ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

VIII PROMOCIÓN.

TEMA: "GUÍA DE AUDITORIA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD CATÓLICA DE CUENCA BASADA EN COBIT 5."

AUTORES:
ENCALADA LOJA. CARLOS
TENECELA POGYO, AIDA

DIRECTOR: MSC. ING. GARRIDO SÁNCHEZ, FERNANDO

SANGOLQUÍ, ABRIL DE 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

CERTIFICADO DE TUTORÍA

Ing. Fernando Garrido Sánchez, MSc.

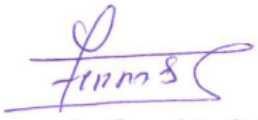
CERTIFICO:

Que el trabajo titulado "GUÍA DE AUDITORIA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD CATÓLICA DE CUENCA BASADA EN COBIT 5." realizado por el Ing. Carlos Enrique Encalada Loja y la Ing. Aída Guillermina Tenecela Pogyo, ha sido dirigido y revisado periódicamente, cumpliendo con las normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas.

Debido a que han concluido satisfactoriamente el trabajo de conclusión de carrera, requisito previo a la obtención del título de Magister, recomiendo su publicación.

El mencionado trabajo consta de (un) documento empastado y (un) disco compacto, el cual contiene los archivos en formato portátil PDF

Sangolquí, 23 de Abril del 2015.



Ing. Fernando Garrido Sánchez, MSc

DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, Carlos Enrique Encalada Loja y Aída Guillermina Tenecela Pogyo

DECLARAMOS QUE:

El proyecto de grado titulado "GUÍA DE AUDITORIA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD CATÓLICA DE CUENCA BASADA EN COBIT 5", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el documento, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra autoría.

En virtud de ésta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de Maestría en mención.

Sangolquí, 06 de mayo de 2015

Ing. Carlos Enrique Encalada Loja.

Ing. Aída Guillermina Tenecela Pogyo

AUTORES

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

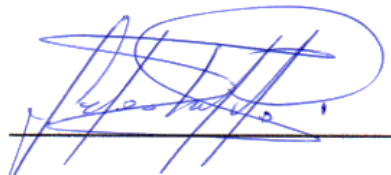
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

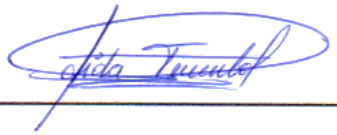
AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, Carlos Enrique Encalada Loja y Aída Guillermina Tenecela Pogyo, portadores de la cédula de identidad 0101805190 y 0301637468 respectivamente. Autorizamos a la Universidad de las Fuerzas Armadas ESPE la publicación, en la biblioteca virtual de la Institución del trabajo "GUÍA DE AUDITORIA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD CATÓLICA DE CUENCA BASADA EN COBIT 5", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, 06 de mayo de 2015



Ing. Carlos Enrique Encalada Loja.



Ing. Aída Guillermina Tenecela Pogyo

AUTORES

DEDICATORIA

A mí esposa Sandra mis hijos: Carlos Andrés, María Mercedes y Carla Andrea cumulo de infinito amor, fuente de inspiración que dirige mi vida con la Gracia de Dios.

A la memoria de mi Abuelita.

Carlos Encalada Loja.

DEDICATORIA

A Carlos Peralta Castro, mi esposo, Carlos Emanuel Peralta Tenecela, mi hijo, mi razón de vivir, este esfuerzo es por ustedes y para ustedes.

A mis padres y hermanas fuente de cariño y comprensión, ejemplo de trabajo y tesón.

Aída Tenecela Pogyo.

AGRADECIMIENTO

A mi familia toda, por el sustento moral y anímico en el trayecto vivido en esta dura pero fructífera tarea.

Un imperecedero agradecimiento a La Universidad Católica de Cuenca por intermedio de su Rector Titular Dr. Enrique Pozo Cabrera, por el soporte institucional para quienes mi infinita gratitud.

Al Ing. Mario Ron e Ing. Rubén Arroyo, por su amistad y profesionalismo.

Al Ing, Fernando Garrido por su acertada dirección.

A mi compañera Aida Tenecela por su paciencia, dedicación y esfuerzo para alcanzar esta meta.

A todos quienes de una u otra manera compartieron su tiempo desinteresadamente y apoyaron la realización de este trabajo de titulación.

Que Dios les bendiga siempre…

Carlos Encalada Loja.

AGRADECIMIENTO

A Dios, por darme la vida y la oportunidad de hacer realidad este sueño.

A Carlos Peralta Castro, por apoyarme desde el primer día que te comenté mi deseo de iniciar este sueño, a ti y a tu familia por cuidar de nuestro hijo durante el tiempo invertido en lograr esta meta.

A mis padres, mis hermanas, mis compañeros y compañeras de trabajo, amigos y amigas, quienes me alentaron siempre a cumplir este objetivo.

Al Ing. Marcelo Cárdenas Molina y Lcda. Cecilia Calle, por su constante motivación para la realización de este programa de Maestría.

A la Universidad Católica de Cuenca y al Personal que participó en la realización de este trabajo, por su tiempo y colaboración.

Al Ing. Fernando Garrido Sánchez, por la acertada orientación que supo brindarnos en el desarrollo de este proyecto.

A mi compañero, Carlos Encalada Loja por su gran esfuerzo y dedicación.

A Fátima Baculima, Pilar Morquecho y Angelo Núñez, compañeros de aula, gracias por su comprensión, por su paciencia y por todos los momentos vividos durante el desarrollo del programa de maestría.

Aída Tenecela Pogyo.

ÍNDICE GENERAL

ÍNDICE DE TABLAS.

ÍNDICE DE FIGURAS

RESUMEN

El objetivo de este trabajo de titulación es realizar una Guía de Auditoría para evaluar el Control Interno de la Seguridad de la Información de la Universidad Católica de Cuenca. La metodología para la elaboración de la Guía de Auditoría, se basó en entrevistas a los auditados partiendo de la identificación del alcance y los objetivos de la auditoría, luego se realizó el estudio inicial del entorno a auditar y se determinó los recursos necesarios para realizar la auditoría, con la información obtenida y procesada se elaboró el plan de trabajo que permitió desarrollar las actividades de auditoría en base a la identificación de los objetivos empresariales y el uso de los apéndices del marco de referencia COBIT 5 para Seguridad de la Información, se realizó un mapeo de los objetivos y procesos de TI y se elaboró 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 Institución, principalmente en base al proceso DSS05 denominado "Gestionar los servicios de seguridad" de COBIT 5. Como resultado se obtuvo un diagnóstico del Control Interno de la Seguridad de la Información de la Universidad Católica de Cuenca y se pudo establecer los hallazgos de auditoria que se plasmaron en el informe final de auditoría. Como fase final se elaboró la carta de presentación dirigida a la alta dirección a quien se informó de los hallazgos más críticos que requieren urgente atención.

