CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año V. Vol. V. N°1. Edición Especial. 2019
Hecho el depósito de ley: pp201602FA4721
ISSN-L: 2542-3029; ISSN: 2610-802X
Universidad Nacional Experimental Francisco de Miranda (UNEFM). Santa Ana de Coro. Venezuela

Oswaldo Alejandro Zhañay Soliz; Juan Carlos Erazo Alvárez; Cecilia Ivonne Narváez Zurita

DOI 10.35381/cm.v5i1.271

Modelo de Auditoria de Sistemas de Información para las Cooperativas de ahorro y crédito del segmento 1, 2, y 3, de la ciudad de Cuenca

Information Systems Audit Model for Savings and Credit Cooperatives of segment 1, 2, and 3, in the city of Cuenca

Oswaldo Alejandro Zhañay Soliz
ozhanays@psg.ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca
Ecuador
https://orcid.org/0000-0003-2385-1644

Juan Carlos Erazo Álvarez
jcerazo@ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca
Ecuador
https://orcid.org/0000-0001-6480-2270

Cecilia Ivonne Narváez Zurita
inarvaez@ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca
Ecuador
https://orcid.org/0000-0002-7437-9880

Recibido: 7 de septiembre de 2019
Aprobado: 22 de septiembre de 2019

RESUMEN

La auditoría de sistemas de información es un procedimiento que recoge, agrupa y evalúa evidencias de un sistema, y parte de la necesidad de verificar que los sistemas informáticos funcionen correctamente. Las unidades de análisis son las cooperativas de ahorro y crédito del segmento 1, 2 y 3 de la ciudad de Cuenca, que en su mayoría (84.21%) a pesar de contar con Departamentos de Auditoría Interna, carecen de especialistas informáticos, lo que causa inconvenientes al realizar las auditorías de los sistemas de información. Por esta razón, esta investigación se propone desarrollar un

modelo de auditoría que sirva como guía para estas organizaciones. Para lograrlo, se realizó un estudio no experimental, con enfoque mixto, utilizando encuestas para determinar aspectos importantes a considerarse al realizar una auditoría de sistemas de información para luego a través de una comparación de modelos existentes seleccionar aquellos más relevantes que se alinean a la investigación; el resultado es un Modelo de Auditoría a sistemas de información aplicable a las entidades investigadas en este trabajo.

Descriptores: Modelo; Auditoria informática; Coso; Cobit; Sistemas de información; ISO.

ABSTRACT

Information systems auditing is a procedure that collects, groups and evaluates evidence of a system, and part of the need to verify that computer systems work correctly. The analysis units are credit and savings cooperatives of segment 1, 2 and 3 of the city of Cuenca, which mostly (84.21%) despite having Internal Audit Departments, lack IT specialists, which causes inconveniences when performing information system audits. For this reason, this research aims to develop an audit model that serves as a guide for these organizations. To achieve this, a non-experimental study was carried out, with a mixed approach, using surveys to determine important aspects to be considered when performing an information systems audit and then through a comparison of existing models, select the most relevant ones that align to the research. ; The result is an Audit Model for information systems applicable to the entities investigated in this work.

Descriptors: Model; Computer audit; Coso; Cobit; Information systems; ISO.

INTRODUCCIÓN

Porter y Burton, (1981) señalan a la Auditoría como la verificación de información por parte de una tercera persona, distinta de quien la preparó, con la intención de validar su autenticidad, dando a conocer los resultados de esta verificación, para aumentar la utilidad de tal información. La Auditoria es muy antigua y diversa, naciendo principalmente para sistemas contables y financieros, encargándose de la verificación de la información financiera con base en cumplimiento de las normas contables. En el mundo actual debido al avance de las tecnologías de la información nace un nuevo concepto: Auditoria Informática que examina los sistemas e infraestructura informática para encontrar

vulnerabilidades y errores que puedan causar daños a la información y equipos tecnológicos (Florian, 2016).

En las ciudades de Quito y Guayaquil de Ecuador, se encuentran presentes las 5 firmas auditoras más grandes a nivel mundial: Price Waterhouse Coopers, Deloitte, Ernst&Young, KPMG, BDO (Binder Dijker Otte), quienes entre sus principales clientes tienen al Sector Financiero.

Por otra parte, en la era digital que actualmente vivimos los procesos se realizan más fácilmente y con mejor comunicación; sin embargo, esto ha causado un incremento en los delitos informáticos y fraudes, como lo indica la encuesta de 2018 realizada por PWC (Price Waterhouse Coopers) a diferentes organizaciones de 123 países, con 7.228 encuestados, donde muestra resultados que revelan el avance rápido de este tipo de delitos a nivel internacional. Por ejemplo, se determinó que los ciberataques han afectado a 31% de los encuestados a nivel global, señalando el uso del malware 36% y pishing 33% como las técnicas más frecuentes (PWC Peru, 2018).

También el 54% de empresas españolas han sido víctima de algún delito económico, habiendo aumentado este porcentaje casi en un 20% desde 2009. Los encuestados piensan que los ciberataques aumentarían significativamente en los próximos dos años, en número e impacto, debido a la alta complejidad y sofisticación de los métodos de ataque (PWC España, 2018).

Además, una de cada tres empresas indica haber sido víctimas de crímenes económicos, lo cual es una importante preocupación para las organizaciones; y dentro de éstos el 24% corresponden a delitos informáticos (PWC, 2015).

Por lo que respecta al sector financiero, específicamente la banca es de los sectores con mayor digitalización en sus procesos. A diario un creciente número de clientes usan la banca electrónica, realizan sus transacciones en internet, o usan sus dispositivos electrónicos móviles. La ventaja del uso de medios y canales digitales trae consigo nuevos riesgos que tienen que ser evitados minimizando posibles fraudes y ataques tecnológicos.

Por poner un ejemplo, en 2018 hubo ataques a Bancos de México y Chile, quedando claro que las entidades de servicios financieros en América Latina son un blanco para ataques cibernéticos, por lo que estas organizaciones deben estar seguras de tener los recursos técnicos necesarios, personal correctamente capacitado y procedimientos apropiados para la defensa ante delincuentes o delitos cibernéticos (Organizacion de los estados americanos, 2018).

Además, el Estudio del Estado de la Ciberseguridad en el Sector Bancario en América latina y el Caribe realizado por la OEA (2018) determina que los servicios más contratados por las entidades financieras son: pruebas de seguridad 65%, Monitoreo de la Infraestructura de Seguridad 37%, Monitoreo de controles de seguridad 20% y servicios de seguridad en la nube 19%. En el 72% del total de bancos de la región, la Junta directiva recibe aportes periódicos acerca de indicadores y gestión de riesgos de seguridad digital También el 68% del total de entidades bancarias indica que han adoptado normas Information Security Management System (ISMS)-Iso 27001, el 50% han adoptado Control Objetives for Information and Related Technology (COBIT), el 43% del total ha adoptado Information Technology Infrastructure Library (ITIL) & IT Service Management (ITSM) y el 41% del total ha adoptado Payment Card Industry Data Security Standards (PCI-DSS) (Organizacion de los estados americanos, 2018).

Por otra parte, considerando que este trabajo de investigación está dirigido a las Instituciones Financieras de la ciudad de Cuenca, y de manera más específica a las Cooperativas de Ahorro y crédito (entidades del sector popular y solidario) de segmento 1,2 y 3; por tratarse de las instituciones con mayor valor de Activos, y por tanto más propensas a los ataques y pérdida de información; que en la ciudad de Cuenca son en total 19 cooperativas (Superintendencia de Economía Popular y Solidaria, 2013).

