UTMACH

JAPON ALBUJA PRISCILA ALEXANDRA  
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 23 DE AGOSTO DE 2019

MACHALA  
23 de agosto 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 LOS LABORATORIOS DE COMPUTACIÓN DE LA UAIC 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.



---

GONZALEZ SANCHEZ JORGE LUIS  
0703333898  
TUTOR - ESPECIALISTA 1



---

CHIMARRO CHIPANTIZA VICTOR LEWIS  
0703703413  
ESPECIALISTA 2



---

ILLESCAS ESPINOZA WILMER HENRY  
0704128776  
ESPECIALISTA 3

## Urkund Analysis Result

**Analysed Document:** PRISCILA APÓN.docx (D54792341)  
**Submitted:** 8/13/2019 4:50:00 AM  
**Submitted By:** jgonzalez@utmachala.edu.ec  
**Significance:** 3 %

Sources included in the report:

<https://www.gestiopolis.com/control-interno-segun-coso/>

Instances where selected sources appear:

1

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

La que suscribe, JAPON ALBUJA PRISCILA ALEXANDRA, en calidad de autora del siguiente trabajo escrito titulado PROPUESTA DE UN SISTEMA DE CONTROL INTERNO INFORMÁTICO PARA LOS LABORATORIOS DE COMPUTACIÓN DE LA UAIC 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 disposiciones 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, 23 de agosto de 2019



JAPON ALBUJA PRISCILA ALEXANDRA  
0704249838

## **RESUMEN**

La sociedad del conocimiento se gesta en el intercambio de información, siendo indispensable contar con sistemas informáticos para gobernar las TIC`s en cada aspecto cotidiano, solventado varias tareas en forma interdisciplinaria como salud, educación, trabajo, entidades gubernamentales, empresas o cualquier institución capaz de interactuar digitalmente. La Universidad Técnica de Machala emplea en su tarea de formar a profesionales herramientas y plataformas virtuales, a través de sistemas computacionales y derogar sus potencialidades principalmente en ordenadores, donde se simulan procesos didácticos o laborales mediante modelos informáticos; estas facultades expresan condiciones adversas en términos de seguridad e integridad, debido a su conexión a internet, falta de cultura en protección de datos y comportamiento del cuerpo estudiantil quienes son el eje entorno al cual se desarrollan las competencias académicas, organizacionales e institucionales de las carreras ofertadas por la UTMACH. El presente proyecto tiene el objetivo de proponer un sistema de control informático esquematizando sus componentes e inferencias de operación para mejorar la administración/uso de los ordenadores en el centro de cómputo de la Unidad Académica de Ingeniería Civil, evidenciando que su implementación traerá consideraciones relevantes en el aprovechamiento de las TIC`s para fines educativos.

**Palabras Clave:** Auditoría informática, control interno, centro de cómputo, sistemas.

## **ABSTRACT**

The knowledge society is gestated in the exchange of information, being essential to have IT systems to govern ICT`s in every day aspect, solving several tasks in an interdisciplinary way such as health, education, work, government entities, companies or any institution capable of to interact digitally. The Technical University of Machala employs in its task to train professionals and virtual platforms, through computer systems and derogate their potential mainly in computers where didactic or work processes are simulated by computer models; These faculties express adverse conditions in terms of security and integrity, due to their connection to the Internet, lack of data protection culture and behavior of the student body who are the axis around which academic, organizational and institutional competences of careers are developed. offered by the UTMACH. The present project has the objective of proposing a computer control system schematizing its components and inferences of operation to improve the administration / use of computers in the computer center of the Civil Engineering Academic Unit, evidencing that its implementation will bring relevant considerations in the use of ICTs for educational purposes.