PALABRAS CLAVES:

- **GUÍA DE AUDITORÍA**
- **CONTROL INTERNO**
- **COBIT 5 PARA SEGURIDAD DE LA INFORMACIÓN**
- **BUENAS PRÁCTICAS**

ABSTRACT

The aim of this certification work is to do an Audit Guide for the evaluation of Internal Control Information Security for the Universidad Católica de Cuenca. The methodology for developing the Audit Guide for assessing information security was based on interviews with the audited people based primarily on identifying the scope and objectives of the audit. After that, the initial study was performed in the audited scenario and resources needed to conduct the audit. The information obtained and processed helped to make the work plan that allowed developing audit activities based on identifying business objectives and use of COBIT 5 reference frame appendices. For Information Security a mapping of targets and IT processes was made. The main instruments were elaborated for implementing the Audit Guide, which once implemented allowed to identify the initiatives of Information Security that were applied by the institution mainly based on DSS05 process called Manage security services of COBIT 5. As a diagnosis result of Internal Control Information Security of the Universidad Católica de Cuenca was obtained and could set the audit findings reflected in the final audit report. The final step was to write the presentation letter to senior management who were informed of the most critical findings requiring urgent attention.

KEYWORDS:

- **GUIDE AUDIT**
- **INTERNAL CONTROL**
- **COBIT 5 FOR SECURITY OF INFORMATION**
- **BEST PRACTICES**

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, cada vez existe más empresas e instituciones del sector público y privado que han tomado conciencia de la importancia de la Seguridad de la Información a fin de generar confianza en todas las partes interesadas.

En este sentido COBIT[1] 5 es un marco de gobierno de las tecnologías de información que proporciona una serie de herramientas para que la Dirección Institucional pueda relacionar los objetivos de control con los aspectos técnicos y los riesgos de la Institución en el área de la Seguridad de la Información. (ISACA-COBIT 5, 2012)

La Seguridad de la Información basado en el marco de COBIT 5, proporciona una guía más detallada y práctica para los profesionales de seguridad de la Información y otras partes interesadas a todos los niveles de la empresa.

Lo que se pretende con el desarrollo de este trabajo de investigación, es realizar una Guía de Auditoría para la evaluación del Control Interno de la Seguridad de la

[1]COBIT.- Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información..

Información enfocada al mejoramiento de la misma en la Universidad Católica de Cuenca (UCACUE). En primera instancia se identificará las iniciativas en seguridad de la información implementados por la Universidad Católica de Cuenca, 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 permitirá determinar cuánto se debe mejorar en el proceso de seguridad y el alcance de las políticas de Seguridad de la Información a ser propuestas.

La estructuración del presente documento se inicia con los antecedentes, la justificación e importancia del proyecto, el planteamiento y formulación del problema así como los objetivos que se pretende alcanzar con la aplicación a un caso práctico de Auditoria.

En el Capítulo I, se desarrolla el marco teórico y conceptual que servirá como base para la elaboración de la Guía de Auditoría; en el Capítulo II se determina la metodología a aplicar y se elabora la Guía de Auditoría de acuerdo a las fases de la metodología de referencia, en el Capítulo III contempla la información correspondiente a los resultados del trabajo realizado y la forma en la que fueron ejecutados; finalmente en el Capítulo IV se determinan las conclusiones y recomendaciones en función de los resultados alcanzados.

ANTECEDENTES

La Universidad Católica de Cuenca (UCACUE) está ubicada en la ciudad de Cuenca de la provincia del Azuay y desde hace 44 años está al servicio de la colectividad formando profesionales con sólida preparación científica y técnica.

La Universidad Católica de Cuenca cuenta con un departamento de Tecnologías de Información y Comunicación, que gestiona y administra sus recursos tecnológicos, brinda servicios de TI[2] y facilita la gestión de toda la información de sus estudiantes, docentes, personal administrativo, matrículas, calificaciones, mallas curriculares, proyectos, entre otros a través del sistema SIGEAC[3] de desarrollo

[2] TI.- Tecnologías de la Información
[3] SIGEAC.- Sistema de Gestión Académico de desarrollo propio de la Universidad Católica de Cuenca.

propio; en la actualidad se encuentra en la fase de migración a una plataforma ERP[4] para el control integrado de todos los procesos, como parte de su objetivo organizacional y administrativo.

La importancia de la información para la Institución exige que se implementen un conjunto de métodos y herramientas que permitan proteger la información ante cualquier amenaza ya sean estas internas o externas, originadas accidentalmente o con un fin determinado, que pueda afectar las características principales de la seguridad como son la confidencialidad, integridad y disponibilidad de la información.

Actualmente existen instituciones como ISACA[5], que han trabajado sobre el tema de Seguridad de la Información y proporciona una guía más detallada y práctica para los profesionales de Seguridad de la Información ante los problemas de confidencialidad, integridad y disponibilidad que afectan a la información y los activos de TI relacionados con ella, cada vez con mayor frecuencia en las instituciones o empresas. COBIT 5 para la Seguridad de la Información fue diseñada como una guía que ofrece principios, prácticas, herramientas analíticas y modelos globalmente aceptados, diseñados para ayudar al negocio y a los líderes de TI a maximizar la confianza y el valor de la información y los activos tecnológicos de las empresas. (Computerworld Mexico, 2012)

JUSTIFICACIÓN E IMPORTANCIA

Por lo descrito en los antecedentes, se ha considerado necesario que la Universidad Católica de Cuenca cuente con una Guía de Auditoría para la evaluación del Control Interno de la Seguridad de la Información cuyos resultados de aplicación le permita una gestión efectiva y mejoramiento continuo.

La Secretaría Nacional de Administración Pública, SNAP, mediante acuerdo ministerial número 166, dispone a las entidades de la Administración Pública

[4] ERP.- Sistema de Planificación de Recursos Empresariales.

5 ISACA es el acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.

Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000[6] para la Gestión de Seguridad de la Información, que deberán dar cumplimiento al Esquema Gubernamental de Seguridad de la Información de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información (SNAP, Secretaría Nacional de la Administración Pública, 2013). Esto constituye para el sector público un avance en implementación de Seguridad de la Información, sin embargo no existe normativa que exija las Universidades Privadas su implementación., para el caso de las Instituciones de Educación Superior cofinanciada, es decir, que manejan fondos públicos, la obligación del cumplimiento del entorno regulatorio exige a la Universidad Católica de Cuenca su implementación.