Además, en la encuesta realizada a Alta Gerencia, Jefes Departamentales y Personal de TI de las Cooperativas de Ahorro y Crédito, se determinó que no existen empresas auditoras con alta presencia en la ciudad y carecen departamentos internos que se dediquen al control y seguridad de los sistemas de información; sin embargo, existe el

Departamento de Auditoría Interna que no conoce a fondo la forma de realizar una Auditoría de Sistemas de Información; por lo que este trabajo se propone desarrollar un Modelo de Auditoría de Sistemas de Información aplicable a las Cooperativas de Ahorro y Crédito que sirva como guía y pueda adaptarse a sus necesidades, teniendo como fundamento los estándares internacionales más utilizados a nivel mundial en materia de Seguridad Informática.

Importancia de la auditoria informática o auditoria a los sistemas de información en el sector bancario, estándares y marcos de referencia más utilizados

En la actualidad, con la rapidez de avances tecnológicos, el crecimiento de la economía y el volumen de datos producidos, las instituciones deben tener la capacidad de manipular la información de forma segura con el fin de impulsar su desarrollo y continuidad; utilizando como herramienta principal los sistemas de información, que no son otra cosa que una agrupación de componentes dirigidos al procesamiento y gestión de datos e información de diferente formato, producidos para cubrir un objetivo. Estos componentes pueden ser: individuos, actividades, datos y recursos materiales (GestioPolis, 2018).

En lo referente al proceso de Auditoría, Piattini y Peso (2001) señalan que una auditoría con el computador es un procedimiento que recoge, agrupa y evalúa evidencias de un sistema, que parte de la necesidad de comprobar que los sistemas informáticos funcionen correctamente por considerarse la información como uno de los activos más importantes en una empresa. Luego, Piña (2015) define a la auditoria informática como un conjunto de procesos y técnicas que se usan para la evaluación y control de un sistema informático, y puede comprender no solamente la evaluación de equipos, sistemas informáticos o procesos, sino la evaluación en general de los sistemas de información.

Por otra parte, Aguirre Bautista (2005) indica que Auditoria Informática es la revisión que se lleva a cabo sobre los recursos informáticos en una empresa para generar un informe profesional sobre el estado de desarrollo y utilización de dichos recursos. Refiriéndose

por recursos informáticos a: Información, programas o software, Infraestructura y finalmente los recursos humanos.

Así también Lopez (2012) aporta que la auditoría de los sistemas de información tiene como funciones principales vigilar la efectividad del sistema de información, para que llegue a los objetivos con el menor costo, cotejar la ejecución de las leyes y estándares válidos en la institución, vigilar el control interno practicado sobre los sistemas de información que cuida los activos de información de la institución: talento humano, instalaciones, infraestructura tecnológica, sistemas y aplicaciones e información tributaria. También refiere que la metodología de auditoria de sistemas de información consiste en una serie de pasos organizados de manera lógica para culminar de la mejor manera los proyectos de auditoría informática; puede acoplarse a empresas pequeñas, medianas y grandes de cualquier giro de negocio.

Ahora bien, Aguirre Bautista, (2005) determina una metodología general para la auditoria informática cuyos pasos a seguir se numeran a continuación:

1. Investigación previa. Se trata de encuentro con el cliente para conocer las necesidades y características dl al Institución a ser auditada.
2. Planeamiento de la auditoria informática. Aquí se elaboran los planes de trabajo que se efectuarán durante la auditoria a la institución, pues estar constituida por varias etapas, como son: diagnóstico, investigación preliminar, construcción del plan de auditoria informática.
3. Documentación de la auditoria informática. En este paso se obtendrá toda la información sobre la empresa estudiada, es decir la documentación para evidenciar la opinión del auditor. Se pueden usar: cuestionarios, entrevistas, observación, etc.
   3.1. Documentación del software, hardware
   3.2. Desarrollo y manual de estándares
   3.3. Organigrama del área informática

4. Análisis, evaluación y presentación. El análisis puede ser realizado por estadística, la evaluación se refiere al entendimiento por parte de auditor, luego la interpretación y la presentación del informe.
5. Dictamen de la auditoria informática. En el informe es el documento en el cual el auditor coloca el resultado del trabajo realizado, basado en normal propias de cada situación

Por otro lado, Derrien (1994) establece que el objetivo general de una auditoria informática es confirmar la fiabilidad de la herramienta informática y la forma en que es utilizada dicha herramienta. Luego según el Estatuto de Auditoría Informática de la Information Systems Audit and Control Association ISACA (2001) “los objetivos de la función de la auditoría deben brindar a la Dirección de una seguridad razonable que los controles se cumplen, fundamentar los riesgos resultantes donde existían debilidades significativas de control y aconsejar a la Dirección sobre acciones correctivas”

Por su parte Gonzáles (2012) menciona que los objetivos de la auditoría informática son:

- Control de la función informática
- Análisis de eficiencia de los sistemas informáticos
- Verificación de la normativa general de la empresa en el ámbito general informático
- Revisión de la eficiente gestión de recursos materiales y humanos informáticos

Finalmente, Derrien (1994) menciona 4 componentes de la Auditoria informática:

- Verificación de la organización general del servicio.
- Verificación de procedimientos relativos al desarrollo y mantenimientos de las aplicaciones
- Verificación de los procedimientos relativos a la utilización de las cadenas de tratamiento
- Verificación de las funciones técnicas

En lo que se refiere a los enfoques que pueden darse a una auditoría informática, existen tres que son los más utilizados en la actualidad: R.O.A. (RISK ORIENTED APPROACH) o Enfoque Orientado al Riesgo, el CHECKLIST o Lista de Verificación y la AUDITORIA

DE PRODUCTOS (por ejemplo, Red Local Windows NT; sistemas de Gestión de base de Datos DB2; paquete de seguridad RACF, etc.) (Lopez, 2012).

Finalmente es necesario anotar lo mencionado por Magee (2015) y Lopez (2012) en cuanto a que existen a nivel internacional organizaciones reconocidas por sus aportes con el desarrollo de Marcos de Referencia y Estándares para el control y auditoría de sistemas de información son: ISACA Asociación de Auditoría y control de sistemas de información, ISO Organización internacional para la estandarización y NIST Instituto Nacional de Estándares y Tecnología de los Estados Unidos, cuyos productos son los estándares más utilizados por las organizaciones para la implementación de diferentes Sistemas de Gestión y Gobernabilidad de TI como COBIT, COSO, ISO 27000, 22301, 27000, etc.

COBIT

Control Objectives for Information and related Technology, u Objetivos de control para la información y tecnologías relacionadas, es un Marco de Referencia publicado en el año 1996 por ISACA; aunque en sus inicios contaba con herramientas para la Auditoría Informática y la actualidad se encuentra en la versión Nro 5, abarcando inclusive lo referente al Gobierno Corporativo de TI. Se basa en 5 principios y está compuesta por 4 Dominios Principales: alinear, planificar y organizar plan y 32 procesos de estos Dominios (Saavedra y Torres, 2012).

Figura 1
Principios de Cobit 5

Fuente: (Saavedra y Torres, 2012)

ISO 27001

Creadas por el British Standards Institution (BsI), en el año 1995, con el nombre BS 7799, cuyo objetivo era el de brindar un conjunto de buenas prácticas para la gestión de seguridad de la información. Más tarde, en 1999 aparece la segunda parte de la norma BS 7799-2, misma que contiene los requerimientos que debe completar un Sistema de Gestión de Seguridad de la Información; fueron estas dos normativas, las adoptadas por la ISO para llegar a ser la ISO 17799 en el año 2000. Finalmente en el 2002 las normativas adoptaron la filosofía de Sistemas de Gestión (ISO -International Organization for Standardization, 2011).

