UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LAS METODOLOGÍAS DE LA AUDITORIA INFORMÁTICA PARA EVALUAR LA SEGURIDAD DIGITAL EN LA UTMACH.

PAREDES CASTRO BYRON OSWALDO
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2020

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LAS METODOLOGÍAS DE LA AUDITORIA INFORMÁTICA PARA EVALUAR LA SEGURIDAD DIGITAL EN LA UTMACH.

PAREDES CASTRO BYRON OSWALDO
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2020

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE LAS METODOLOGÍAS DE LA AUDITORIA INFORMÁTICA PARA EVALUAR LA SEGURIDAD DIGITAL EN LA UTMACH.

PAREDES CASTRO BYRON OSWALDO
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 21 DE FEBRERO DE 2020

MACHALA
21 de febrero de 2020

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado ANÁLISIS DE LAS METODOLOGÍAS DE LA AUDITORIA INFORMÁTICA PARA EVALUAR LA SEGURIDAD DIGITAL EN 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

PARRA OCHOA EUDORO BENITO
0701063406
ESPECIALISTA 2

OCHOA CAICEDO HECKLER ROTHWELL
0702681917
ESPECIALISTA 3

Fecha de impresión: viernes 21 de febrero de 2020 - 12:36

ANÁLISIS DE LAS METODOLOGÍAS DE LA AUDITORIA INFORMÁTICA PARA EVALUAR LA SEGURIDAD DIGITAL EN UNIVERSIDADES NACIONALES

por Byron Oswaldo Paredes Castro

Fecha de entrega: 10-feb-2020 11:06p.m. (UTC-0500)
Identificador de la entrega: 1255241512
Nombre del archivo: BYRON_OSWALDO_PAREDES_CASTRO.pdf (104.65K)
Total de palabras: 2441
Total de caracteres: 13495

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

El que suscribe, PAREDES CASTRO BYRON OSWALDO, en calidad de autor del siguiente trabajo escrito titulado ANÁLISIS DE LAS METODOLOGÍAS DE LA AUDITORIA INFORMÁTICA PARA EVALUAR LA SEGURIDAD DIGITAL EN 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.

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

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

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

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

Machala, 21 de febrero de 2020

PAREDES CASTRO BYRON OSWALDO
0704914738

RESUMEN

Hoy en día la humanidad se encuentra en la sociedad del conocimiento, caracterizada por las prestaciones y facilidades sustentada en medios digitales; sin embargo, existen riesgos paralelos a sus cualidades como corrupción de datos e información, fallos del sistema, pérdida de acceso, entre otros capaces de afectar a instituciones o empresas indistintamente. Por lo tanto, es de suma relevancia contar con un protocolo o normativa al auditar la seguridad de los sistemas informáticos con la meta de mantener en óptimas condiciones el desempeño organizacional, desarrollar competitividad y evitar posibles ataques tanto externos como internos. El objetivo general del presente trabajo es Analizar las metodologías de auditoria informática para evaluar la seguridad digital de la Universidad Técnica de Machala; el enfoque es explorativo y superficial basado en información bibliográfica sobre los procesos al detectar vulnerabilidades en contraste con las medidas apreciadas en la UTMACH. La metodología aplicada es el análisis comparativo al dirimir criterios sobre las distintas maneras de auditar una institución educativa, diagnosticar debilidades, proponer controles e identificar cual metodología se ajusta mejor a los requerimientos de la UTMACH. En los resultados se explican las comparaciones entre procesos de auditoria, se justifica la elección de las normativas ISO como modelo de seguridad y propone una serie de pasos para su futura implementación a nivel organizacional.

Palabras clave: Auditoria Informática, metodologías, seguridad, evaluación.

ABSTRACT

Today humanity is in the knowledge society, characterized by the benefits and facilities supported by digital media; however, there are risks parallel to its limitations such as data and information corruption, system failures, loss of access, among other damages of affecting institutions or companies interchangeably. Therefore, it is very important to have a protocol or regulation when auditing the security of computer systems with the goal of maintaining organizational performance in optimal conditions, developing competitiveness and avoiding possible external and internal attacks. The general objective of the present work is to analyze the computer audit methodologies to evaluate the digital security of the Technical University of Machala; the approach is exploratory and superficial based on bibliographic information about the processes when detecting vulnerabilities in contrast to the measures appreciated in the Utmach. The methodology applied is the comparative analysis when deciding criteria on the different ways of auditing an educational institution, diagnosing weaknesses, proposing controls and identifying methodological qualification best fits the requirements of the Utmach. The results explain the comparisons between audit processes, justify the choice of ISO standards as a security model and propose a series of steps for future implementation at the organizational level.

