Guía de auditoría para la evaluación del control interno de seguridad de la información con enfoque COBIT 5: caso Universidad Católica de Cuenca (UCACUE).

Article · December 2016

DOI: 10.26423/rctu.v3i3.204

1 author:

Carlos Encalada
Universidad Católica de Cuenca (UCACUE)
3 PUBLICATIONS **0** CITATIONS

Revista Científica y Tecnológica UPSE, Vol. III, N. 3, Pág. 113-121 (Dic., 2016)

14

GUÍA DE AUDITORÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE COBIT 5: CASO UNIVERSIDAD CATÓLICA DE CUENCA (UCACUE

Carlos Encalada Loja, Diego Cordero Guzmán.

Recibido: septiembre de 2016
Aprobado: diciembre de 2016

GUÍA DE AUDITORÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE COBIT 5: CASO UNIVERSIDAD CATÓLICA DE CUENCA (UCACUE)

AUDIT GUIDE FOR THE EVALUATION OF INTERNAL CONTROL INFORMATION SECURITY WITH FOCUS COBIT 5: CASE CATHOLIC UNIVERSITY OF CUENCA (UCACUE)

Carlos Encalada Loja[1], Diego Cordero Guzmán[1]

[1] Unidad Académica de Tecnologías de la Información y Comunicación
Universidad Católica de Cuenca (UCACUE)
Cuenca-Ecuador
cencalada@ucacue.edu.ec

Resumen

El objetivo del trabajo es realizar una Guía de Auditoría para la evaluación del Control Interno de la seguridad de la información alineada a los criterios de las mejores prácticas de COBIT 5, con la intención de soportar de mejor manera la seguridad de la información en la Universidad Católica de Cuenca. Se toma como referencia el marco de trabajo de COBIT 5, sintetizado en las siguientes fases: análisis del entorno organizacional, determinación del alcance y los objetivos de la auditoría, identificación de actores clave a ser entrevistados, enfoque preliminar del contexto a ser auditado, determinación de recursos necesarios para realizar la auditoría, elaboración del plan de trabajo, implementación de tareas y actividades. En una fase de mayor detalle se ejecuta el mapeo de los objetivos y procesos de TI y se elaboran los instrumentos principales para la aplicación de la Guía de Auditoría, que una vez implementados permitieron identificar las iniciativas en seguridad de la información efectuadas por la organización, en concreto se explotó el código de proceso DSS05 de COBIT 5, denominado "Gestionar los servicios de seguridad". Como resultado se obtuvo un diagnóstico del Control Interno de la seguridad de la información de la Universidad.

Palabras clave: *Guía de auditoría, control interno, COBIT 5, seguridad de la información, servicios de seguridad*

Abstract

The aim of this work is generate a for IT Audit dedicated to evaluation of Internal Control Information Security aligned to the criteria of best practices of COBIT 5, with the intention to support better safety information in the Catholic University of Cuenca. COBIT 5 is taken as reference, summarized in the following phases: analysis of the organizational environment, determining the scope and objectives of the audit, identifying key players to be interviewed, preliminary approach context to be audited, determination resources needed to perform the audit work plan development, implementation of tasks and activities. In a phase of more detailed mapping goals and IT processes are executed after the main instruments for implementing the Audit Guide ere developed, which once implemented it possible to identify initiatives in information security provided by the organization, specifically the process DSS05 code COBIT 5, entitled "Managing the security services" was exploited. As a result a diagnosis of Internal Control Information Security at the Catholic University of Cuenca was obtained and could establish audit findings that were reflected in the final report. Terminal phase as the letter addressed to top management on the most critical findings requiring urgent attention was drawn.

Keywords: *Guide audit, internal control, COBIT 5, information security, service security*

Recibido: septiembre de 2016
Aprobado: diciembre de 2016

1. Introducción

En la actualidad, la información es un recurso clave para las empresas e instituciones, la tecnología juega un papel muy importante en el procesamiento de la misma, por lo que, su uso es cada vez más generalizado tanto en entornos públicos como privados.

La seguridad de la información se enfoca en la protección de la confidencialidad, integridad y disponibilidad de la información lo que incluye proteger la infraestructura, servicios y aplicaciones de amenazas internas o externas, deliberadas o accidentales que la vulneren. La seguridad de la información por tanto requiere un accionar proactivo y no reactivo, por lo que es necesario incluirla como un elemento estratégico que aporte a la consecución de los objetivos institucionales.