Por otra parte, Fernández-medina (2006) y Boswell & Bhargava (2014) definen un Sistema de Gestión de Seguridad de la información como un Sistema de Gestión que

busca implementar políticas de control que puedan verificar que la seguridad de la información se esté gestionando correctamente, verificando con frecuencia si los procedimientos, políticas, estrategias, y demás mecanismos que se han implementado están consiguiendo los objetivos planteados.

ISO 27001: ESTRUCTURA

Para empezar es necesario aclarar que la ISO 27001 no obliga a controles de información específicos debido a la enorme variedad de validaciones que pueden ser necesarias en cada organización; las verificaciones sugeridas en la ISO 27002 pueden escogerse según las necesidades y características propias de la institución(IsecT Ltd., s. f.).

Así, la estructura de la norma ISO 27001 (ISO -International Organization for Standardization, 2011), es la siguiente:

Introducción

Alcance

Referencias normativas

Términos y Definiciones

Contexto de la Organización

Comprensión de la organización y su contexto

Comprensión de las necesidades y expectativas de las partes interesadas.

Determinar el alcance del sistema de gestión de seguridad de la información.

Sistema de Gestión de Seguridad de la Información.

Liderazgo

Liderazgo y compromiso

Política

Roles organizacionales, responsabilidades y autoridades.

Planificación

Acciones para abordar los riesgos y oportunidades

Objetivos y la planificación para alcanzarlos seguridad de la información.

Soporte

Recursos

Competencia

Conciencia

Comunicación

Información documentada

Operación

Planificación y control operacional

Evaluación de riesgos de seguridad de la información

Tratamiento del riesgo de seguridad de la información

Evaluación del rendimiento

Monitoreo, medición, análisis y evaluación.

Auditoría Interna

Revisión de Gestión

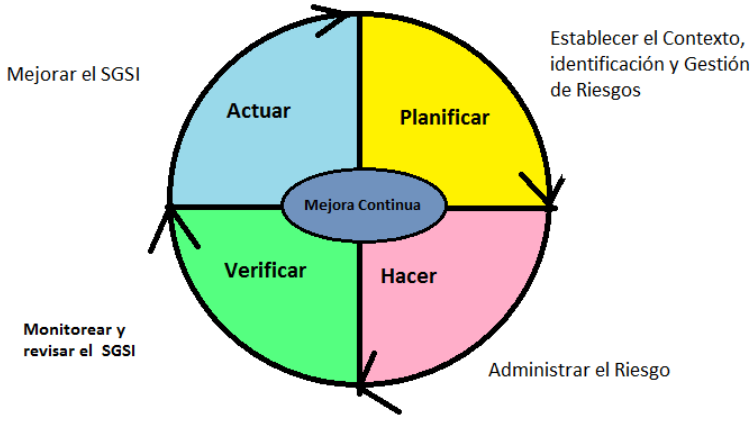
Mejora Continua.

No conformidades y acciones correctivas

Mejora Continua. (Rocano, Narváez, Erazo y Luna, 2019)

El ciclo de vida de la implementación de la norma ISO 27001 está basado en Planear – Hacer – Verificar – Actuar de Demming, y adaptado a la estructura de la normativa (ISO -International Organization for Standardization, 2011).

Figura 1
Implementación de un SGSI con ISO 27001, Copyright (2017)



Fuente: Ellite Certification Ltd.

Como se ha mencionado anteriormente, la ISO 27001 no dicta en sí los controles que se deben implementar en el SGSI, sin embargo, en esto se pueden utilizar la norma ISO 27002.

En el sector público ecuatoriano, es de uso obligatorio la norma INEN ISO 27001, misma que es la traducción exacta de la ISO 27001, realizada por el Servicio Ecuatoriano de Normalización (INEN), con base en la ISO 27001:2013 incluyendo las correcciones Corrigendum 1: 2014 y Corrigendum 2: 2015 (Servicio Ecuatoriano de Normalización, 2016).

ISO 22301

Esta normativa es la primera norma internacional para la Gestión de Continuidad del Negocio, la cual incluye los requerimientos base que permitan recuperarse en el menor tiempo posible de las interrupciones que pueda tener una organización, además de establecer adecuadamente un sistema de Gestión de Continuidad de Negocio (BCMs). La norma aparece por primera vez en el año 1988 con la creación del Diater Recovery

Institute (DRI), y luego en el año 2013 se publica finalmente la primera versión de la norma 22301 (ISO, 2012).

Así pues, la normativa está compuesta por 10 secciones:

1. Ámbito de aplicación
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Apoyo
8. Funcionamiento
9. Evaluación del Desempeño
10. Mejora

Según el objeto de estudio de este trabajo de investigación, es necesario profundizar en el punto 9, que es de competencia de la Auditoría Interna de una organización.

De manera más específica, el apartado 9.2 de la norma indica que: la organización debe realizar auditorías internas en periodos planificados para evaluar el sistema de gestión de continuidad del negocio, y establece que la organización debe:

Planificar, establecer, implementar y mantener un programa de auditoría, incluyendo la frecuencia, método, responsabilidades, requerimientos de planificación y reportaría. El programa de auditoría deberá considerar la importancia de los procesos y los resultados de auditoría previas, Ortega Polanco (2017).

Definir los criterios de auditoría y alcance de cada una de ellas

Seleccionar los auditores y conducirlos para asegurar la objetividad y la imparcialidad del proceso de auditoria

Asegurar que los resultados de las auditorías se reporten a la alta gerencia y

Retener la información documentada como evidencia de la implementación del programa de auditoría y los resultados.

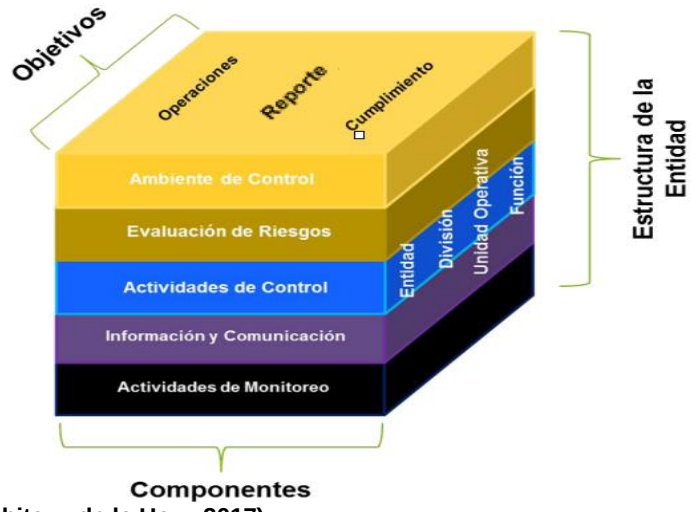
Año V. Vol. V. N°1. Edición Especial. 2019
Hecho el depósito de ley: pp201602FA4721
ISSN-L: 2542-3029; ISSN: 2610-802X
Universidad Nacional Experimental Francisco de Miranda (UNEFM). Santa Ana de Coro. Venezuela

Finalmente, la norma ISO 22301 responsabiliza a la Gerencia del área auditada de asegurarse que cualquier acción correctiva se realice de manera de eliminar cualquier no conformidad detectada y sus causas (ISO, 2012).