La utilización de las Normas ISO/IEC 27000:2005[7] y actualmente ISO/IEC 27000:2013[8] se ha ampliado en muchas empresas tanto a nivel público como privado; y, consiste en una serie de estándares internacionales que ofrece recomendaciones para realizar la gestión de la Seguridad de la Información, con el objetivo de proporcionar una base común para desarrollar normas de seguridad dentro de la organización por lo que puede ser implementado en el sector privado y de educación.

COBIT 5 para seguridad de la información, basado en el marco de COBIT 5, puede ser adoptada por instituciones tanto públicas como privadas en sus esfuerzos para aplicar seguridad de la información como una guía para el gobierno y la gestión de la Seguridad de la Información.

La Universidad Católica de Cuenca, consciente de la importancia de la protección del activo más crítico que es la información, ha auspiciado decididamente el desarrollo de este trabajo de titulación, con el firme propósito de establecer políticas basadas en las mejores prácticas mediante el alineamiento con el marco de referencia COBIT 5 que es reconocido mundialmente.

6 NTE INEN-ISO/IEC 27000.- Norma Técnica Ecuatoriana para la gestión de la seguridad de la información.
7 ISO/IEC 27000:2005.- Estándares de seguridad publicados por la organización Internacional Para la Estandarización y la Comisión Electrotécnica Internacional en el año 2005
8 ISO/IEC 27000:2005.- Estándares de seguridad publicados por la organización Internacional Para la Estandarización y la Comisión Electrotécnica Internacional en el año 2013

PLANTEAMIENTO DEL PROBLEMA

El departamento de Tecnologías de Información y Comunicación de la Universidad Católica de Cuenca, es la dependencia que se encarga de mantener actualizados y custodiar los sistemas de información así como de brindar apoyo a los procesos académicos, administrativos y de investigación.

Los sistemas de TI vulnerables pueden exponer a los directores de la institución a no cumplir con las leyes lo que genera problemas en el buen desarrollo de sus actividades. La utilización de las redes de computadoras como un sistema de comunicación, proporciona nuevos horizontes a las Instituciones Educativas para mejorar el proceso de enseñanza-aprendizaje y poder explorar más allá de las fronteras locales, lo que lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información y la Seguridad de la Información.

Un problema constante al no disponer de una guía de auditoría que permita una validación del control interno aplicado a la seguridad de la información, enfocado en la protección de toda la infraestructura computacional, tanto física como lógica. Los sistemas de información deberían tener un alto grado de seguridad, porque los datos de toda la Universidad están albergados en los servidores locales, por lo que es crítica toda su infraestructura.

Estos riesgos que se enfrentan diariamente, sumado a la carencia de guías y controles que permitan validar y orientar si las metodologías implementadas cumplen sus objetivos, si la seguridad en los servicios cumple con los requisitos mínimos para su incorporación e implementación, si la atención de los incidentes y vulnerabilidades son encaminados y gestionados adecuadamente, si los niveles de defensa perimetral e interna definidos disponen de un mecanismo efectivo para validar su implementación, si los sistemas están adecuadamente configurados y asegurados, si existe una arquitectura de seguridad definida, si existen procesos identificados e implementados dentro de la Universidad, constituyen un problema cada vez más preocupante y de atención urgente.

FORMULACIÓN DEL PROBLEMA

¿Cómo una guía de Auditoría mediante la adopción de COBIT 5 como un marco metodológico y de buenas prácticas, permitirá evaluar el control interno de la Seguridad de la Información de la Universidad Católica de Cuenca?

¿Cómo COBIT 5 puede contribuir a la implementación de iniciativas de Seguridad de la Información?

¿De qué manera una guía de auditoría con un enfoque ágil soportará la toma de decisiones acerca de los riesgos de la información?

OBJETIVO GENERAL

Desarrollar una Guía de Auditoría basada en COBIT 5 como marco de referencia y mejores prácticas, para la evaluación del Control Interno de Seguridad de la Información en la Universidad Católica de Cuenca.

OBJETIVOS ESPECÍFICOS

- Identificar los componentes del marco de referencia COBIT 5 para el Gobierno y la Gestión de Seguridad de la Información para documentar una guía de auditoría para la evaluación del Control Interno en la Universidad Católica de Cuenca.
- Obtener un diagnóstico del Control Interno del nivel de seguridad de los servicios TI de la Universidad Católica de Cuenca y establecer el grado de madurez con respecto a la Guía de Auditoría construida.
- Mantener un proceso de evaluación de Control Interno aplicado a la Seguridad de la Información para la protección de los recursos de TI relacionados de la Universidad Católica de Cuenca, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

CAPÍTULO I

1 FUNDAMENTACIÓN TEÓRICA

1.1 Marco Teórico

El entorno tanto de una empresa u organización así como en las Instituciones de Educación Superior 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.

La auditoría de sistemas enfocada solo al cumplimiento normativo no representa ningún tipo de interés para la alta dirección y las gerencias, en el mejor de los casos cumplir con la ley. Este tipo de escenarios 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) gestionable y acorde con las necesidades del negocio, así como unos servicios de tecnología altamente eficientes. (Díaz, 2012)

Actualmente, 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. A fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones. (Galán, 1996)

Otro factor importante a tomar en cuenta en el tema de la seguridad de la información, es el desarrollo acelerado de las redes informáticas, esto trajo consigo un aumento considerable en la velocidad de procesamiento y en la transmisión de información del negocio, 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 han 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[9]

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.

La posición de COBIT 5 sobre esta fundamental distinción entre es:

- Gobierno: El Gobierno asegura 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. (ISACA-COBIT 5, 2012).

[9] ISO 27002: 2013.- Código de prácticas para la gestión de la Seguridad de la Información actualizada en el año 2013

- Gestión: La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. (ISACA-COBIT 5, 2012)

En COBIT 5, los procesos APO13[10] Gestionar la seguridad, DSS04[11] Gestionar la continuidad y DSS05[12] 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 empresa, con aspectos de Seguridad de la Información dentro de cada actividad y proceso realizado. Por lo tanto, COBIT 5 para Seguridad de la Información proporciona la nueva guía de ISACA para el gobierno y la gestión corporativa de la seguridad de la información. (ISACA-COBIT 5, 2012)

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 IT, usuarios y por supuesto los auditores involucrados en el proceso" (EAFIT Universidad, 2007).