Keywords: Computer Audit, methodologies, security, evaluation.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

1. INTRODUCCIÓN

El mundo moderno en el que se vive actualmente ha logrado dotar de tecnología a la humanidad, con la cual facilita la ejecución de muchas tareas incluso de las más sencillas.

Con la adopción de tecnologías para formar parte de las actividades realizadas a diario, el hombre se ve expuesto a cientos de peligros que atentan contra las vulnerabilidades que los sistemas informáticos. Con el fin de contrarrestar esto se debe tener un plan de gestión de riesgos que permita tener un mayor control y de esta manera fortalecer la seguridad informática.

Ante esta situación se aplican auditorias informáticas utilizando diferentes metodologías con las cuales es posible analizar y evaluar la seguridad digital de una institución, estas auditorías permiten determinar el nivel de riesgo que existe en la institución y las fallas por mal manejo o por intrusos en el sistema; con los resultados obtenidos se puede tomar decisiones precisas respecto a la correcta gestión de seguridad digital o las medidas que pueden tomarse para combatir los problemas informáticos que hay o podrían haber.

En esta investigación se pretende analizar las metodologías que se emplean en la auditoria informática al momento de evaluar el ejercicio de un sistema informático.

Los objetivos específicos que delinean el proyecto son:

- Caracterizar las diversas metodologías de auditoria informática mediante una revisión literaria para fundamentar epistemológicamente el estudio.
- Diagnosticar vulnerabilidades y riesgos en los sistemas informáticos de la Utmach mediante las diversas metodologías para comparar los hallazgos
- Analizar las diversas metodologías de auditoria informática por medio de una matriz de riesgos para evaluar la seguridad digital en la Utmach

El alcance del proyecto es seleccionar la mejor metodología acorde al contexto de la Utmach, caracterizar las vulnerabilidades informáticas y dar un valor cualitativo a los riesgos en sus sistemas, con el objeto de proponer mejoras e instaurar un modelo de auditoria institucional en lo referente a seguridad computacional.

2. DESARROLLO

En el texto que continua se explican algunas conceptualizaciones referentes al tema en cuestión; mediante la investigación bibliográfica realizada en diferentes fuentes y bases de datos se ha logrado extraer la información necesaria con la que se plantea y resuelve el caso práctico que da solución al problema planteado.

2.1 Marco teórico:

En esta parte se explica la parte teórica de la investigación a través de conceptos formados a través de información recopilada mediante el método investigativo.

2.1.1 ¿Qué es una Auditoría Informática?

Para definir el término auditoría existen muchos criterios pero todos llevan a lo mismo, el significado común que se puede apreciar es el de que consiste en un proceso de la organización que se encarga de revisar su funcionamiento, las actividades que ha realizado y los recursos que ha utilizado para ello, determinando así el estado de la entidad (Carrión, Mendoza, & Vera, 2017).

En todo proceso de auditoría es importante que exista un plan previo a su ejecución, en este se debe colocar los procedimientos que se piensan seguir para recoger la información necesaria que les permita analizar el estado de la organización y finalmente emitir un juicio.

Cuando se trata de una auditoria informática se realiza el mismo conjunto de procesos, con el ligero cambio de que se aplican específicamente a los sistemas informáticos de las organizaciones, es decir a los servidores y a la información; con el fin de verificar que todo marche en orden y acorde a lo planificado inicialmente.

Es así que una auditoria pasa a formar parte de la organización, es un miembro mas debido a la importancia que adquiere al ser una actividad mediante la cual es posible detectar fallas en el sistema informático que bien podrían prevenirse, o reducir el impacto que generarían si se hallan a tiempo, podría también servir de ayuda para establecer un plan de manejo integral de riesgos y amenazas informáticas (Hernández, 2016).

Una auditoria consta de una serie de componentes que deben cumplirse, estos se explican a mediante el *cuadro 1.*

Cuadro 1. *Componentes de una auditoría.*

Componente de una auditoría	
Ambiente de control	Actitud del personal que influye en los resultados de la auditoría
Valorar el riesgo	Es el reconocimiento y estudio de los riesgos presentes en la organización
Actividades de control	Sistemas de manejo integral aplicadas por el personal de la empresa
Información y comunicación	Proporciona información en el menor tiempo posible que permite cumplir con las actividades de la empresa
Monitoreo	Es un proceso que califica la ejecución de los controles informáticos de acuerdo al tiempo y forma de aplicación

Fuente*: (Hernández, 2016)*

La aplicación de esta metodologia es con el fin de controlar y vigilar si existen peligros en el sistema; además de controlar que los procesos efectuados por la organización se estén cumpliendo bajo los protocolos establecidos por la empresa (Cevallos, Moreno, & Chávez, 2018).