El cumplimiento de regulaciones y normativas exige a ciertos sectores implementar seguridad de la información, pues cada vez existen más empresas e instituciones del sector público y privado que han tomado conciencia de su importancia a fin de generar confianza en todas las partes interesadas.

En este sentido COBIT 5 es un marco de gobierno de las tecnologías de información que proporciona una serie de herramientas para que el nivel directivo de la organización pueda relacionar los objetivos de control con los aspectos técnicos y los riesgos en el área de la seguridad de la información [1].

El presente trabajo genera como resultado una Guía de Auditoría Informática para la evaluación del Control Interno de la seguridad de la información encaminada al mejoramiento continuo en la Universidad Católica de Cuenca. Para esto se identificaron las iniciativas en seguridad de la información implementados por la universidad, en base al proceso DSS05 denominado "Gestionar los servicios de seguridad" de COBIT 5, y enmarcada en la Gerencia de TI. La categorización de este nivel permitió determinar ¿cuánto? se debe mejorar en el proceso de seguridad.

Se parte de una revisión del marco teórico elemento referencial básico para el fin propuesto, luego se describe la metodología de trabajo ejecutada, para después poner énfasis en los resultados alcanzados y las subsecuentes conclusiones del estudio.

2. Materiales y Métodos

2.1. Marco Teórico

La auditoría de sistemas si se enfocara solamente al cumplimiento normativo no representaría interés para el nivel directivo y gerencial, en el mejor de los casos cumplir con la ley. Este escenario demuestra día a día que cada vez se hace más necesaria la integración de los estándares internacionales para lograr auditorías efectivas que garanticen un gobierno corporativo de tecnología de la información (TI) acorde con las necesidades de la organización, así como unos servicios de tecnología altamente eficientes [2].

En la actualidad, en las organizaciones, la auditoría se concibe como una actividad de evaluación independiente que agrega valor mediante el hallazgo de oportunidades de mejora a los procesos y en el caso de los sistemas de información, su ayuda radica en: la revisión y la evaluación de los controles y procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información. De modo que por medio de la ejecución de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones. [3]

Otro factor importante que se debe tomar en cuenta en el tema de la seguridad de la información, es el desarrollo acelerado de las redes informáticas, mecanismo que trajo consigo un aumento considerable en la velocidad de procesamiento y en la transmisión de información, pero con riesgos cada vez mayores en lo referente a seguridad de los datos transportados por estos medios.

En este sentido, se nota cómo hoy en día, la convergencia de las tecnologías de la información ha ocasionado una marcada dependencia que impide una separación certera entre la seguridad propia de las aplicaciones, seguridad informática, con la seguridad de la información como tal.

Por esta razón, debido al amplio espectro que implica el concepto de seguridad de la información, se decidió acoger como un estándar certificable la ISO 17799 —anteriormente British Standard (BS) 7799/1999— en el 2005, la que más tarde se convirtió en la ISO 27002:2013[i].

De acuerdo con el estudio preliminar sobre información acerca de los papeles de trabajo que deben acompañar todo examen de auditoría no se ha encontrado una referencia bibliográfica específica sobre

este tema, en base a que cada Institución es un universo diferente con sus propias definiciones de áreas críticas.

Por lo tanto, cobra validez el hecho de que existan marcos de referencia y buenas prácticas para evaluaciones y auditorías de distintos tipos, que permitan alinear los criterios y recomendaciones como es el caso de este proyecto a COBIT 5, enfocado al gobierno y gestión integral entre TI y el Negocio.

- Gobierno: garantiza que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas. [1].

- Gestión: planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas organizacionales. [1].

En COBIT 5, los procesos: APO13ii, "Gestionar la seguridad"; DSS04iii, "Gestionar la continuidad"; DSS05iv, "Gestionar los servicios de seguridad", proporcionan una guía básica acerca de cómo definir, operar y monitorizar un sistema para la gestión general de seguridad. De cualquier forma, se asume que la Seguridad de la Información se encuentra presente a lo largo de toda la organización y es ahí en donde COBIT 5 proporciona la nueva guía de ISACA para el gobierno y la gestión corporativa de la seguridad de la información. [1]

De este modo se convierte en una exigencia estratégica observar estándares y normas técnicas como: COBIT 5 que es "un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores de TI, usuarios y por supuesto los auditores involucrados en el proceso" [4].