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. (ISO org, 2014)

1.2 Metodología de investigación

La metodología para el desarrollo de la guía de auditoría de evaluación de la Seguridad de la Información en la Universidad Católica de Cuenca, empleará 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

[10] APO13.- Proceso número trece del dominio Alinear, Planificar y Organizar del marco de referencia COBIT 5.
[11] DSS04.- Proceso número cuatro del dominio Entregar, Dar Servicio y Soporte del marco de referencia COBIT 5.
[12] DSS05.- Proceso número cinco del dominio Entregar, Dar Servicio y Soporte del marco de referencia COBIT 5

analiza a diferentes autores que proponen metodologías de auditorías de sistemas en general, aplicable al tema de Seguridad de la Información en las siguientes fases:

- **Fase 1**. Identificar el alcance y los objetivos de la Auditoría Informática. En esta fase se determinan los límites y el entorno en que se realizara la auditoría, es el momento donde se determina hasta donde debe llegar la tarea, debe existir un acuerdo muy preciso entre autoridades y usuarios sobre las funciones (seguridad, dirección, etc.). El éxito del proceso de auditoría depende de una clara definición de esta fase (Kuna, 2006).
- **Fase 2.** Realizar el estudio inicial del entorno a auditar. En esta fase es necesario examinar las funciones y actividades generales de la organización a auditar y en particular de las relacionadas con las tecnologías de la información. Se debe obtener información sobre:
    - La organización (definir el organigrama)
    - Los departamentos.
    - Las relaciones funcionales y jerárquicas entre las distintas áreas de la organización
    - El flujo de información,
    - El número de puestos de trabajo y personas por puesto de trabajo.
    - La estructura organizativa del departamento de informática, características de hardware y software, las metodologías de desarrollo y mantenimiento de aplicaciones, y aspectos relacionados con la seguridad (Kuna, 2006).
- **Fase 3.** Determinación de los recursos necesarios para realizar la auditoría de sistemas. Después de realizar el estudio preliminar se debe determinar los recursos materiales y humanos necesarios para implementar el plan de auditoría. (Kuna, 2006)
- **Fase 4.** Elaborar el Plan de Trabajo. En esta fase se definen el calendario de actividades a realizar. (Kuna, 2006)
- **Fase 5.** Realizar las actividades de auditoría. Es el momento donde se efectivizan las actividades planificadas en la fase anterior, se aplica distintas técnicas y se utiliza herramientas que garanticen el cumplimiento de los objetivos planteados. (Kuna, 2006)

- **Fase 6.** Realizar el Informe Final. El objetivo final del auditor es entregar por escrito un informe, en donde constarán las conclusiones y recomendaciones. El auditor justifica personalmente su auditoría en forma documentada. "La elaboración del Informe Final es la única referencia constatable de toda auditoría, y el exponente de su calidad" (Kuna, 2006).
- **Fase 7.** Carta de Presentación. Es la última etapa de la auditoría consta de un resumen de 3 o 4 folios del contenido del informe final, dirigida a las autoridades de la empresa u organización donde se realizó la auditoría. (Kuna, 2006).

1.3 Antecedentes del estado del arte

La información es uno de los recursos más importantes en las Instituciones, durante todo el ciclo de vida de la misma, la tecnología juega un papel muy importante debido al uso generalizado en todo tipo de empresas, por lo que, se vuelve menester gestionar adecuadamente la seguridad de la información.

La definición de "Seguridad de la Información" según ISACA: son procesos de protección contra divulgaciones a usuarios no autorizados (confiabilidad), modificaciones no adecuadas (integridad) y falta de acceso cuando se requiere (disponibilidad). (ISACA, 2012)

Ante estos problemas de confidencialidad, integridad y disponibilidad que afectan a la información y los activos de TI relacionados con ella en las instituciones o empresas cada vez con mayor frecuencia, se diseñó COBIT 5 para la seguridad de la información.

En la actualidad la lucha desigual por la seguridad es más difícil y complicada, el aprovechamiento de la confianza es una manera frecuente de operación para los atacantes y otros actores malintencionados. Se aprovechan de la confianza que tienen los usuarios en sistemas, aplicaciones, las personas y los negocios con los que interactúan regularmente. Entonces los ataques sofisticados y específicos afectan los activos críticos de la cadena de valor de las empresas e instituciones de educación

superior, en segundos; mientras que se necesitan semanas, meses o años para que las violaciones de seguridad puedan detectarse. Para frenar la gran cantidad de ataques modernos es preciso contar con mejores prácticas y tecnologías que permitan la operación continua y fortalecimiento de las instituciones.

Las vulnerabilidades y amenazas informadas por CISCO[13] mostraron un crecimiento sostenido en 2013, a partir de octubre del mismo año los totales de alertas anuales acumulados aumentaron un 14% interanual desde 2012. (CISCO, 2014)

El número de nuevas alertas en 2013 y 2014 indica que se registraron más vulnerabilidades que en años anteriores; lo que se traduce en que los proveedores, los desarrolladores y los investigadores de seguridad trabajan para encontrar, corregir y registrar más vulnerabilidades en sus productos. En comparación con 2013, el número total de nuevas alertas y la cifra total anual no presentan ninguna variación o muestran un leve descenso durante 2014. (CISCO, 2015)

Los usuarios no sólo son el objetivo de los ataques informáticos, sin saberlo son utilizados para efectuarlos. Durante el 2014 las investigaciones hechas por Cisco revelaron que los atacantes han dejado de lado cada vez más su enfoque de comprometer servidores y sistemas operativos que infectan a los usuarios por medio del navegador y correo electrónico. CISCO afirma que la descarga de sitios comprometidos por parte de los usuarios contribuyó a un aumento del 228% en los ataques de Silverlight[14], junto con un incremento del 250% en las infecciones silenciosas por medio de spam y publicidad maliciosa. (CISCO, 2015)

En Latino América, en el año 2014 los tipos de fallas de seguridad como: el fraude, robo de datos, pérdida de integridad y acciones de ingeniería social presentan un incremento con respecto del año 2013, además surgen fallas de seguridad como los incidentes relacionados con la privacidad de los datos, así como plataformas para atacar otras empresas, que no se reportaron en años anteriores. (Cano Martínez, 2014)

---

[13] CISCO es una empresa de telecomunicaciones, servicios de consultoría y educación en temas de comunicación en redes.

[14] Silverligth.- Es un plug-in de navegador web gratuito que permite mejorar la experiencia interactiva multimedia.