COSO

COSO (Commitee of Sponsoring Organization of the Treadway Comission) es un Marco de Referencia desarrollado por el Comité de Organizaciones que patrocinan la comisión de Treadway, se trata de una organización privada de los Estados Unidos que ha desarrollado este marco de referencia como un modelo a seguir de Control Interno para que las organizaciones evalúen sus sistemas de control. De esta forma, el Marco de Referencia COSO se publicó por primera vez en 1992 con 5 componentes de control interno, luego en el 2004 se publica COSO-ERM con 8 componentes de control interno, hasta que en el año 2013 se actualiza el marco de referencia enfocándose más en el reporte no financiero y riesgos de fraude. La normativa consta de 3 objetivos, 5 componentes, 17 principios y 85 puntos de foco. (Cotaña Mier, 2015)

Figura 2
Estructura del marco de referencia COSO 2013



Fuente: (Montaño, Combita, y de la Hoz , 2017)

Luego, los 17 principios se encuentran clasificados como se detalla a continuación:

Ambiente de Control

1. Demuestra compromiso para con la integridad y los valores éticos
2. Ejerce responsabilidad por la vigilancia.
3. Establece estructura, autoridad, y responsabilidad
4. Demuestra compromiso para con la competencia
5. Hace forzosa la accountability

Valoración del riesgo

6. Especifica objetivos confiables
7. Identifica y analiza el riesgo
8. Valora el riesgo de fraude.
9. Identifica y analiza el cambio importante.

Actividades de control

10. Selecciona y desarrolla las actividades de control
11. Selecciona y desarrolla los controles generales sobre la tecnología
12. Despliega mediante políticas y procedimientos.

Información y Comunicación

13. Usa información relevante
14. Comunica internamente
15. Comunica externamente

Actividades de Monitoreo

16. Dirige evaluaciones continuas y/o separadas
17. Evalúa y comunica deficiencias.

Dentro de las Actividades de Monitoreo, COSO brinda ciertos lineamientos que pueden considerarse para conseguir Sistemas de información confiables, válidos y de buena calidad de información: Evaluación de la dependencia entre los procesos, los controles automáticos y los controles generales de TI, Evaluación periódica de la calidad de la información generada por los sistemas (oportuna, actual, precisa, completa, accesible, protegida, verificable y conservada), Diseño y evaluación de actividades de control sobre

la infraestructura de TI; acceso a los sistemas; adquisición, desarrollo y mantenimiento de los mismo. Configuración de los sistemas de información considerando un análisis de Segregación de Funciones. Realización de un análisis costo-beneficio de la implementación de controles de TI. (Castillo, Erazo, Narváez y Torres, 2019)

AUDITORÍA A LOS SISTEMAS DE INFORMACIÓN EN LAS ENTIDADES FINANCIERAS.

Para empezar Piattini y Peso (2001) señalan que la auditoría informática en las entidades bancarias es reciente, por lo que algunas entidades financieras no la tienen implantada o se encuentra en proceso de implementación De forma más específica el aspecto más significativo de la Auditoria informática en el sector financiero es la revisión de las aplicaciones informáticas, debido al alto impacto económico y técnico que puede tener un error detectado en los sistemas de información, y que conllevan a afectaciones importantes en varios ámbitos dentro y fuera de la institución.

También se debe indicar que en la actualidad existen tres metodologías más utilizadas a nivel internacional para realizar una auditoría informática: Risk Oriented Approach (ROA), Checklist y Auditoría de Productos; cualquiera de estas metodologías se sirve de los estándares descritos en el apartado anterior como herramientas para lograr los controles necesarios en una organización (Lopez, 2012).

Así pues, si bien es común realizar una auditoría orientada al riesgo informático, el presente trabajo propone elaborar un Modelo híbrido de Auditoría que se enfoque también en la seguridad de los sistemas de información; haciendo uso de los estándares internacionales más utilizados como Cobit, COSO, ISO 27000 e ISO 22301.

Luego Hernandez Hernandez (1993), Álvarez Basaldúa (2005) y el (Ministerio de Tecnologías & de la Información y las Comunicaciones de Colombia (2016) definen que para realizar una Auditoría Informática es vital seguir lo detallado a continuación:

1. Planeación
2. Familiarización con el Sistema actual

3. Determinar las áreas a auditar
4. Elaborar el análisis de los documentos recopilados
5. Elaborar el Informe de la Auditoría
6. Presentar el Informe a la Gerencia.

Mientras que Piattini y Peso (2001) destacan que una auditoria informática de una aplicación bancaria comprenderá labores de verificación de los procedimientos de recolección e ingreso de datos y de los procedimientos de producción de la información de salida del proceso destinada principalmente a clientes, Rodríguez Rodríguez & Puertas (2017).

METODOLOGÍA

La presente investigación es de tipo no experimental, ya que se propone un Modelo de Auditoria de Sistemas de Información, es decir solo llega hasta el análisis, diseño, no su implementación.

Según el tipo de enfoque esta investigación es mixta, pues presenta elementos tanto cualitativos como cuantitativos. La Investigación cualitativa existe en el análisis de ciertas características del mercado, observación de problemas y vacíos de empresas en el área de Auditoria Informática, lo cuantitativo lo encontramos en el análisis de encuestas, cálculos.

De acuerdo con el tipo de alcance esta investigación fue descriptiva explicativa, descriptiva por cuanto en una primera instancia en el marco teórico a las variables independiente y dependiente se las estudió, y también a sus componentes. Explicativa ya que detectó un vacío en servicios de Auditoria Informática en la ciudad de Cuenca.

La presente investigación es transversal puesto que los datos, como por ejemplo las encuestas serán levantados y evaluados en un solo momento del tiempo.

También se empleó el método histórico Lógico en la revisión de bibliografía y documentación para la conceptualización del marco teórico. La técnica de investigación

usada en la presente investigación fueron Entrevistas, realizadas a diferentes directivos de las Cooperativas, con su instrumento Guía de Entrevista, para el diagnóstico de servicios de Auditoria informática en la Ciudad de Cuenca.

UNIVERSO DE ESTUDIO Y TRATAMIENTO MUESTRAL

Para la presente investigación, se ha seleccionado como población o Universo a las Cooperativas de Ahorro y crédito de la Ciudad de Cuenca del segmento 1, 2 y 3 que según (Super intendencia de Economía Popular y Solidaria, 2019) corresponden al Segmento 1: 7 Cooperativas, al segmento 2: 9 Cooperativas y al Segmento 3 3 Cooperativas, dando un total de 19 Cooperativas, como se puede observar en la Tabla a continuación:

Tabla 1
Cooperativas en Cuenca Segmento 1, Segmento 2 y Segmento 3

Segmento 1	Segmento 2	Segmento 3
- 29 de octubre Ltda	- Educadores Del Azuay Ltda	- Multiempresarial
- Jardín Azuayo Ltda	- La Merced Ltda	- Señor De Giron
- Vicentina Manuel Esteban Godoy Ortega Ltda	- De La Pequeña Empresa Gualaquiza	- Promoción De Vida Asociada Ltda Provida
- Policía Nacional Ltda	- Mas Ahorro Solidario Mascoop	
- De La Pequeña Empresa Biblián Ltda	- Alfonso Jaramillo León Ccc	
- Juventud Ecuatoriana Progresista Ltda	- Coopac Austro Ltda - Erco Ltda - Santa Isabel Ltda. - Crea Ltda	
- Riobamba Ltda		
Total: 7	Total:9	Total: 3

Fuente (Superintendencia de Economía Popular y Solidaria SEPS, 2015)

Para esta investigación la población de cooperativas de ahorro y crédito del segmento 1, 2, y 3 en Cuenca, corresponde a 19 cooperativas, por lo que no se consideró una toma muestral.