Por su parte, ISO 2700X (ISO/IEC 17799) también denominada como ISO 27002 es el nuevo nombre de la ISO/IEC 17799:2005, es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. [5].

2.2.Metodología

Las herramientas y técnicas metodológicas utilizadas para recopilación de información que permitieron realizar el proceso de planeación de la Auditoría Informática al Control Interno de la Seguridad de la Información aplicado en la Universidad Católica de Cuenca, fueron: la entrevista y el checklist

Además, se tomó como referencia a Kuna con su tesis de Magister que tiene por título "Asistente para la realización de Autoría de Sistemas en Organismos Públicos o Privados", en la que analiza a diferentes autores que proponen metodologías de auditorías de sistemas en general, aplicable al tema de Seguridad de la Información [6], resumido en las fases, que se especifican en la figura 1.

2.3. Guía de Auditoría para la Evaluación del Control Interno de la Seguridad

El entorno organizacional entre las que se incluye la universidad puede ser una representación compleja y foco de vulnerabilidades que aunque no se ven, existen, por ello y debido a la importancia de evitar la fuga o robo de información confidencial de la Universidad Católica de Cuenca, las modificaciones no adecuadas así como la falta de acceso a la información cuando se requiere, es vital apoyarse en una auditoría de la Seguridad de la Información que verifique el estado del control interno de la seguridad de la Institución.

De categoría cofinanciada, la Universidad Católica de Cuenca fue creada el siete de septiembre de 1970, en la ciudad de Cuenca, cuenta con extensiones universitarias en las localizaciones de Quito, Azogues, Cañar, San Pablo de la Troncal, Macas. Oferta carreras de tercer nivel en las ramas de las ciencias sociales, ingeniería, ciencias de la salud, ciencias empresariales y económicas. Se caracteriza por brindar una educación de calidad y cristiana; en la actualidad cuenta con aproximadamente 10.000 estudiantes [7].