**Keywords:** Computer audit, internal control, computer center, systems.

## ÍNDICE DE CONTENIDOS

portada	1
Índice De Contenidos	5
Índice De Ilustraciones	5
Índice De Cuadros	6
1. Introducción	7
1.1 Metodología	8
1.1.1 Investigación Bibliográfica:	8
1.1.2 Análisis De Contenidos:	8
1.1.3 Inductivo-Deductivo:	8
2. Desarrollo	9
2.1 Fundamentación Teórica	9
2.1.1 Seguridad Informática Y De La Información	9
2.1.2 Control Interno	9
2.1.3 Vulnerabilidades Y Amenazas En Centros De Cómputo	10
2.1.4 Herramientas O Software De Control En Centros De Cómputo	11
2.1.4.1 Cyberadmin 5	11
2.1.4.2 Control De Ciber	11
2.1.4.3 Tenaxsoft	12
2.1.4.4 Help Desk	12
2.1.5 Plan De Control Interno	12
2.1.6 Identificar Riesgos Y Variables A Controlar	13
2.1.7 Modelo De Gestión Aplicable	14
2.1.8 Método Para Automatizar Y Sistematizar El Control Interno	15
2.1.9 Diagrama De Flujo Del Proyecto	15
3. Conclusiones Y Recomendaciones	16
Referencias Bibliográficas	18

## ÍNDICE DE ILUSTRACIONES

<b>Ilustración 1</b> El conocimiento científico	9
<b>Ilustración 2</b> Rol de las TIC`s en territorio ecuatoriano	13
<b>Ilustración 3</b> Esquematización de la propuesta	16

## ÍNDICE DE CUADROS

<b>Cuadro 1</b> Principales riesgos informáticos en empresas	10
<b>Cuadro 2</b> Matriz de riesgos en el centro de cómputo de UAIC	14

## 1. INTRODUCCIÓN

Los sistemas de comunicación e información permiten solventar necesidades cotidianas inherentes del ser humano, el manejo de grandes cantidades de datos ha facilitado el desarrollo de las ciencias, mejora en las prestaciones sociales y optimizado los negocios en forma revolucionaria, transformando la forma en que se interactúa con el medio laboral e interpersonal gracias a las bondades computacionales.

La auditoría informática hoy en día es un proceso constante, encargado de mantener la eficiencia, seguridad, disponibilidad e integridad de la información; mantenimiento al mismo los riesgos a un costo razonable para la organización; además su dualidad al retroalimentar los hallazgos o eventualidades garantiza una filosofía de mejora continua en todos los mecanismos internos de la empresa (Caycedo-Casas, 2017).

Las exigencias contemporáneas conllevan a innovar en las ciencias educativas, desarrollar competencias profesionales con flexibilidad y adaptabilidad a la hora de distribuir o construir conocimientos; el uso de las TIC`s han trastocado el contexto académico dotando de medios e insumos virtuales para potenciar las destrezas de la relación alumno-docente acorde a los cambios vertiginosos que la globalización ha impuesto tanto a la vida personal como en sociedad e incluso profesional (Hernández, 2017).

Los centros de cómputo son la infraestructura esencial de cualquier institución educativa para utilizar las potencialidades de las TIC`s, debido a que facilitan a los estudiantes de un ordenador equipado con los componentes físicos y lógicos afines a las cátedras de especialidad, permiten modelar situaciones reales mediante softwares de simulación; pero también debe contar con las consideraciones necesarias al garantizar la calidad de los procesos como acceso a internet, instalaciones electrónicas/eléctricas/datos e implementos de seguridad computacional (Gamboa, 2016).

La protección de datos en toda es un derecho tanto del ser humano como de las organizaciones, cuya secuencia es la siguiente:

- Encriptado de contraseñas, rangos de seguridad y gestión de acceso por llaves lógicas
- Concientizar al personal, dotar de control, monitorea, disciplina y vigilancia
- Implementar procedimientos de auditoría, seguimiento, respaldo, sensibilidad e integridad en medios digitales
- Cumplir con las normativas legales y técnicas vigentes a nivel nacional e internacional (CARVAJAL, 2018)

La UTMACH particularmente en la Unidad académica de Ingeniería Civil ha designado varios laboratorios de cómputo para el aprendizaje de cátedras técnicas como informática, Matlab, NTIC`s, dibujo digitalizado, métodos numéricos y otras áreas que demandan recursos lógicos en su desarrollo; por lo tanto, se debe ejercer una metodología de control para mantener las virtudes en sus instalaciones, minimizar los riesgos e integrar consideraciones que mejoren el desempeño institucional mediante la auditoría informática.