RESULTADOS

Luego de realizar una revisión de literatura de los estándares internacionales COBIT 5, ISO 22301, ISO 27000 y COSO; y de los enfoques de la auditoría a los sistemas de información de una entidad financiera, se desarrolló una encuesta dirigida a personal técnico de TI, gerentes y jefes departamentales de las cooperativas de ahorro y crédito del segmento 1, 2 y 3 de la ciudad de Cuenca para determinar los aspectos principales que deben considerarse al realizar un auditoría a los sistemas de información y con ellos elaborar la propuesta de un modelo de auditoría, se obtuvieron los siguientes resultados: El 89.47% de los encuestados señala que cuenta con un Departamento de Auditoría Interna; sin embargo, el 84.21% no tiene personal especialista de Auditoría Informática, y por tal razón al momento de realizar una Auditoría a los Sistemas de Información el 64.82% está dispuesto a contratar personal o empresas externas a la organización especialistas en Auditoría y Seguridad Informática para realizar los controles de los sistemas internos de la organización.

También hay que tomar en cuenta que existe una opinión dividida sobre la efectividad del uso de los sistemas de información para el procesamiento y manejo de los activos de información de una entidad; donde el 33.3% está totalmente de acuerdo en que el uso de herramientas automatizadas puede mantener y mejorar la confiabilidad de la información generada, mientras que el 55% está menos seguro de la efectividad de estas herramientas.

Finalmente, el 74.1% cree que es importante implementar medidas de control, monitoreo, auditorías para verificar la efectividad de las medidas de seguridad informática implementadas y calidad de la información generada.

Por esta razón, el desarrollo de un modelo de auditoría a los sistemas de información resulta altamente beneficioso para las entidades financieras que cuenten con personal dedicado a la Auditoria pero que carece de conocimientos específicos respecto a lo que se debe evaluar en los Sistemas de Información, como es el caso del 89.47% de la población encuestada.

PROPUESTA

Para el desarrollo de esta propuesta de Modelo de Auditoría se ha tomado como base la metodología propuesta por Becker, Knackstedt, y Pöppelbuß (2009) quienes plantean un proceso para desarrollar Modelos de Madurez que podrían aplicar para el caso de esta investigación:

1. Comparación con modelos existentes: se realizó la comparación de los estándares más utilizados: COBIT, COSO, ISO 27001 e ISO 22301.
2. Procedimiento iterativo: se revisaron de manera general cada estándar, y se fueron resaltando los aspectos relevantes de cada uno, que se alinean a los resultados de la encuesta realizada en la investigación, se observa en la Tabla 2:

Tabla 2
Cuadro comparativo entre estándares

ESTANDAR	CARACTERÍSTICAS BASE	CONTROLES A AUDITAR / IMPLEMENTAR	SE ESPECIALIZA EN	ESPECIFICO PARA INSTITUCIONES FINANCIERAS	FUENTE
COBIT 4.1	Enfocado al riesgo	Dentro de los objetivos de control de COBIT se detallen las siguientes actividades que se deben adquirir y mantener en una organización, y que por lo tanto pueden y deben ser medidos, controlados y verificados: - AI1. Identificar Soluciones Automatizadas - AI2.Reporte de Análisis de Riesgos - AI3.Adquirir y mantener Infraestructura tecnológica. - AI4.Habilitar Operación y uso - AI5.Conseguir recursos de TI - AI6. Manejar Cambios - AI7. Instalar y acreditar soluciones y cambios - ME1. Monitorear y evaluar desempeño de TI	Gobernanza de TI , Riesgo Informático	Se puede adaptar	Cobit 4.1
ISO 27001	SE enfoca en la Seguridad de la Información	La sección de auditoría interna incluye las siguientes actividades: - Planificar la auditoría: Comunicar a las partes interesadas - Realización de una auditoría basada en 4 aspectos: - La forma de los documentos (actualización, codificación) - El contenido de los documentos eficacia y eficiencia de las medidas descritas en ellos - Verificar que los documentos cumplan los requisitos contenidos en la ISO 27001 - Que realmente se aplique lo que dicen los documentos	Seguridad de la información, Riesgo	Todo tipo de organizaciones	https://www.pmg-ssi.com/2014/12/iso-27001-auditorias-internas-del-sgsi/
ISO 22301	Enfocado al riesgo	- Planificar, establecer, implantar y mantener programa de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación y presentación de informes. El programa de auditoría deberá tener en cuenta la importancia de los procesos en cuestión de los resultado de la auditoría anterior - Definir los criterios de auditoría y El alcance de cada auditoría - Servicios de auditores y auditorías de conducta para asegurar la objetividad y la imparcialidad del proceso de auditoría - Garantizar los resultados de las auditorías se reportan a la administración correspondiente - Retener la información documentada como evidencia de la ejecución del programa de auditoría y los resultados de la auditoría El programa de auditoría, incluyendo la planificación, se basará en los resultados de las evaluaciones de riesgo.	Riesgo en el Sistema de Gestión de Seguridad de la Información	Todo tipo y tamaño de organización	https://www.pmg-ssi.com/norma-22301/9-2-la-auditoria-interna/
COSO	3 objetivos principales, 5 componentes, 17 principios y 85 puntos de foco	Lineamientos recomendados para contar con sistemas de calidad, confiables y protegidos. Dentro de Actividades de control: - Evaluación de la dependencia entre los procesos, los controles automáticos y los controles generales de TI. - Evaluación periódica de la calidad de la información generada por los sistemas (oportuna, actual, precisa, completa, accesible, protegida, verificable y conservada) - Diseño y evaluación de actividades de control sobre la infraestructura de TI; acceso a los sistemas; adquisición, desarrollo y mantenimiento de los mismo. - Configuración de los sistemas de información considerando un análisis de - Segregación de Funciones. - Realización de un análisis costo-beneficio de la implementación de controles de TI.	Auditoría de Organizaciones		http://cotana.informatica.edu.bo/downloads/Control%20interno%20-%20COSO.pdf

Fuente: elaboración propia

3. Evaluación del modelo, de manera iterativa: se revisó el modelo resultante, en 3 ocasiones para verificar que se incluyan todos los puntos críticos

4. Debe tratarse de un procedimiento multi metodológico. Al realizar la comparación de los diferentes estándares se asegura que el proceso de desarrollo es multi metodológico debido a que cada Marco de Referencia tiene una metodología de

aplicación diferente y está enfocado a resolver un problema diferente dentro de la Gestión de Tecnologías de la Información y Control Interno.

5. Identificación de la relevancia del problema: Luego de los resultados obtenidos de la investigación previa de campo, y la revisión de literatura, se concluye que los aspectos más críticos al evaluar un sistema de información son: la seguridad de la información que se genera dentro de la organización y el riesgo al cual están sujetos los componentes de un sistema de información.

6. Definición del problema: Como se menciona anteriormente, las circunstancias actuales de los avances tecnológicos y las amenazas existentes resultado del alto nivel de conectividad necesario para satisfacer las necesidades de alta disponibilidad de información y servicios para los usuarios finales de las Entidades financieras; es de vital importancia contar con sistemas de información que sean confiables y seguros. Y estas características pueden comprobarse al realizar un proceso de auditoría.