Durante el año 2014 se observa un incremento en el porcentaje de empresas Latinoamericanas que poseen una política formal de Seguridad e Información, documentada e informada a todo el personal que va del 44.58% al 49.38%. En ese mismo año, existe un 38.17% de empresas que no tienen implementadas normas, regulaciones o buenas prácticas referentes a Seguridad de la Información. El 63.33% de las empresas que han tomado la decisión de adoptar estándares y buenas prácticas han optado por ISO 27001 y un 19.63% por COBIT 4.1 /5 (Cano Martínez, 2014)

En América Latina, la fuga de información sensible así como la seguridad y control de la computación en la nube encabezan la lista de los principales problemas de TI que representarán desafíos para la seguridad de una organización. La falta de alineación entre las funciones de Seguridad de la Información y las necesidades de Desarrollo Organizacional se evidencia en que el principal obstáculo para su implementación constituye la falta de apoyo directivo. (Cano Martínez, 2014)

En Ecuador a pesar de que se han hecho esfuerzos, todavía no se trabaja en seguridad de manera sistemática con políticas definidas para el sector de las Universidades, de acuerdo a la encuesta que fue enviada a los representantes de las Universidades miembros de CEDIA[15], 29 universidades en total. Esta encuesta tuvo el carácter de anónimo y de contestación opcional para los participantes. El 37,97 % (11) de las universidades miembros respondieron al llamado de la encuesta. (CEDIA, 2014).

Se resalta el estudio estadístico de algunas preguntas, como el presupuesto asignado para la Gestión de la Seguridad de la Información reveló que el 82% de las Universidades no tiene asignado un presupuesto para trabajar exclusivamente para la Gestión de la Seguridad y el 18% si lo tiene. Sobre la línea de Investigación en el campo de la Seguridad de la información, los resultados fueron que el 91% no lo tiene y el 9% si, la investigación que se realiza en este 9% corresponde a Vulnerabilidades. (CEDIA, 2014)

[15] CEDIA Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado, forma parte del Proyecto Internet2 desde Octubre del 2002, a través de un Memorando de Entendimiento con la Corporación UCAID (University Corporation for Advance Internet Development) de USA.

Más del 82% de las Universidades que contestaron la encuesta han trabajado y están trabajando en Políticas o Normativas de Seguridad, por lo que se puede apreciar un interés por las instituciones por Gobernar la Seguridad de la Información. (CEDIA, 2014)

En este sentido mantener la relación entre la tecnología, los procesos y el recurso humano, requiere establecer un marco de gestión integral basado en COBIT 5, que sintetice y aterrice las inversiones de Seguridad de la Información para generar el valor esperado de la seguridad en la Institución.

La inversión y la gestión de la Seguridad de la Información son dos temas complementarios, los que sugieren establecer un control interno que permita comprender por una parte, las relaciones que exige la seguridad en la Universidad Católica de Cuenca (UCACUE) y por otro, la detallada lista de actividades y acciones que se requieren para viabilizar el concepto intangible de la Seguridad de la Información mediante la aplicación de Auditoria de evaluación de los niveles de seguridad (Soy i Aumatell, 2002).

Es necesario entonces formalizar un modelo de gestión de seguridad que considere el área crítica de TI, es decir, todas las operaciones y control que permitan el análisis e interpretación de información generada por la evaluación del control interno a través de actividades que aporten conocimiento considerable a la UCACUE para que pueda llevar a cabo sus actividades en un ambiente seguro, así como disminuir notablemente la acción de los riesgos inherentes a las labores informatizadas dentro de TI.

En consecuencia hablar sobre seguridad de la información es lograr un permanente ciclo de mejora sobre: tecnología, procesos y personas que establecen relaciones tangibles, en la asignación de recursos, para producir un bien intangible como lo es la seguridad desde el punto de vista de la información considerada como un activo critico empresarial.

1.4 Marco conceptual

1.4.1 Control Interno

- **Generalidades.**

El Control Interno se define como un proceso llevado a cabo por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objetivo de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos relacionados con las operaciones, la información y el cumplimiento. Esta definición refleja ciertos conceptos fundamentales:

- Está orientado a la consecución de objetivos en una o más categorías, operaciones, información y cumplimiento.
- Es un proceso que consta de tareas y actividades continuas, es un medio para llegar a un fin y no un fin en sí mismo.
- Es efectuado por las personas, no se trata solamente de manuales, políticas, sistemas y formularios, sino de personas y las acciones que éstas implican en cada nivel de la organización para llevar a cabo el control interno.
- Es capaz de proporcionar una seguridad razonable, no una seguridad absoluta, al consejo y a la alta dirección de la entidad.
- Es adaptable a la estructura de la entidad, flexible para su aplicación al conjunto de la entidad o a una filial, división, unidad operativa o proceso de negocio en particular. (Instituto de auditores internos de España, 2013)

El Marco COSO[16] establece tres categorías de objetivos, que permiten centrarse en diferentes aspectos del control interno:

- Objetivos Operativos.- Hacen referencia a la efectividad y eficiencia de las operaciones de la entidad, incluidos sus objetivos de rendimiento financiero y operacional, y la protección de sus activos frente a posibles pérdidas.

[16] Committee of Sponsoring Organizations of the Treadway Commission

- Objetivos de información.- Hacen referencia a la información financiera y no financiera, interna y externa y pueden abarcar aspectos de confiabilidad, oportunidad, transparencia y otros conceptos establecidos por los reguladores, organismos reconocidos o políticas de la propia entidad.
- Objetivos de cumplimiento.- Hacen referencia al cumplimiento de las leyes y regulaciones a las que está sujeta la entidad. (Instituto de auditores internos de España, 2013)

- **Componentes del control interno**

El control interno consta de cinco componentes los que se relacionan entre sí, y deben estar integrados en el proceso de gestión. Estos componentes son:

- Entorno de control.
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión (Instituto de auditores internos de España, 2013)

- **Clasificación de los controles**

Los controles se pueden clasificar de la siguiente manera:

- **Preventivos**.- anticipan eventos no deseados antes de suceder
- **Detectivos**.- Identifican eventos en el momento en que se presentan.
- **Correctivos**.- Aseguran tomar acciones para revertir un evento no deseado (Espinoza Cruz, 2009).