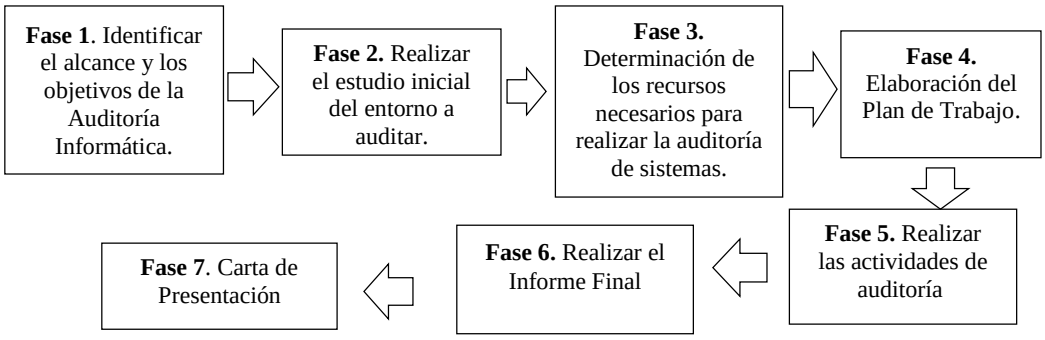

Figura 1. Guía de auditoría por fases

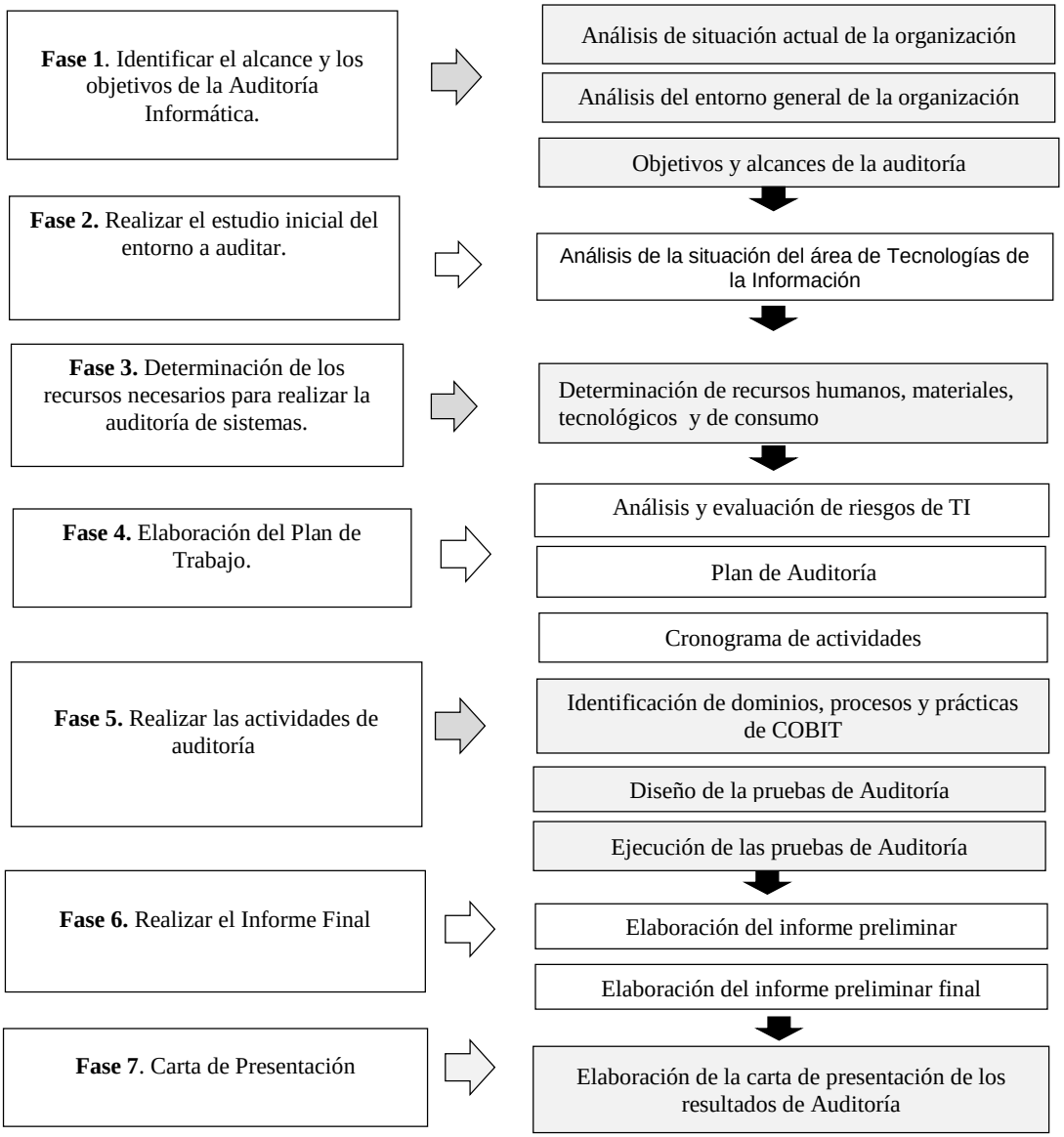

Figura 2. Guía de auditoría por fases
Fuente: Elaborado en base a Kuna [6].

3. Resultados

3.1. Procesos de Seguridad de la Información seleccionados

Para la evaluación del control interno de la Seguridad de la Información en la Universidad Católica de Cuenca basada en COBIT 5, fue necesario identificar claramente los dominios, procesos y prácticas de gestión aplicables. Para alcanzar tal fin se realizó un análisis minucioso para seleccionar los procesos, tanto principales como secundarios que aportan significativamente a la consecución de los objetivos y que requieren ser evaluados.

Durante el desarrollo de la investigación se elaboró la Guía de Auditoría, con el objetivo correspondiente a la Seguridad de la Información, a partir de esto se procede con la selección de los procesos de COBIT 5 relacionado al objetivo planteado, para ello se utilizó la tabla de mapeo entre las metas relacionadas con TI y los procesos de TI que proporciona COBIT 5 en su marco de referencia.

En la Tabla 1 se puede apreciar los procesos seleccionados para evaluar la seguridad de la información en la UCACUE, en la que identifica los procesos principales (P) y secundario (S).