7. Presentación de los resultados dirigida a completar las necesidades de los usuarios: se presenta la propuesta de modelo de auditoría de forma de check list para que sea de fácil comprensión y manejo para los usuarios finales.

8. Documentarlo científicamente.: Finalmente, el modelo propuesto está fundamentado en los estándares internacionales probados extensamente a nivel mundial. Considerando los resultados de las encuestas, los aspectos más importantes que se deberían verificar en una auditoria a un sistema de información en cooperativas de segmento 1,2 y 3 serian:

1. No hay especialista de auditoría informática, por tanto, no tienen conocimiento exacto de QUE SE DEBE AUDITAR en un Sistema de información, por lo que:

a. Identificar los Sistemas automatizados que tiene la empresa (COBIT)

b. Recopilar información por escrito como: Procedimientos, Políticas de Seguridad, Manuales, Análisis de Riesgos si los tiene el Departamento de TI. (ISO 27001)

c. Verificar las medidas de seguridad de la infraestructura tecnológica: Cuartos de Servidores, acceso a los mismos, certificación de cableado estructurado, Sistemas de Respaldos de información, Sistemas de backup de enlaces de datos. (COSO)

d. Verificar las medidas de seguridad con respecto a personal, segregación de funciones y perfiles del personal que accede a los centros de datos, bases, etc. (COSO)

2. Existe desconfianza en la calidad de datos obtenidos, por tanto

a. Es necesario que la auditoría haga un análisis por muestreo de la calidad y confiabilidad de los datos generados por las aplicaciones informáticas (COSO)

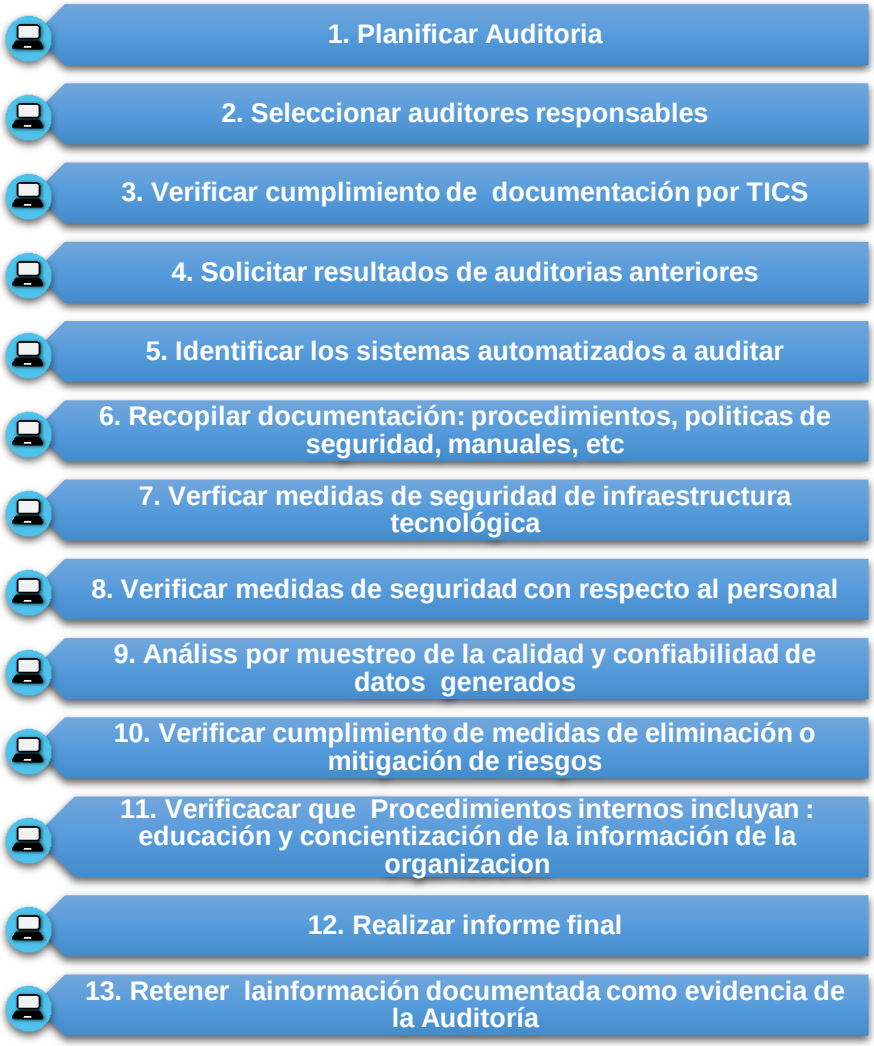
b. Además, se requiere que se audite o verifique si se han cumplido con las medidas de seguridad propuestas para mitigar o eliminar los riesgos (COBIT / ISO 22301)

3. Tomando en cuenta que los entrevistados también consideran que existe un riesgo por fuga de información:

a. Se debe verificar que los procedimientos internos incluyan educación y concientización al personal sobre la confidencialidad de la información de la organización y el cuidado de las credenciales de acceso a los sistemas de información (ISO 27001)

EL Modelo desarrollado, se detalla a continuación:

Figura 3
Modelo desarrollado



Fuente: elaboración propia

A continuación, se detalla cada paso a seguir en el Modelo desarrollado:

En primer lugar, se encuentran los puntos que toda Auditoría Interna debe tener para obtener un buen resultado:

1. Se debe planificar con anticipación, definir el alcance de la auditoría, en este caso se debe determinar si se realizará a uno de los Sistemas, a los de un Departamento

específico o a todos los de la organización y luego comunicar las fechas a las partes interesadas: Gerencia, Jefaturas Departamentales, etc.

2. Seleccionar los auditores responsables; podría contratarse un personal externo por primera vez si no se tiene la seguridad de cumplir a cabalidad.

3. Verificar que en la organización y el Departamento de TI cumplan lo que dicen los documentos a través de registros.

4. Solicitar los resultados de auditorías anteriores y verificar el cumplimiento de las recomendaciones pasadas y la corrección de las NO conformidades.

5. Luego de definido el alcance de la auditoría se debe identificar los sistemas automatizados que serán auditados, sean éstos aplicaciones cliente – servidor, web, servicios web, ERP, BI, etc.

6. Solicitar los documentos existentes, por ejemplo: Políticas de seguridad, procedimientos escritos sobre los procesos de desarrollo e implementación de sistemas de información, Manuales, Documentos verificables de control de accesos, control de cambios, Actas de control, etc. Se debe también verificar la actualización y codificación de estos documentos.

7. Verificar medidas de seguridad de infraestructura tecnológica, hace referencia a los accesos físicos al centro de datos, mecanismos de seguridad en los servidores, sistemas de respaldo de las aplicaciones y bases de datos, etc.

8. En cuanto a los aspectos de seguridad correspondientes al personal se encuentran las actas entrega – recepción de las credenciales de acceso a los sistemas, firma de acuerdos de confidencialidad, inducción a las buenas prácticas de seguridad informática, uso correcto de los recursos informáticos, etc.

9. Análisis por muestreo de la calidad y confiabilidad de los datos generados en los sistemas auditados; es decir, verificar un porcentaje pequeño de transacciones o reportes y realizar un cálculo doble para corroborar la información generada durante el proceso automatizado.