- **Control interno en TI**

El uso de las tecnologías de la información hace cada vez más relevante la implementación del control interno en las áreas de TI de las organizaciones, por lo que persigue los siguientes objetivos: establecer como prioridad la

seguridad y protección de la información, del sistema computacional y de los recursos informáticos de la empresa; promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa; implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa e instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa; establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa. (Muñoz Razo, 2002)

Según la estructura COSO 2013:

- Las actividades de control se realizan en todos los niveles de la entidad, en las diversas etapas de los procesos de negocio, y sobre el entorno de TI.
- Las actividades de control y TI se relacionan una con otra de dos maneras: TI apoya los procesos de negocio, TI es usada para automatizar actividades de control.
- La mayoría de los procesos de negocio tienen una mezcla de controles manuales y automatizados, de acuerdo a la disponibilidad de TI en la entidad.
- La confiabilidad de TI en los procesos de negocio depende de la selección, desarrollo, y despliegue de las actividades generales de control de TI.
- Los cambios en TI pueden reducir la efectividad de las actividades de control o hacer redundantes algunas actividades de control, siempre que ocurran cambios la administración debe volver a valorar la relevancia de los controles existentes y refrescarlos cuando sea necesario. (Deloitte, 2013)

1.4.2 Auditoria de la información y la Seguridad de la Información

- **Conceptos de la auditoría de la información**

La palabra auditoría proviene del latín “auditorius”, y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír (Echenique, 2003).

El diccionario Español Sopena lo define como: Revisor de Cuentas colegiado. En un principio esta definición carece de la explicación del objetivo fundamental que persigue todo auditor: evaluar la eficiencia y eficacia (Echenique, 2003)

Knowledge and Information Resources Management Network (Kimnet), se refiere a la Auditoria Informática como: un examen sistemático del uso de los recursos y los flujos de información, verificado con las personas y los documentos existentes, con el propósito de establecer la medida en que éstos contribuyen a los objetivos organizativos.

La auditoría de la información definida como un diagnóstico sobre el uso de la información dentro de una organización constituye una metodología de gestión global idónea para determinar el rol que desarrolla la información en una determinada organización de una forma que resulte inteligible a cualquier gestor. (Soy i Aumatell, 2002)

De los anteriores conceptos descritos se puede deducir que la auditoría de la información es un examen crítico a los elementos propios del control interno o de gestión destinada a identificar posibles problemas, ineficiencias y recomendar soluciones relacionadas con procesos, funciones, áreas diversas de la Institución.

- **Objetivos de la auditoría de la información**

La Auditoria de la Información constituye una práctica de control interno destinada a revisar las operaciones de las diferentes áreas o funciones con el objetivo de informar sobre su funcionamiento lo que promueve recomendaciones para alcanzar mejoras orientadas a proteger el activo de la información y optimizar los recursos disponibles (Soy i Aumatell, 2002).

La auditoría asociada con el análisis de cualquier iniciativa o acción relacionada con la información, supone cumplir con los siguientes objetivos:

- Revisar el uso de la información dentro de la organización.
- Identificar y mapear los recursos de información disponibles.
- Determinar qué información es esencial, por qué y para quién.
- Establecer cómo se utiliza y se comparte.
- Evaluar los costes y el valor de la información.

La información conseguida, debidamente analizada, proporciona una imagen integral sobre la utilización de la información en la organización, la evaluación de los recursos y servicios disponibles. (Soy i Aumatell, 2002)

1.4.3 Seguridad de la información

- **Generalidades**

La seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, disrupción o destrucción no autorizada (ISACA - COBIT 5 para Seguridad de la Información, 2012).

De acuerdo a la conceptualización de ISACA, la Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente del formato que los datos puedan tener: electrónicos, impresos, audio u otras formatos.

Tanto las empresas públicas como las empresas privadas acumulan una gran cantidad de información confidencial, en el caso de la UCACUE sobre sus funcionarios, empleados, estudiantes, investigación y la situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios internos y externos, en computadores y transmitida a través de las redes de datos. El problema radica, cuando esta información vaya a parar en manos de un competidor o se vuelva pública en forma no autorizada, podría causar la pérdida de credibilidad de la Institución, pérdida de negocios, demandas

legales o incluso la quiebra de la misma. Por lo tanto proteger la información confidencial es un requisito funcional del negocio y una obligación legal.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información (ISACA - COBIT 5 para Seguridad de la Información, 2012).

- **Confidencialidad**

La confidencialidad significa preservar las restricciones autorizadas sobre el acceso o divulgación, incluyen los medios para proteger la privacidad y la información propietaria (ISACA - COBIT 5 para Seguridad de la Información, 2012).

La confidencialidad entonces se refiere a que la información solo puede ser conocida por usuarios autorizados. Para la Seguridad de la información es la propiedad de prevención de la divulgación de información a personas o sistemas no autorizados.

- **Integridad**

La Integridad significa proteger contra la destrucción o modificación inadecuada de la información e incluye asegurar el no repudio y autenticidad de la información. (ISACA - COBIT 5 para Seguridad de la Información, 2012)

La integridad se refiere a la seguridad de que la información no ha sido alterada, borrada, o copiada durante el proceso de transmisión o en el propio equipo computacional de origen. Para la Seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de alteraciones no autorizadas.

- **Disponibilidad**

La disponibilidad significa asegurar que se puede acceder y usar la información de manera confiable y en el momento adecuado (ISACA - COBIT 5 para Seguridad de la Información, 2012).

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, es decir, impedir su pérdida o bloqueo, ya sea por ataques, operación accidental, situaciones fortuitas o de fuerza mayor.

No todos los riesgos que amenazan la información son de origen nocivo. Por lo que, las medidas de seguridad no deben limitarse a la protección contra ataques e intrusiones de usuarios externos, pues dentro de la misma organización y por parte de usuarios de confianza existen riesgos contra la disponibilidad de la información ya sea por negligencia, descuido, ignorancia o cualquier otro tipo de mala práctica, la información puede ser alterada, sustituida o permanentemente borrada. Además están siempre presentes los riesgos de pérdida o alteración por virus o situaciones fortuitas de fuerza mayor, tales como incendios, inundaciones o catástrofes naturales. (Soy i Aumatell, 2002)

1.4.4 COBIT 5

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde la tecnología de la información (TI) lo que mantiene el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite que las TI se gobiernen y gestionen de un modo holístico para toda la empresa, abarca al negocio completo de principio a fin y a las áreas funcionales de responsabilidad de TI, considera los intereses relacionados con TI de los grupos de interés internos y externos. COBIT 5 para Seguridad de la Información se basa en los mismos principios que el marco de COBIT 5. (ISACA - COBIT 5 para Seguridad de la Información, 2012)