Tabla 1. Procesos COBIT 5 seleccionados

COBIT 5		Meta relacionada con las TI
Dominios	Procesos	Seguridad de la información, infraestructura de procesamiento y aplicaciones.
APO01	Gestionar el Marco de Gestión de TI	S
APO07	Gestionar los Recursos Humanos	S
APO09	Gestionar los acuerdos de servicio	S
APO13	Gestionar la Seguridad	P
BAI08	Gestionar el conocimiento	S
DSS05	Gestionar Servicios de Seguridad	P
MEA02	Supervisar, evaluar y valorar el sistema de control interno	S

3.2. Prácticas de Gestión aplicables identificadas

Seleccionados los procesos tanto principales como secundarios, que serán evaluados, se procede a determinar las prácticas de gestión aplicables por cada proceso según la realidad de la Institución, dichas prácticas se explican en el documento "COBIT 5 para Seguridad de la Información", en el que se define de manera detallada la descripción de la práctica, sus entradas y salidas así como las actividades específicas correspondientes a seguridad de la información. En la Tabla 2 se listan las prácticas identificadas para evaluar la seguridad de la información en la UCACUE por cada proceso seleccionado.

3.3 Pruebas de auditoría diseñadas

Para cada uno de los procesos seleccionados y listados en la Tabla 1, se debe elaborar los checklist necesarios que permitan evaluar las prácticas de gestión identificadas. De esta manera se determinaron 15 checklist para la evaluación de la Seguridad de la Información de la Universidad Católica de Cuenca en algunos de los que se ha agrupado las prácticas de gestión que se interrelacionan.

En cada uno de los 15 checklist se elaboró los cuestionamientos que permiten evaluar adecuadamente el proceso mediante la verificación del cumplimiento de las actividades específicas de cada práctica de gestión según "COBIT 5 para Seguridad de la Información", así como los controles de ISO 27002 que sean aplicables en la UCACUE.

Se desarrolló el instrumento para la aplicación de las pruebas de auditoría en base a: dominios, procesos y prácticas de "COBIT 5 para la Seguridad de la Información" descritos en la Tabla 2, lo que permitió generar el formato AUD-FOR-TIC-001 (ver Tabla 3), en base al que se realizaron los checklist para evaluar el control interno.

3.4. Hallazgos de auditoría identificados

Aplicado los checklist al personal correspondiente se procede con el levantamiento de hallazgos de auditoría, que para un mejor entendimiento

Tabla 2. Prácticas de Gestión por proceso

DOMINIO	PROCESO	PRÁCTICAS
Alinear, Planificar y Organizar (APO)	APO01 Gestionar el Marco de Gestión de TI	APO01.01 Definir la estructura organizativa
		APO01.02 Establecer roles y responsabilidades.
		APO01.03 Mantener los catalizadores del sistema de gestión
	APO07 Gestionar los Recursos Humanos	APO07.01 Mantener la dotación de personal suficiente y adecuado
		APO07.02 Identificar personal clave de TI
		APO07.03 Mantener las habilidades y competencias del personal
	APO09 Gestionar los acuerdos de servicio	APO09.01 Identificar servicios TI
		APO09.02 Catalogar los servicios de TI
	APO13 Gestionar la Seguridad	APO13.01 Establecer y mantener un Sistema de Gestión de Seguridad de la Información
Construir, Adquirir e Implementar (BAI)	BAI08 Gestionar el conocimiento	BAI08.02 Identificar y clasificar las fuentes de información
Entrega, Servicio y Soporte (DSS)	DSS05 Gestionar Servicios de Seguridad	DSS05.01 Proteger contra software malicioso
		DSS05.02 Gestionar la seguridad de la red y las conexiones
		DSS05.03 Gestionar la seguridad de los puestos de usuarios finales
		DSS05.04 Gestionar la identidad del usuario y el acceso lógico
		DSS05.05 Gestionar el acceso físico a los activos de TI
		DSS05.06 Gestionar documentos sensibles y dispositivos de salida
		DSS05.07 Supervisar la Infraestructura para detectar eventos relacionados con seguridad
Supervisar, Evaluar y Valorar (MEA)	MEA02 Supervisar, evaluar y valorar el sistema de control interno	MEA02.01 Supervisar el control interno
		MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio
		MEA02.03 Realizar autoevaluación de control
		MEA02.04 Identificar y comunicar las deficiencias de control

y presentación se han establecido mediante un formato identificado como AUD-FOR-TIC-002 (ver tabla 4). Este formato en su encabezado incluye información sobre: dominios, procesos y prácticas de COBIT 5 que se evalúan, además el campo EVIDENCIA determina la relación directa con el checklist aplicado, que constituye la fuente de información para determinar el hallazgo.