## **1.1 METODOLOGÍA**

Comprenden las técnicas utilizadas para obtener, procesar e interpretar información, se esquematiza a través de una triangulación dialéctica para estructurar una secuencia lógica al dirimir los criterios u opiniones versados este estudio.

### **1.1.1 Investigación Bibliográfica:**

Se basa en indagar en documentos publicados sobre la temática y en la misma línea de investigación, para argumentar teóricamente el desarrollo del proyecto; se debe sintetizar la información apreciada en base a las variables de interés, haciendo hincapié en el estado de arte alcanzado en trabajos académicos similares (Pineda Acero, Cervera Muñoz, & Oviedo García, 2017).

### **1.1.2 Análisis de contenidos:**

Consiste en realizar comparaciones entre los componentes de un sistema de información, para inferir su conducta, determinar cómo interactúan y en qué grado se relacionan en forma contextual; esto permite estructurar la investigación en función de los puntos clave como es la seguridad informática y métodos de control en centros de cómputo, con el objeto de dar una solución eficiente a cualquier problema abordado (Pulido Polo, 2015).

### **1.1.3 Inductivo-deductivo:**

En un proceso trascendental en la construcción del conocimiento, gracias a que permite analizar las partes de un caso conflictivo relacionando la interacción entre sus variables específicas, para luego analizar su comportamiento conjunto denotando leyes o hipótesis generales entorno al estudio; en si compone una técnica lógica y precisa usada desde la antigüedad al inferir saberes partiendo de lo general a lo particular o viceversa (Jiménez & Jacinto, 2017).

La estructura científica de una investigación se resume en forma genérica, en la siguiente figura.



interno conjugando personal-marca en forma sistemática (Carrión, Morales, Jaramillo, & Peña, 2018).

Los componentes del control interno son:

- “Ambiente de Control
- Evaluación de Riesgos
- Actividades de Control
- Información y Comunicación
- Supervisión o Monitoreo” (Washington Alfredo Camacho Villota, 2017).

### 2.1.3 Vulnerabilidades y amenazas en centros de cómputo

El primer término son todas las posibles entradas a un agente externo que podría causar daños al sistema, generalmente son las debilidades desatendidas como ignorar estándares de seguridad, conducta inapropiada o intervención de terceros; las amenazas son los factores que consuman el riesgo como hackers, virus, ebot, desastres naturales o eventos imprevistos que vulneran al sistema (Benitez & Martínez, 2018).

Las principales vulnerabilidades informáticas se resumen en el *cuadro 1*.

**Cuadro 1 Principales riesgos informáticos en empresas**

Activos	Amenazas	Vulnerabilidades
Documentación física	Incendio, robo o pérdida	No existir sistema contra incendios ni de respaldo
Personal	Enfermedades	Falta de seguimiento y seguro social
Servidores	Hackers	Puertos abiertos innecesariamente
Antivirus	Virus	Falta de antivirus o desactualización de los mismos
Software de facturación	Alteración de datos	Bajo nivel de seguridad en bases de datos
Bases de datos	Pérdida de información	Falta de back up
Instalaciones eléctricas/conexiones	Descarga eléctrica, variación de voltaje	Falta de mantenimiento y equipos de protección
Sistema Contable	Fraude interno	Falta de empoderamiento a empleados
Firewall	Carencia de actualización	Falta de actualizaciones periódicas
LAN	Pérdida de comunicación	Falta de plan de contingencia
Internet	Pérdida de conexión	Falta de protocolo de seguridad
Equipos tecnológicos	Daño de hardware	Falta de mantenimiento preventivo

**Fuente:** (Tejena-Macías, 2018)

#### **2.1.4 Herramientas o software de control en centros de cómputo**

Las tecnologías informáticas por si solas han impulsado el desarrollo de la humanidad, dando la capacidad de dinamizar la información, gestionar fácilmente los saberes técnicos o especializadas, además de permitir controlar en tiempo real un sin número de actividades, analizar datos o inferir resultados en base a premisas lógicas; las TIC`s deben integrarse a todos los procesos corporativos para maximizar su potencial a la vez que mantienen una disciplina interna a través de medidas tanto lógicas como físicas (software como servicio/regular al personal) (Cano-Pita, 2018).