- **Principios y habilitadores de COBIT**

COBIT 5 se basa en cinco principios para el gobierno y gestión de las TI (ver Fig.1):

- **Principio 1.** Satisfacer las Necesidades de las Partes Interesadas. Las empresas existen para crear valor para sus partes interesadas lo que mantiene el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. (ISACA-COBIT 5, 2012)

  Las partes interesadas son todos aquellos proveedores, clientes, socios, empleados y funcionarios que se ven afectados positivamente o negativamente por las decisiones que se tomen en la Institución. El término "Partes Interesadas" proviene de la palabra inglesa Stakeholder utilizado para referirse a los grupos de interés de una empresa.
- **Principio 2.** Cubrir la Empresa Extremo-a-Extremo. COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo: Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la de función de TI, sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa (ISACA-COBIT 5, 2012)
- **Principio 3**. Aplicar un Marco de Referencia único integrado. Hay muchos estándares y buenas prácticas relativos a TI, cada uno ofrece ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa (ISACA-COBIT 5, 2012).
- **Principio 4.** Hacer Posible un Enfoque Holístico. Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos (ISACA-COBIT 5, 2012).
- **Principio 5**. Separar el Gobierno de la Gestión. El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes

estructuras organizativas y sirven a diferentes propósitos (ISACA-COBIT 5, 2012).

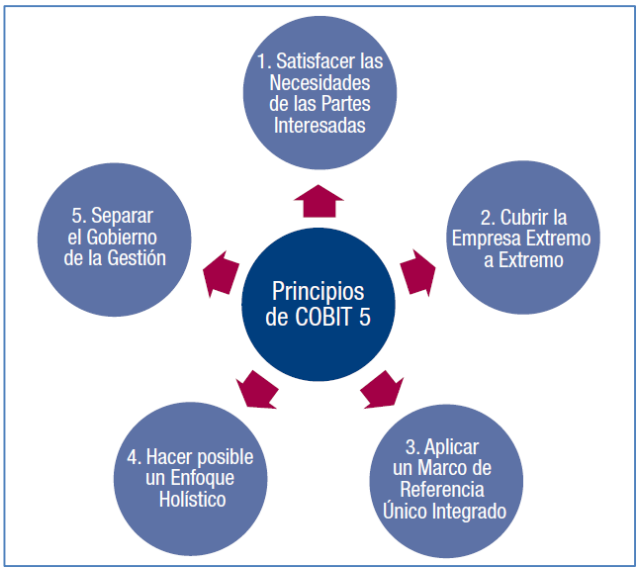


Figura 1. Principios de COBIT 5.
Fuente: (ISACA - COBIT 5 para Seguridad de la Información, 2012, pág. 21)

COBIT 5 define un conjunto de catalizadores o habilitadores para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. COBIT 5 para Seguridad de la información proporciona orientación específica en relación con todos los catalizadores:

- Las políticas, principios y marcos de referencia de Seguridad de la Información.
- Los procesos, que incluyen detalles y actividades específicos de Seguridad de la Información.
- Las estructuras organizativas específicas de Seguridad de la Información.
- En términos de cultura, ética y comportamiento, los factores determinantes para el éxito del gobierno y la gestión de la Seguridad de la Información.
- Los tipos de información específicos de la Seguridad de la Información para permitir el gobierno y la gestión de la Seguridad de la Información en la empresa.

- Las capacidades de servicio necesarias para proporcionar Seguridad de la Información y las funciones relacionadas con la empresa.
- Las personas, habilidades y competencias específicas para Seguridad de la Información.

Para cada catalizador COBIT 5 analiza todos los componentes relevantes y da una descripción específica de Seguridad de la Información de los componentes de los catalizadores y directrices detalladas sobre éstos. (ISACA - COBIT 5 para Seguridad de la Información, 2012)

- **Dominios**

El modelo de referencia de procesos de COBIT 5 divide los procesos en dos dominios principales: **Gobierno y Gestión,** cada uno contiene dominios que son una evolución del estructura de procesos y dominios de COBIT 4.

Gobierno:

- **EDM**.- Evaluar, orientar y supervisar

Gestión:

- **APO**.- Alinear, Planificar y Organizar
- **BAI**.- Construir, Adquirir e Implementar
- **DSS**.- Entrega, Servicio y Soporte
- **MEA**.- Supervisar, Evaluar y Valorar.

En función de estos dominios se establece el modelo de referencia de procesos de COBIT5. (ISACA-COBIT 5, 2012)

- **Matriz RACI**

Las matrices RACI unen las actividades de proceso con las estructuras organizativas y/o los roles individuales en la empresa. Describen el nivel de implicación de cada rol para cada práctica del proceso (ISACA-COBIT 5, 2012):

- (A) Responsable de que se haga,
- (R) Responsable de hacerlo,

- (C) Consultado e
- (I) Informado.

- **Modelo de capacidad de los procesos.**

COBIT 5 introduce una nueva forma de medir la madurez de los procesos a través del "Process Capability Model", basado en el estándar internacionalmente reconocido "ISO/IEC 15504 Software Engineering – Process Assessment Standard", diferente en su diseño y uso al modelo de madurez que incluía COBIT 4.1. (ISACA-COBIT 5, 2012)

Existen seis niveles de capacidad (ver figura 2), que se pueden alcanzar por un proceso, incluida la designación de "proceso incompleto" si las prácticas definidas en el proceso no alcanzan la finalidad prevista; a continuación se describen estos seis niveles:

- Proceso incompleto.- El proceso no está implementado o no alcanza su propósito. A este nivel, hay poca o ninguna evidencia del logro sistemático del propósito del proceso.
- Proceso ejecutado.- El proceso implementado alcanza su propósito.
- Proceso gestionado.- El proceso ejecutado se encuentra implementado de forma gestionada (planificado, supervisado y ajustado); los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
- Proceso establecido.- El proceso gestionado está ahora implementado y utiliza un proceso definido que es capaz de alcanzar sus resultados de proceso.
- Proceso predecible.- El proceso establecido se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.
- Proceso optimizado.- El proceso predecible es mejorado de forma continua para cumplir con los metas empresariales presentes y futuros.