10. Verificación del cumplimiento de medidas de eliminación o mitigación del riesgo, hace referencia dentro del estándar COBIT a la matriz de riesgos (si existe) donde se identifican los riesgos existentes, su probabilidad de ocurrencia y el impacto al negocio; además de las acciones a seguir para eliminar o mitigar los riesgos críticos.
11. Es necesario verificar que los procedimientos internos de la organización incluyan actividades de educación y concientización al personal sobre la seguridad de la información, esto puede lograrse a través de charlas, cursos en línea, entrega de infografía, etc.
12. Realizar el informe correspondiente al término de la Auditoría y reportarlo a la Gerencia de TI y Gerencia General incluyendo el alcance de esta, el detalle de el o los sistemas evaluados, la evidencia recopilada y los hallazgos encontrados.
13. Retener la información documentada como evidencia del proceso de auditoría.

CONCLUSIONES

Luego de haber realizado el presente documento se puede concluir que:

El proceso de auditoría es una parte fundamental de los marcos de referencia más utilizados por las organizaciones a nivel mundial; ya que se trata de una herramienta para verificar el correcto funcionamiento de un proceso dentro de la entidad para asegurar la mejora continua.

Por otro lado, debido al nivel tecnológico y alta conectividad que actualmente se usa para realizar transacciones bancarias desde diversas plataformas y dispositivos electrónicos, se debe asegurar que los sistemas de información procesen los datos de manera confiable, íntegra y oportuna; por lo que deben sujetarse a procesos de control y auditoría.

Además, conociendo que a nivel internacional existen Estándares con varios años de evolución que guían los pasos para realizar estos procedimientos, se pueden lograr buenos resultados al combinar los aspectos relevantes de cada uno de ellos para adaptarlos a la necesidad de la organización.

Sin embargo, estos estándares se enfocan unos en Riesgos, otros en seguridad de la información, siendo necesario profundizar un poco más en los dos aspectos hasta conseguir un estándar híbrido, o una evolución del modelo de control interno más completo.

Por último, se debe mencionar que el Estándar COSO se perfila como el más utilizado en materia de control interno, y es aplicable en diferentes enfoques de auditoría: desde la auditoría común, hasta la auditoría informática, o de sistemas de información.

REFERENCIAS CONSULTADAS

1. Aguirre Bautista, J. de J. (2005). Auditoria en Informática. Recuperado de http://fcasua.contad.unam.mx/apuntes/interiores/docs/2005/informatica/6/1664.pdf

2. Alvarez Basaldúa, L. D. (2005). SEGURIDAD EN INFORMÁTICA (AUDITORÍA DE SISTEMAS). Recuperado de http://192.203.177.185/bitstream/handle/ibero/1010/014663_s.pdf?sequence=1&isAllowed=y

3. Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. Business & Information Systems Engineering, 1(3), 213-222. https://doi.org/10.1007/s12599-009-0044-5

4. Boswell, L., & Bhargava, T. (2014). Potential Uses of Maturity Models for Capacity Development in Emerging Democracies/Conflict Nations | PAE.

5. Castillo Morocho, J. C., Erazo Álvarez, J. C., Narváez Zurita, C. I., & Torres Palacios, M. M. (2019). Auditoría de gestión y su incidencia en la eficiencia y eficacia de las operaciones de una empresa comercial. Visionario Digital, 170.

6. Cotaña Mier, M. (2015). Control Interno. Recuperado 28 de septiembre de 2019, de http://cotana.informatica.edu.bo/downloads/Control interno - COSO.pdf

7. Derrien, Y. (1994). Técnicas de la Auditoria Informatica. Barcelona: Marcombo.

8. Fernández-medina, E. (2006). Modelos de madurez para SGSI desde un enfoque práctico Modelos de madurez para SGSI desde un enfoque práctico, (February).

9. Florian Caro, C. E. (2016). La Auditoria Tributaria , Origen Y Evolucion. Universidad Libre de Colombia. Recuperado de http://www.unilibre.edu.co/bogota/pdfs/2016/4sin/B20.pdf

10. GestioPolis. (2018). Auditoría de los Sistemas deInformación en la Organización - . Recuperado 25 de septiembre de 2019, de https://www.gestiopolis.com/auditoria-de-sistemas-de-informacion-en-la-organizacion/?fbclid=IwAR0Ras1pmFxEQhlhOW8UE7dhDNZz9XNXfYr6aPx5NYzC7IXaiM7bt_YN-PQ

11. Gonzáles Dueñas, C. M. (2012). Auditoria Informatica. Recuperado 13 de septiembre de 2019, de https://es.slideshare.net/maitin30/auditoria-informatica-14008209

12. Hernandez Hernandez, E. (1993). Auditoria de Informatica (Un enfoque metodológico). Universidad Autónoma de Nuevo leon. Recuperado de http://eprints.uanl.mx/6977/1/1020073604.PDF

13. ISACA. Guía de Auditoría y Aseguramiento de SI 2001 Estatuto de Auditoría (2001). Recuperado de http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2001_gui_Spa_0415.pdf

14. IsecT Ltd. (s. f.). ISO/IEC 27001 certification standard.

15. ISO -International Organization for Standardization. (2011). Familias de las Normas ISO 27000, 19.

16. López, A. (2012). Auditoria de sistemas de información. Recuperado 25 de septiembre de 2019, de https://www.uv.mx/personal/artulopez/files/2012/10/07-Auditoria-de-SI.pdf?fbclid=IwAR2GH04xlW_pT5LY-VYjES1_gbvZ6KtSTclv9QIoutunEY3G0eBWJEcrmrc

17. MAgee, K. (2015). IT Auditing and Controls – Auditing Organizations, Frameworks and Standards. Recuperado 27 de septiembre de 2019, de https://resources.infosecinstitute.com/itac-organizations/#

18. Ministerio de Tecnologías, & de la Información y las Comunicaciones. Modelo de Seguridad y Privacidad de la Información (2012). Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

19. Montaño Ardila, V., Combita Niño, H., & de la Hoz Franco, E. (2017). Alineación de Cobit 5 Y Coso IC–IF para definición de controles basados en Buenas Practicas

TI en cumplimiento de la Ley Sarbanes–Oxley. Revista ESPACIOS, 38(23). Recuperado de http://www.revistaespacios.com/a17v38n23/17382303.html

20. Organizacion de los estados americanos. (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.

21. Ortega Polanco, V. (2017). Gestión de la imagen corporativa de organizaciones universitarias desde el enfoque del marketing emocional. *CIENCIAMATRIA*, *3*(5), 150-171. https://doi.org/10.35381/cm.v3i5.19

22. Piattini Velthuis, M. G., & Peso Navarro, E. del. (2001). Auditoria Informática un enfoque práctico (2 Edición). Alfaomega.

23. Piña, E. (2015). Respuestas auditoria informatica webquest pdf. Recuperado 10 de septiembre de 2019, de https://es.slideshare.net/Enderluis2/respuestas-auditoria-informatica-webquest-pdf

24. Porter, T., & Burton, J. (1981). Auditoria: Un análisis conceptual. Mexico DF: Editorial Diana.

25. PWC. (2015). Simposio Segunda Plenaria mayo 2015. Recuperado de www.pwc.com

26. PWC España. (2018). Encuesta mundial sobre fraude y delito económico 2018. Recuperado 15 de septiembre de 2019, de https://www.pwc.es/es/forensic-services/encuesta-mundial-fraude-delito-economico-2018.html

27. PWC Peru. (2018). Encuesta Global sobre Delitos Económicos y Fraude2018.

28. Rocano Criollo, D. A., Narváez Zurita, C. I., Erazo Álvarez, J. C., & Luna Altamirano, K. A. (2019). Gestión logística con enfoque en la ISO28000, para empresas comerciales. Visionario Digital, 145.