Los programas de control más comunes actualmente son:

##### **2.1.4.1 CyberAdmin 5**

Es un software versátil e íntegro, permite regular contenido web, guardar sesiones, monitorear actividades, visualizar flujos de caja y datos remotamente e incidir directamente en los ordenadores con alertas incluidas; sus principales beneficios son:

- “Control Impresiones
- Control Escaneos
- Control Grabaciones
- Punto de Venta
- Acceso Remoto
- Alertas y Bloqueos USB
- Control de Consolas
- Control Remoto de PCs
- Filtro de Contenido: Control anti-porno.
- Guardar Partidas (Arcus©)
- Programa de puntos” (CyberAdmin, 2019)

##### **2.1.4.2 Control de ciber**

Es un software de licencia *free*, en español que incorpora varias funcionalidades configurables a las necesidades del centro de cómputo, algunas son:

- Ajusta parámetros de tiempo, mensajería, notificaciones y bloqueo de pantalla
- Impide la ejecución de programas, uso de ordenadores y gestionar paquetes de datos
- Protege los datos por claves, permite reiniciar los ordenadores y sincronizar a todos con el servidor local
- Permite guardar sesiones y actualizar automáticamente los programas seleccionados
- Impide cambio en configuración de los ordenadores

- Genera reportes periódicamente (Fuentes, 2017)

#### **2.1.4.3 TenaxSoft**

Con su programa *CyberPlanet* es una solución completa, eficiente y rentable; proporciona criterios al cobrar, administrar o gestionar cualquier centro de cómputo o inclusive escalable a negocios pequeños; proporciona dos versiones gratuita y pagada; actualmente es el software líder en Latinoamérica, sus potencialidades son:

- Sistema funcional y eficiente
- Soporte real en línea o asesoría técnica disponible
- Controla impresiones, escaneos, tarifas, reportes y grabaciones de seguridad
- Gestiona videojuegos, programas, estados
- Manejo remoto y reportes continuos
- Estado de caja, configuración de ordenadores, venta remota y publicidad (TenaxSoft, 2018)

#### **2.1.4.4 Help Desk**

Es un proceso de gestión en infraestructura informática; sustentado en un conjunto de recursos tanto técnicos como humanos, facilita dar soporte a distintos tipos o privilegios de usuarios, conforma una entidad logística adaptable a cualquier necesidad, mejora la estructura organizacional y desempeño, gracias a que retroalimenta tareas/proceso mediante análisis visibles del desarrollo empresarial; además es de licencia libre siendo favorable para su uso en instituciones públicas (Gallardo, Madrid, & Cárdenas, 2018).

#### **2.1.5 Plan de control interno**

Es importante mantener la calidad y seguridad dentro de un establecimiento académico, donde el uso de las TIC`s ha optimizado los procesos pero contrae riesgos al entorno educativo; la información como tal debe ser protegida, sin embargo por sí sola no expresa peligro dependiendo del factor humano como incertidumbre en los sistemas de control; haciendo imperioso que un profesional capacitado regula las variables pertinente es el centro de cómputo manteniendo orden a través de la disciplina (Mosquera, Verdesoto-Arguello, & Vargas-Marín, 2017).