Para realizar el levantamiento de los hallazgos de Auditoría, por cada proceso evaluado y por cada práctica de gestión se desarrollan los atributos de un hallazgo, a saber: condición, criterio, causa y efecto; de ser pertinente se puede agrupar en un único formulario varias prácticas de gestión. La condición se redacta en base a la situación actual de la práctica de gestión evaluada que se obtiene del análisis del checklist relacionado y aplicado en la fase anterior.

El criterio se establece en función del marco de referencia empleado, en este caso particular "COBIT 5 para Seguridad de la Información". La causa se obtiene de las observaciones anotadas por el auditado en los checklist. El efecto expresará la consecuencia de no cumplir con el criterio. Además, el formato permite integrar dentro del mismo esquema las conclusiones y recomendaciones de los hallazgos.

Tabla 3. Formato AUD-FOR-TIC-001 – Evaluación de controles

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001				
EVALUACIÓN DE CONTROLES:				
DOMINIO:				
PROCESO:				
PRÁCTICA:				
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

Tabla 4. Formato AUD-FOR-TIC-002 – Hallazgos de auditoría

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	
Proceso:	
Práctica:	
Evidencia:	
Condición	
Criterio	
Causa	
Efecto	
Conclusión	
Recomendación.	

3.5. Hallazgos más importantes identificados

- La UCACUE no tiene una estructura orgánica funcional de TI definida.
- No existe un área de Seguridad de la información que defina, administre y supervise el Sistema de Gestión de Seguridad de la Información (SGSI).
- No posee un Comité de Dirección de la Seguridad de la Información.
- No se han definido Políticas y Procedimientos de Seguridad de la Información.
- Ausencia de control interno de la Seguridad de la Información.

3.6. Informe preliminar de auditoría

El informe preliminar de auditoría fue elaborado con los hallazgos identificados así como las conclusiones y recomendaciones planteadas por el auditor. El informe preliminar de auditoría fue validado con todos los auditados, quienes aceptaron y aprobaron el contenido de los hallazgos, sus conclusiones y recomendaciones previo a la emisión del informe final de auditoría.

3.7. Informe final de auditoría

La Guía de Auditoría, concluye con el informe final de auditoría, en base a los hallazgos obtenidos tanto positivos como negativos. El citado informe contiene fundamentalmente el análisis final del cumplimiento o no cumplimiento del control interno de la Seguridad de la Información. De la misma manera que, en el informe preliminar de auditoría se revisó y validó el informe con la alta dirección, según las políticas de auditoría de la Institución.

La evaluación del Control Interno relacionado con la Seguridad de la Información, permitió determinar que la mayoría de controles no son adecuados y están operando parcialmente, así también existen controles que no se han determinado. En este sentido, se establecen recomendaciones para mejorar los controles existentes y crear aquellos que no han sido considerados en relación con los siguientes propósitos: Creación del área de Seguridad de la Información y del Comité de dirección de la seguridad de la información para que se fomente una cultura, ética y comportamiento adecuados en cuanto a seguridad de la información; la creación de la estructura orgánico funcional de TIC; la creación del cargo de CISO (Oficial de seguridad); la creación del manual de funciones en el cual se establezca los roles y responsabilidades del personal y sus perfiles con relación a la Seguridad de la Información; el establecimiento de políticas relacionadas con seguridad de la información, marcos de referencia o buenas prácticas para la gestión de la seguridad de la información; identificación del personal clave para las actividades de seguridad de la información; la creación de un plan de capacitación para actividades específicas en temas de seguridad de la información; la implementación de un Sistema de Gestión de Seguridad de la Información bajo Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información; levantamiento de documentación formal como políticas, procedimientos, arquitectura y estrategia de seguridad que le permita alcanzar un grado de madurez en la gestión de seguridad de redes y conexiones; definición de los niveles de seguridad de acuerdo a los requerimientos de seguridad.

4. Conclusiones

- Es de gran importancia y utilidad para la Universidad Católica de Cuenca contar con una Guía de Auditoría basada en un marco de referencia y mejores prácticas como COBIT 5 que facilite la evaluación de la Seguridad de la Información.