2.1.2 Seguridad digital de Universidades.

Hoy en día son muchas las personas que tienen acceso a la tecnología y al internet; el uso del internet posibilita la realización de muchas actividades relacionadas a cualquier área. La era tecnológica brinda grandes oportunidades, pero así mismo despierta el interés de ciber atacantes que ven en la tecnología, la oportunidad de robar información confidencial para luego utilizarla a su favor.

En el ámbito estudiantil, se conoce que los estudiantes universitarios están relacionados muy estrechamente con la tecnología, pues es el principal gestor de la información y del conocimiento informático (Castillejos, Torres, & Lagunes, 2018).

Cabe destacar que al considerar la enorme cantidad de prestaciones que ofrece el internet a los usuarios, genera también riesgos que deben ser manejados con procesos de control especializados.

Competencia	Descripción
Protección de los dispositivos	Proteger los dispositivos propios y comprender los riesgos y amenazas en red; conocer medidas de protección y seguridad.
Protección de datos personales	Entender los términos habituales de uso de los programas y servicios digitales; proteger activamente los datos personales; respetar la privacidad de los demás; protegerse a sí mismo de amenazas, fraudes y ciberacoso.
Protección de la salud	Evitar riesgos para la salud relacionados con el uso de la tecnología en cuanto a amenazas para la integridad física y el bienestar psicológico.
Protección del entorno	Tener en cuenta el impacto de las TIC sobre el medio ambiente.

***Ilustración 1**. Seguridad a entornos digitales.*

***Fuente:** (Castillejos, Torres, & Lagunes, 2018)*

Al momento que un usuario decida entrar al internet y navegar, este debe contar con un alto grado de seguridad que garantice confiabilidad y confidencialidad de la información. Para mantener este nivel de seguridad informática se han desarrollado unos métodos que permiten proteger la integridad de la información a través de codificación de archivos (Amaro & Rodríguez, 2016).

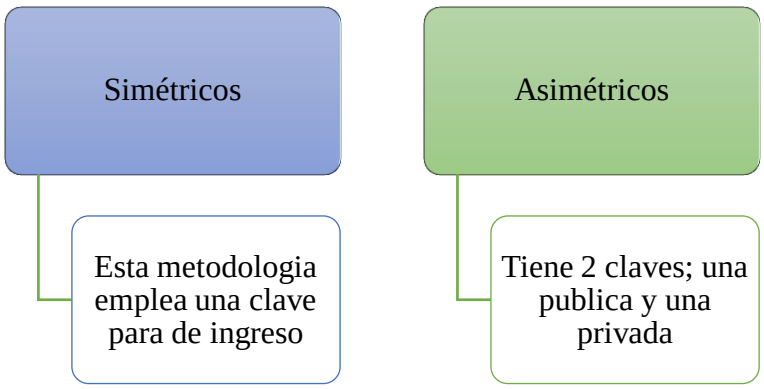

***Ilustración 2**. Métodos de seguridad informática.*

***Fuente**: (Amaro & Rodríguez, 2016)*

2.1.3 Evaluación de seguridad digital.

La seguridad informática se caracteriza por ser la encargada de minimizar y mantener al menor nivel posible los riesgos informáticos, para que las demás actividades realizadas por la entidad se realicen con total normalidad (Quiroz & Macías, 2017).

Como bien se sabe, la seguridad informática es muy importante dentro de la institución y mediante el uso de las herramientas adecuadas, esta ayuda a que la institución cumpla sus objetivos propuestos protegiendo sus recursos y sistemas. La gestión de la seguridad informática corresponde a un proceso importante y exigente, pero una vez que este proceso se gestione correctamente se tendrá protegido el sistema informático de la empresa y libre de peligros que atenten contra su bienestar (Gil & Gil, 2017).

Para conocer si la gestión de la seguridad informática va bien, es necesario realizar una evaluación que conste de una serie de estrategias y técnicas que ayuden a detectar el estado del sistema informático, verificando que esté funcionando bajo las normativas establecidas (Voutssas, 2010).

2.1.4 Normativa ISO 27001.

Esta normativa ha tenido gran acogida a nivel mundial, pues corresponde a la importancia de la seguridad informática en las organizaciones (Valencia & Orozco, 2017).

Para implementar una norma de este tipo en una institución es importante conocer la forma estándar y su estructura.