### **Ilustración 2 Rol de las TIC`s en territorio ecuatoriano**



**Fuente:** (Linzán, Santacruz, & Yáñez, 2018)

En un sistema de control interno se deben incluir los siguientes módulos:

- Comunicación, vigilancia y seguridad
- Control de documentos
- Control de riesgos
- Control de procesos
- Distribución de políticas y responsabilidades
- Auditoría, monitoreo y revisión por la dirección
- Retroalimentar medidas en función de objetivos estratégicos (Secaira, Salvatierra, & Zamora, 2016)

El proceso para plantear un sistema de control, sustentado en los hallazgos dormidos e inferencias apreciadas en investigaciones comparadas es delineado a continuación:

### ***2.1.6 Identificar riesgos y variables a controlar***

Se aprecia que los mayores riesgos derivan del factor humano, el comportamiento de los estudiantes al manipular las máquinas, realizar tareas o irrespetar las normativas del centro de cómputo; por ello se debe disciplinar a los usuarios mediante charlas o capacitaciones que concienticen sobre el uso adecuado de las bondades TIC`s; también tratar de culturizar sus responsabilidades acatando las políticas de la Dirección de TIC`s desarrolladas por la UTMACH como principal dependencia de control tecnológico en la institución.

Esto da las pautas que debe tener la plataforma de control, además de prevenir riesgos mantenimiento los equipos e instalaciones en orden bajo la supervisión de un profesional competente.

Se resumen a través del *cuadro 2*, visitando y entrevistando al personal/estudiantes de UAIC.

**Cuadro 2 Matriz de riesgos en el centro de cómputo de UAIC**

<b>Riesgos</b>	<b>Solución</b>
Virus, malware, códigos maliciosos	Antivirus, escaneos continuos, congelar estado de ordenadores
Daño de equipos e instalaciones	Mantenimiento preventivo, renovar equipos en mal estado
Robo de información o periféricos	Sanciones disciplinarias y control mediante inventarios
Manipular la configuración de los ordenadores	Software de control para restaurar al estado original
Falta de capacitación o implementos tecnológicos	Contratar a personal especializado y adoptar medidas cloud computing
Acceso remoto, hackers o intrusiones al sistema	Cortafuegos, dominio propio, monitoreo del tráfico en datos y puertos IP
Suplantar identidad, secuestros de sesión	Contraseñas fuertes y encriptar claves
Presupuesto insuficiente para renovar infraestructura lógica y digital	Derogar fondos públicos y alquilar servicios rentables
Poca diversidad y control en aplicativos virtuales	Implementar soluciones informáticas adaptables e integradas

**Fuente: Elaboración Propia**

### **2.1.7 Modelo de gestión aplicable**

Es necesario esquematizar las necesidades a resolver y deducir los componentes del sistema, para que al interactuar conjuguen un sistema de control interno capaz de optimizar el uso de los centros de cómputo, dicha fases son:

*Inicio del sistema:* Usuario ingresa por contraseñas fuertes, desde módulo Situmach o autenticación con correo institucional

*Control de seguridad:* Actualizar antivirus, mantener estado del sistema, inventariar activos digitales, cortafuegos e IP protegidas

*Control de activos físicos:* Inventarios, alertas en caso de desconectar un periférico o usb, registro de software, configuraciones y monitoreo en red interna

**Control de conductas:** Filtrar contenido inapropiado, sestear configuraciones seguras en la intranet, impedir ejecución de softwares no autorizados y monitorear en tiempo real uso de ordenadores

**Control de riesgos:** Minimizar pérdidas de información, daños o amenazas en base a una gestión integral y holística en forma interdisciplinaria con las actividades tanto académicas como administrativas

**Retroalimentar:** Comunicación dinámica entre sistema y coordinadores, para enviar reportes o alertas en tiempo real, facilitando una respuesta inmediata

**Plan de contingencia:** Tener un orden estructural basado en un plan contra imprevistos es esencial en el control de cualquier ámbito, en especial para gestionar los fondos y permisos necesarios en la implementación del proyecto