- Con la implementación de la Guía de Auditoría para el control interno de Seguridad de la Información se identifican las oportunidades de mejora y se determinan iniciativas de Seguridad de la Información.

- Como resultado de la aplicación de la Guía de Auditoría, la Universidad Católica de Cuenca cuenta con un diagnóstico del Control Interno de la Seguridad de la Información con sus respectivas recomendaciones basadas a los criterios de COBIT 5 que aportarán a mejorar la Seguridad de la Información.

- Para el uso de COBIT 5 para Seguridad de la Información es fundamental un amplio estudio y entendimiento.

- La "Guía de Auditoría para el Control Interno de Seguridad de la Información", ha sido creada para la Universidad Católica de Cuenca en base a sus necesidades y requerimientos alineándolos a COBIT 5 para Seguridad de la Información.

- El marco de referencia y buenas prácticas de COBIT 5 para seguridad de la información puede ser acogida por cualquier institución y su utilización no implica el cumplimiento total del marco de referencia.

5. Agradecimientos

A la Unidad Académica de Ingeniería de Sistemas, Eléctrica y Electrónica, de la Universidad Católica de Cuenca, por la apertura a procesos de orden investigativo sobre aspectos de las Tecnologías de la Información.

6. Referencias

[1] ISACA-COBIT 5, COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, Estados Unidos, 2012.

[2] R. C. Díaz, «Marco de referencia para auditorías integrales de sistemas en las mipymes colombianas,» *Publicación Semestral revista Gestión y Sociedad*, pp. 15-29, 2012.

[3] L. Galán, Informática y auditoría para las ciencias empresariales, Bucaramanga: Universidad Autónoma de Bucaramanga, 1996.

[4] EAFIT Universidad, «COBIT : MODELO PARA AUDITORIA Y CONTROL DE SISTEMAS DE INFORMACIÓN,» *Boletín 54*, p. 1, 2007.

[5] ISO org, «ISO 27000,» 20 Agosto 2014. [En línea]. Available: http://www.iso27000.es/download/doc_iso27000_all.pdf.

[6] H. Kuna, «Tesis de Magister en Ingeniería del Software,» 2006. [En línea]. Available: http://laboratorios.fi.uba.ar/lsi/rgm/tesistas/kuna-tesisdemagister.pdf

[7] D. Cordero, *Modelo para Gobierno de Tecnologías de la Información (GTI): caso de las Universidades Cofinanciadas de la Zona 6 de la República del Ecuador (Tesis de Grado Doctoral en proceso)*, México: UNAM, 2016.

[8] CEDIA. Informe de resultados de la 1° Encuesta de Seguridad de la Información en Universidades Ecuatorianas miembros de CEDIA. Loja, 2014.

[9] Deloitte. COSO mejora su Control Interno Estructura conceptual integrada, 2013.[En línea].Available: http://webserver2.deloitte.com.co/Consultoria%20en%20riesgo/coso/Heads%20Up%20No%20%2017%20de%202013COSOMejorasuCI.pdf

[10] Echenique, J.A. Auditoría en Informática. Mexico: Mcgraw-Hill, 2003.

[11] Instituto de auditores internos de España. Control Interno - Marco Integrado. Madrid, 2013.

[12] ISACA-COBIT 5, COBIT 5 para Seguridad de la Información. Estados Unidos, 2012.

[13] Microsoft-Technet. Guía de administración de riesgos de seguridad de Microsoft, 2004. [En línea]. Available: https://www.microsoft.com/spain/technet/recursos/articulos/srsgch01.mspx

[14] Cano, J. J. Inseguridad Informática y Computación Anti-forense. Information Systems Control Journal, 2007.

[i] *ISO 27002: 2013.- Código de prácticas para la gestión de la Seguridad de la Información actualizada en el año 2013*
[ii] *APO13.- Proceso número trece del dominio Alinear, Planificar y Organizar del marco de referencia COBIT*
[iii] *DSS04.- Proceso número cuatro del dominio Entregar, Dar Servicio y Soporte del marco de referencia COBIT 5.*
[iv] *DSS05.- Proceso número cinco del dominio Entregar, Dar Servicio y Soporte del marco de referencia COBIT 5*