La normativa ISO 27001 contiene los requerimientos necesarios para determinar un sistema de gestión de seguridad informática; al igual que otras normas, ésta se puede aplicar a cualquier tipo de institución sin importar su función, busca la constante mejora de la organización por lo que resulta factible integrarla a los sistemas de gestión de la empresa (Chilán & Pionce, 2017).

Esta normativa sugiere realizar controles de seguridad periódicamente con el fin de conservar la confidencialidad e integridad de la información y así poder insertar la seguridad informática a la organización y a las actividades que aquí se efectúan (Arcentales & Caycedo, 2017).

2.2 Caso Práctico:

Comprende el proceso de resolución de la parte práctica, aplicar los conocimientos adquiridos en la catedra en forma técnica y objetiva, para demostrar el dominio del tema e inferencias cognitivas en el ejercicio profesional.

2.2.1 Componentes de la seguridad digital

De acuerdo a los pre textos teóricos, consideraciones de las metodologías e indicaciones técnicas sus elementos son:

- Seguridad de redes
- Seguridad de datos e información
- Continuidad de los servicios
- Seguridad del usuario (estudiantes, docentes y personal)
- Auditorias regulares y retroalimentar el proceso

Desde el enfoque de la auditoria se sintetiza en los siguientes pasos:

1. Identificar debilidades, amenazas y riesgos

2. Valores riesgos, activos a proteger y relación causa/efecto
3. Implementar controles físicos y lógicos
4. Medir la efectividad de las medidas de seguridad aplicadas
5. Repetir el proceso denotando una filosófica de mejora continua

Los aspectos que integran la cultura en seguridad informática, en las instalaciones de la Utmach son:

- Normativas y protocolos de seguridad
- Monitoreo y socialización de riesgos
- Aplicación de políticas de seguridad institucionales
- Herramientas e instrumentos al detectar, valorar o tomar acciones contra ataques y amenazas

En breves rasgos se comprime los aspectos más notables al estructurar la seguridad informática, dando a conocer que el departamento de TIC`s es el encargado de gestionarla, las dependencias administrativas de controlar los riesgos en sus procesos y los estudiantes de acatar dichas directrices.

2.2.2 Características de las metodologías de evaluación

Al comparar los diversos modelos de auditoria, se encontraron los criterios expuestos en el siguiente cuadro.

Cuadro 2. *Análisis de las características de las metodologías para auditar la seguridad digital*

METODOLOGÌA	**CARACTERISTICA**
COBIT 5	Se basa en eficiencia, calidad y cumplimiento de los objetivos organizacionales; sus requerimientos son confidencialidad e integridad auditando datos, aplicaciones, tecnologías y recurso humano.
OWASP	Realiza un análisis de las amenazas lógicas de forma anónima (caja negra) y un hackeo ético para interactuar profundamente con la plataforma
NORMAS ISO 27001	Busca calidad e integridad de datos, su proceso es definir políticas, análisis y gestión de riesgos, aplicar controles, revisar e implementar un plan holístico.
Dpto. Dirección de TIC`s (Utmach)	Impone políticas de seguridad, acuerdos de confidencialidad y delega a estudiantes/personal la detección e implementación de controles; no coordina ni gestiona solo delinea el proceso.

Fuente: *Elaboración Propia*

2.2.3 Criterios para valorar los riesgos informáticos

Se toman los riesgos detectados en el campus, no existen indicios de hackeos o alguna eventualidad destacable que vulnero al sistema; pero no es razón para dejar de lado la seguridad, el *descuido* es el mayor peligro según las metodologías estudiadas.

Cuadro 3. *Criterios para valorar los riesgos informáticos en la Utmach*

NIVEL DE RIESGO	**DESCRIPCIÒN DEL RIESGO**
Muy alto	No contar con metodología propia, no realizar auditorías ni prevenir daños severos al sistema
Alto	Fallos en el sistema, perdida de datos, intromisiones, alteración de las plataformas
Regular	Fallos en las redes e internet, perdidas menores de datos
Bajo	No se socializa las políticas de seguridad, no se toman medidas respecto a los riesgos
Muy bajo	Se perciben daños sin relevancia y el sistema funciona sin mayor novedad

Fuente: Elaboración Propia

Se simplifican los análisis, debido a que los riesgos causados por información personal, errores de estudiantes o fallos humanos son incalculables y exigen más que un control, un cierto grado de consciencia sobre su papel dentro del sistema organizacional de la Utmach; además no se registran ni programas ni proyectos en esta área, por lo cual se deduce no existen fondos o actividades relacionadas.