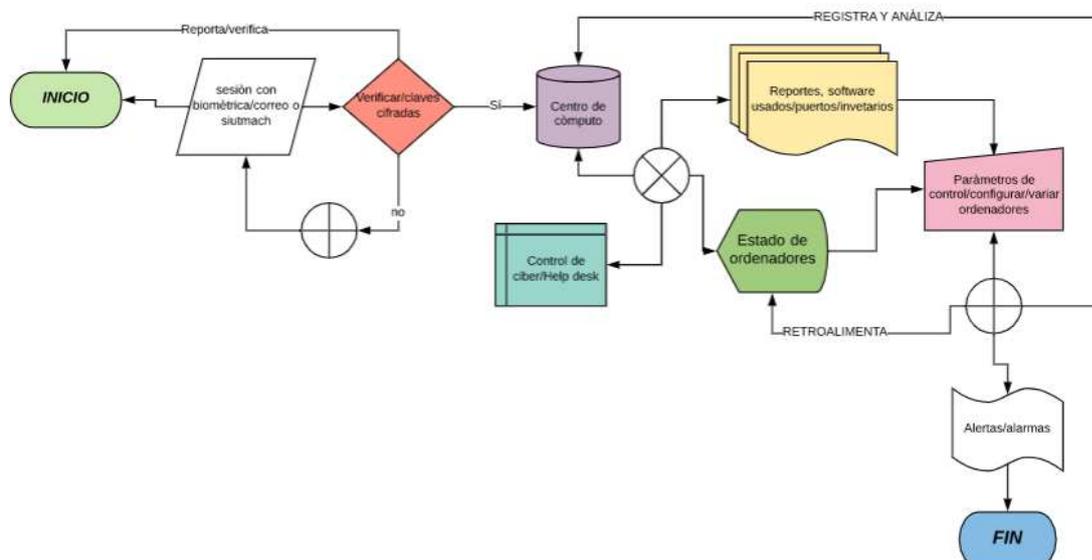
### 2.1.8 Método para automatizar y sistematizar el control interno

Se aconseja implementar la metodología SCADA (Supervisión, Control y Adquisición de Datos), gracias a que es escalable a cualquier organización y adaptable a las necesidades; en conjunto con el software *control de ciber* y *help desk* se pueden automatizar varias funciones en tiempo real, además de poder solicitar a la carrera de ingeniería de sistemas que diseñe un programa de soporte para mejorar las prestaciones del centro de cómputo e incluso se anexe como módulo al SIUTMACH para los docentes encargados.

### 2.1.9 Diagrama de flujo del proyecto

La secuencia lógica del sistema de control se describe en la *ilustración 3*; recalcando que puede anexarse al *Siutmach* o desarrollarse mediante código libre para amalgamar a las plataformas virtuales de la UTMACH.

**Ilustración 3 Esquemización de la propuesta**



**Fuente:** Elaboración Propia

### **3. CONCLUSIONES Y RECOMENDACIONES**

El sistema de control informático puede coadyuvar en el proceso de aprendizaje, manteniendo la disciplina interna, así mismo mejora la seguridad y niveles de privilegios a estudiantes restringiendo limitando el uso hacia actividades académicas, además es una herramienta que optimiza la toma de decisiones gracias a que audita los centros de cómputo en tiempo real.

El análisis de los riesgos, identificar procesos e integrar funcionalidades de control mediante software libre, permite implementar este sistema en todos los laboratorios e incentivar el control interno como medio de empoderamiento institucional; además automatiza tareas secuenciales y permite desarrollar planificaciones, basadas en datos reales del comportamiento estudiantil en respuesta al sistema dentro de un contexto regulado por las autoridades.

La implementación del proyecto depende de la acogida por parte de las autoridades competentes, pueden encomendar su desarrollo a la Dirección de TIC`s e incluso anexarlo como módulo al SIUTMACH, gracia a que será una herramienta docente para controlar los centros de cómputo en la UAIC, además mejorará el desempeño estudiantil e incitará a usar los ordenadores en forma adecuada y con la disciplina necesaria que demanda la institución.