29. Rodríguez Rodríguez, S., Crúz, Y., & Puertas, A. (2017). Indicadores para la comercialización de productos derivados de lotes caprinos (capra hircus), hacia una estrategia endógena de marketing en Colina – Zamora, Falcón, Venezuela. *Revista Arbitrada Interdisciplinaria Koinonía, 2*(3), 198--212. Recuperado de http://fundacionkoinonia.com.ve/ojs/index.php/revistakoinonia/article/view/63/50

30. Saavedra, J., & Torres Olaya, A. (2012). Modelo de gobierno de TI como apoyo al proceso de transformación digital en empresas de la industria editorial.

31. Servicio Ecuatoriano de Normalización. (2016). Prólogo nacional.

32. Super intendencia de Economía Popular y Solidaria. (2019). Estadistica - SEPS. Recuperado 31 de marzo de 2019, de http://www.seps.gob.ec/estadistica?captaciones-y-colocaciones

33. Superintendencia de Economía Popular y Solidaria. (2013). Boletín trimestral I Un vistazo del sector cooperativo por segmentos y niveles. Quito. Recuperado de https://www.seps.gob.ec/documents/20181/26626/Boletín trimestral 24_04_2013_final.pdf/68b53d50-3a0d-461a-8bd9-bbad0c5589a6

REFERENCES CONSULTED

1. Aguirre Bautista, J. de J. (2005). Computer Audit. Recovered from http://fcasua.contad.unam.mx/apuntes/interiores/docs/2005/informatica/6/1664.pdf

2. Alvarez Basaldúa, L. D. (2005). IT SECURITY (SYSTEMS AUDIT). Retrieved from http://192.203.177.185/bitstream/handle/ibero/1010/014663_s.pdf?sequence=1&isAllowed=y

3. Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. Business & Information Systems Engineering, 1 (3), 213-222. https://doi.org/10.1007/s12599-009-0044-5

4. Boswell, L., & Bhargava, T. (2014). Potential Uses of Maturity Models for Capacity Development in Emerging Democracies / Conflict Nations | PAE.

5. Castillo Morocho, J. C., Erazo Álvarez, J. C., Narváez Zurita, C. I., & Torres Palacios, M. M. (2019). Management audit and its impact on the efficiency and effectiveness of the operations of a commercial company. Digital Visionary, 170.

6. Cotaña Mier, M. (2015). Internal control. Retrieved September 28, 2019, from http://cotana.informatica.edu.bo/downloads/Internal control - COSO.pdf

7. Derrien, Y. (1994). Computer Audit Techniques. Barcelona: Marcombo.

8. Fernández-medina, E. (2006). Maturity models for ISMS from a practical approach Maturity models for ISMS from a practical approach, (February).

9. Florian Caro, C. E. (2016). The Tax Audit, Origin and Evolution. Free University of Colombia. Retrieved from http://www.unilibre.edu.co/bogota/pdfs/2016/4sin/B20.pdf

10. GestioPolis. (2018). Audit of Information Systems in the Organization -. Retrieved September 25, 2019, from https://www.gestiopolis.com/auditoria-de-sistemas-de-informacion-en-la-organizacion/?fbclid=IwAR0Ras1pmFxEQhlhOW8UE7dhDNZz9XNXfYr6aPx5NYzC7IXaiM7bt_Y-

11. Gonzales Dueñas, C. M. (2012). Computer Audit Retrieved September 13, 2019, from https://es.slideshare.net/maitin30/auditoria-informatica-14008209

12. Hernandez Hernandez, E. (1993). Informatics Audit (A methodological approach). Autonomous University of Nuevo Leon. Retrieved from http://eprints.uanl.mx/6977/1/1020073604.PDF

13. ISACA SI Audit and Assurance Guide 2001 Audit Statute (2001). Retrieved from http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2001_gui_Spa_0415.pdf

14. IsecT Ltd. (s. F.). ISO / IEC 27001 certification standard.

15. ISO-International Organization for Standardization. (2011). Families of ISO 27000, 19.

16. Lopez, A. (2012). Information systems audit. Retrieved September 25, 2019, from https://www.uv.mx/personal/artulopez/files/2012/10/07-Auditoria-de-SI.pdf?fbclid=IwAR2GH04xlW_pT5LY-VYjES1_gbvZ6KtSTclv9QIoutunEY3G0eBWJEcrmr

17. MAgee, K. (2015). IT Auditing and Controls - Auditing Organizations, Frameworks and Standards. Retrieved September 27, 2019, from https://resources.infosecinstitute.com/itac-organizations/#

18. Ministry of Technologies, Information & Communications. Information Security and Privacy Model (2012). Recovered from https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

19. Montaño Ardila, V., Combita Niño, H., & de la Hoz Franco, E. (2017). Alignment of Cobit 5 and Coso IC – IF for definition of controls based on Good IT Practices in

compliance with the Sarbanes – Oxley Act. ESPACIOS Magazine, 38 (23). Recovered from http://www.revistaespacios.com/a17v38n23/17382303.html

20. Organization of American States. (2018). State of Cybersecurity in the Banking Sector in Latin America and the Caribbean.

21. Ortega Polanco, V. (2017). Management of the corporate image of university organizations from the focus of emotional marketing. SCIENCE, 3 (5), 150-171. https://doi.org/10.35381/cm.v3i5.19

22. Piattini Velthuis, M. G., & Peso Navarro, E. del. (2001). Computer Audit a practical approach (2 Edition). Alpha Omega.

23. Piña, E. (2015). Responses computerquest audit webquest pdf. Retrieved September 10, 2019, from https://es.slideshare.net/Enderluis2/respuestos-auditoria-informatica-webquest-pdf

24. Porter, T., & Burton, J. (1981). Audit: A conceptual analysis. Mexico DF: Diana Editorial.

25. PWC (2015). Second Plenary Symposium May 2015. Retrieved from www.pwc.com

26. PWC Spain. (2018). Global survey on fraud and economic crime 2018. Retrieved September 15, 2019, from https://www.pwc.es/es/forensic-services/encuesta-mundial-fraude-delito-economico-2018.html

27. PWC Peru (2018). Global Survey on Economic Crimes and Fraud2018.

28. Rocano Criollo, D. A., Narváez Zurita, C. I., Erazo Álvarez, J. C., & Luna Altamirano, K. A. (2019). Logistics management with focus on ISO28000, for commercial companies. Digital Visionary, 145.

29. Rodríguez Rodríguez, S., Crúz, Y., & Puertas, A. (2017). Indicators for the commercialization of products derived from goat lots (capra hircus), towards an endogenous marketing strategy in Colina - Zamora, Falcón, Venezuela. Interdisciplinary Arbitrated Review Koinonía, 2 (3), 198--212. Recovered from http://fundacionkoinonia.com.ve/ojs/index.php/revistakoinonia/article/view/63/50

30. Saavedra, J., & Torres Olaya, A. (2012). IT governance model to support the process of digital transformation in companies in the publishing industry.

31. Ecuadorian Standardization Service. (2016). National Prologue

32. Super Administration of Popular and Solidarity Economy. (2019). Statistics - SEPS. Retrieved March 31, 2019, from http://www.seps.gob.ec/estadistica?captaciones-y-colocaciones

33. Superintendence of Popular and Solidarity Economy. (2013). Quarterly bulletin I A look at the cooperative sector by segments and levels. Quito Retrieved from https://www.seps.gob.ec/documents/20181/26626/ Quarterly bulletin 24_04_2013_final.pdf / 68b53d50-3a0d-461a-8bd9-bbad0c5589a6