2.2.4 Análisis y Resultados

Las semejanzas entre las metodologías concuerdan en la auditoria es un *proceso* multiobjetivo, de carácter sistemático e interdisciplinario concatenando etapas de identificación, valoración, implementación y control de los riesgos; no obstante, la Utmach para dominar los conceptos, pero no la parte práctica al hacer notar un monitoreo constante de la seguridad. Todas buscan proteger los datos e información, pero no dan la misma importancia al usuario como veedor, responsable o ejecutor de los respectivos controles.

Las diferencias entre metodologías es el *enfoque* de las amenazas, unas valoran más la tecnología y recursos lógicos, otras el talento humano y la ISO integra todo en una filosofía de mejora continua, a opinión personal esta se ajusta mejor a los requerimientos de la Utmach.

En conclusión, la normativa ISO 27001 es la que mejor se adapta al contexto organizacional, pero existe un paradigma puesto que, si se aplican controles, imponen políticas, sanciones y recomendaciones a escala general; pero no se evidencian análisis, informes o acciones conjugadas a favor de preservar la seguridad informático o al menos investigar en el área para planificar una auditoria completa que permita explotar las potencialidades de los mecanismos computacionales.

3. CONCLUSIONES:

En virtud de los criterios u opiniones expresados en la documentación pertinente se concluye lo siguiente:

- Las características de las metodologías son dinámicas e intrínsecas a los ámbitos de desempeño institucional, como activos informáticos, hardware y personal en forma paralela a su aplicación en los procesos académicos e institucionales; la Cobit resalta talento humano, la Oswap ataques lógicos externos e Iso 27001 estructura una filosofía de seguridad transversalmente enfocada al proceso; en contraste con la dirección de TIC`s que delega políticas y responsabilidades indistintamente acorde a los riesgos, pero sin darle seguimiento o auditorias regulares.
- Los riesgos encontrados son variados, siendo el más significativo la falta de una metodología sistemática en términos de seguridad; pese a conocer los procesos de auditoria, imponer políticas y contar con normativas no se observa una aplicación rigurosa en la Utmach, indicando que la gestión de riesgos es cuestión personal y de segundo plano sin realizar estudios o planes; por lo tanto, se deduce que es un asunto de formalidad no de cultura en protección de datos, además tampoco se hallaron evidencias de fallos ni ataques que vulneren sus sistemas.
- Analizando las metodologías de auditorías conocidas se concluye que la más adecuada es la normativa ISO por ser dinámica, retrospectiva e interactiva con todos los implicados en la seguridad informática, elevando la protección de datos a una filosofía continua de mejora y evaluación; también se dirime que la seguridad digital es *BAJA* no por la falta de controles o políticas ni por la ausencia de connatos, sino porque de acuerdo a la literatura la ausencia de procesos normados, acciones debidamente concatenadas y un monitoreo constante es la verdadera causa de la inseguridad, es decir no darle la importancia correspondiente, es el mayor riesgos porque la seguridad no es un concepto o ausencia de peligros, es un proceso constante en toda organización sin importar las circunstancias.

4. REFERENCIAS BIBLIOGRÁFICAS

Valencia, F., & Orozco, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista lbérica de Sistemas e Tecnologias de Información*, 73-88.

Amaro, J., & Rodríguez, C. (2016). Seguridad en internet. *Paakat: Revista de Tecnología y Sociedad*, 2-10.

Arcentales, D., & Caycedo, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias*, 157-173.

Carrión, H., Mendoza, M., & Vera, C. (2017). Importancia de la auditoría interna para el perfeccionamiento de los niveles eficiencia y calidad en las empresas. *Dominio de las Ciencias*, 908-920.

Castillejos, B., Torres, C., & Lagunes, A. (2018). La seguridad en las competencias digitales de los millennials. *Apertura*, 54-69.

Cevallos, D., Moreno, C., & Chávez, Á. (2018). LA AUDITORÍA INTERNA COMO HERRAMIENTA EFECTIVA PARA LA PREVENCIÓN DE FRAUDES EN LAS EMPRESAS FAMILIARES. *Revista Científica de la Universidad de Cienfuegos*, ISSN: 2218-3620.

Chilán, E., & Pionce, W. (2017). Apuntes teóricos introductorios sobre la seguridad de la información. *Dominio de las Ciencias*, 284-295.

Gil, V., & Gil, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*, 193-197.

Hernández, O. (2016). La auditoría interna y su alcance ético empresarial. *Actualidad Contable Faces*, 15-41.

Quiroz, S., & Macías, D. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias*, 137-156.

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