El mayor problema es la conducta estudiantil, debido a que es la debilidad más inherente y difícil de controlar; por lo tanto, a más de medidas lógicas se recomienda dar charlas para concientizar sobre el uso adecuado de las máquinas, capacitarlos para entender el potencial de las TIC`s en el enriquecimiento cognitivo; además las medidas preventivas a través de alertas en el software de control favorecen una respuesta rápida por parte del personal encargado.

## REFERENCIAS BIBLIOGRÁFICAS

Benitez, Y. N., & Martínez, N. S. (2018). Requisitos de Seguridad para aplicaciones web. *Revista Cubana de Ciencias Informáticas, Vol 12.*, 205-221.

Cano-Pita, G. E. (2018). Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones. *Dominio de las Ciencias Vol. 4, núm. 1*, 499-510.

Carrión, P. A., Morales, L. O., Jaramillo, F. Y., & Peña, J. N. (2018). El control interno como herramienta indispensable para una gestión financiera y contable eficiente en las empresas bananeras del cantón Machala (Ecuador). *Espacios Vol. 39 (Nº 03)*, 30.

CARVAJAL, E. T. (2018). TECNOLOGÍAS, SEGURIDAD INFORMÁTICA Y DERECHOS HUMANOS . *IUS ET SCIENTIA (ISSN: 2444-8478), Vol.4, nº 1*, 19-39.

Caycedo-Casas, D. A.-F. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias Vol. 3*, 157-173.

CyberAdmin. (2019). *CyberAdmin 5*. Obtenido de <http://www.cyberadmin.net/>

Fuentes, O. (2017). *Control de ciber*. Obtenido de <http://www.cbm.com.ar/>

Gallardo, J. A., Madrid, M. C., & Cárdenas, A. E. (2018). Estudio sobre la implementación del software Help Desk en una institución de educación superior. *Paakat: Revista de Tecnología y Sociedad, Año 8, Núm. 14*, 1-20.

Gamboa, P. d. (2016). Las TIC en la gestión del proceso de enseñanza-aprendizaje en el área Comunicación Organizacional: licenciatura en Ciencias de la Comunicación . *Revista Iberoamericana para la investigación y el desarrollo educativo, Vol. 8, Núm. 16*, 1-25.

Hernandez, R. M. (2017). Impacto de las TIC en la educación: Retos y Perspectivas. *Propósitos y Representaciones, Vol 5, No 1.*, 325-347.

Jiménez, A. R., & Jacinto, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista EAN, 82*, 179-200.

Linzán, J. F., Santacruz, M. R., & Yáñez, J. F. (2018). CREACION DE UN INFOCENTRO PARA EMPRENDIMIENTOS AUTO SUSTENTABLES EN COMUNIDAD INDIGENA CEPLOA – ASIA. *Revista Científica investigar, Vol 2, No 21*, 125-144.

Mosquera, F. W., Verdesoto-Arguello, A. E., & Vargas-Marín, H. J. (2017). Software de seguridad que permita la confidencialidad de los datos del sistema de gestión y servicios académicos para planteles de educación media (SiViSA). *Dominio de las Ciencias Vol. 3, núm. 3*, 91-107.

Pineda Acero, J. A., Cervera Muñoz, A., & Oviedo García, W. (2017). Revisión bibliográfica de la aplicación de la metodología DEA en Colombia por actividad económica. *Civilizar. Ciencias Sociales y Humanas, vol. 17, núm. 32*, 133-160.

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

Quiroz-Zambrano, S. M. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, Vol. 3, núm. 1*, 676-688.

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*, 1-26.

Secaira, J. I., Salvatierra, J. X., & Zamora, P. N. (2016). Sistema informático de Gestión de Calidad para las empresas. *Revista Publicando, 3(8)*, 52-58.

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo del Conocimiento, Vol 3, No 4.*, 230-244.

TenaxSoft. (2018). *CyberPlanet*. Obtenido de <https://tenaxsoft.com/ventajas.html>

Washington Alfredo Camacho Villota, D. J. (2017). Sistema de control interno: Importancia de su funcionamiento en las empresas. *Revista Observatorio de la Economía Latinoamericana, Ecuador*.