Cada nivel de capacidad puede ser alcanzado sólo cuando el nivel inferior se ha alcanzado por completo. (ISACA-COBIT 5, 2012)

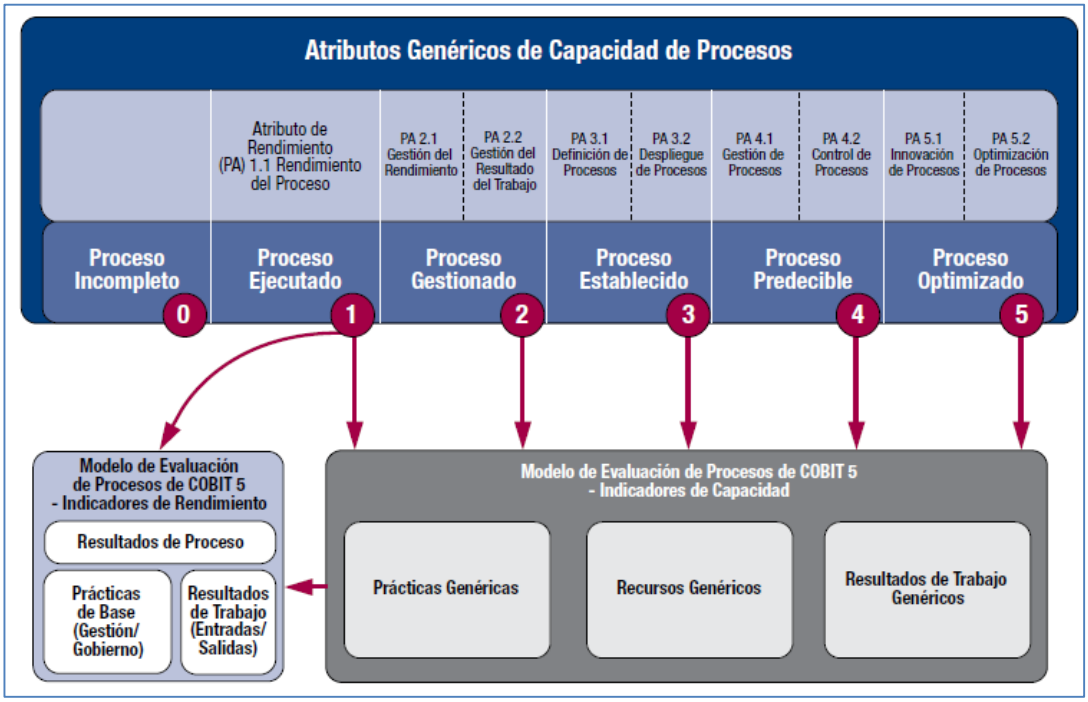


Figura 2. Resumen del Modelo de Capacidad de Procesos de COBIT 5
Fuente: (ISACA - COBIT 5 para Seguridad de la Información, 2012, pág. 42) .

➢ Beneficios de COBIT 5 para Seguridad de la Información

Utilizar COBIT 5 para Seguridad de la Información proporciona a la empresa una serie de capacidades relacionadas con la Seguridad de la Información que puede resultar en beneficios como:

- Menor complejidad y mayor coste-beneficio debido a una mejorada y más fácil integración de estándares buenas prácticas y/o guías específicas del sector de Seguridad de la Información.
- Mayor satisfacción de usuario con la estructura y resultados de Seguridad de la Información.
- Mejor integración de la Seguridad de la Información en la empresa.
- Toma de decisiones de riesgo con conocimiento y conciencia del riesgo.
- Mejor prevención, detección y recuperación.
- Reducción (del impacto) de los incidentes de Seguridad de la Información.
- Soporte mejorado a la innovación y la competitividad.
- Mayor conocimiento de la Seguridad de la Información. (ISACA - COBIT 5 para Seguridad de la Información, 2012)

CAPÍTULO II

2 MEMORIA TÉCNICA METODOLÓGICA

2.1 Ejecución del proceso de investigación.

En este apartado se describen las herramientas y técnicas utilizadas para recopilación de información que permiten realizar el proceso de planeación de la Auditoría al Control Interno de la Seguridad de la Información aplicado en la Universidad Católica de Cuenca.

2.1.1 Entrevista.

La entrevista se fundamenta en el concepto de interrogatorio; que consiste en que bajo la forma de una conversación correcta y fluida en lo posible, el auditado conteste concretamente a una serie de preguntas variadas, que se formulan de manera sencilla. Sin embargo, esta sencillez es solo aparente, tras ella existe una preparación muy elaborada y sistematizada que es diferente para cada caso en particular. (Cano, 2007)

2.1.2 Checklist.

Esta técnica consiste en la aplicación de cuestionarios preestablecidos concentrándose en las áreas específicas de los escenarios auditados, que permitirán la complementación sistemática de la información relevante para establecer el cumplimiento o no de los objetivos.

En base a respuestas claras y concisas por parte del Auditado, se deberá mantener una directriz constante durante el diálogo de búsqueda de evidencias (Cano, 2007)

2.2 Guía de Auditoría para la Evaluación del Control Interno de la Seguridad de la Información en la UCACUE.

La Guía de Auditoría para la Evaluación del Control Interno de la Seguridad de la Información en la UCACUE, comprende la evaluación de los elementos relacionados con la tecnología de la información, como:

- Seguridad Perimetral,
- Acceso a los Sistemas de aplicación,
- Seguridad Física y Lógica,
- Los Usuarios

Con el objetivo de garantizar el cumplimiento de las normas y procedimientos establecidos por la Institución de Educación Superior en todo lo relacionado con la información y la tecnología de la información, de tal manera, que se pueda minimizar los riesgos que amenacen la confidencialidad, integridad y disponibilidad de la información.

La Universidad Católica de Cuenca estima que su información es la base de su funcionabilidad, es decir, considera un activo estratégico que diariamente está expuesto y sometido a nuevos y graves riesgos: Hackeo, virus, averías, errores humanos.

Estas amenazas tienen efectos insospechados, que como consecuencia imposibilitan que la información aporte el valor que tiene, por lo que, es vital controlar la inseguridad y la desconfianza que esto genera.

No es posible eliminar las amenazas, se debe reducir la posibilidad de que actúen y el perjuicio que pueden ocasionar. Esto significa que se pueda controlar el riesgo para generar seguridad y confianza, con lo que se aporta veracidad y calidad a la información tratada. Por ello es necesario proteger la información y la confianza de las partes interesadas, mediante la implementación de controles efectivos que permitan alcanzar una verdadera “cultura de la seguridad” con el compromiso de la Dirección, Administración y Funcionarios de la institución.

La aplicación de la "Guía de Auditoría basada en COBIT 5", pretende desarrollar un proceso de mejora continua y maduración, a través de la evaluación y mejores prácticas, con el propósito de apoyar a la Universidad Católica de Cuenca para la protección de los recursos de TI relacionados.

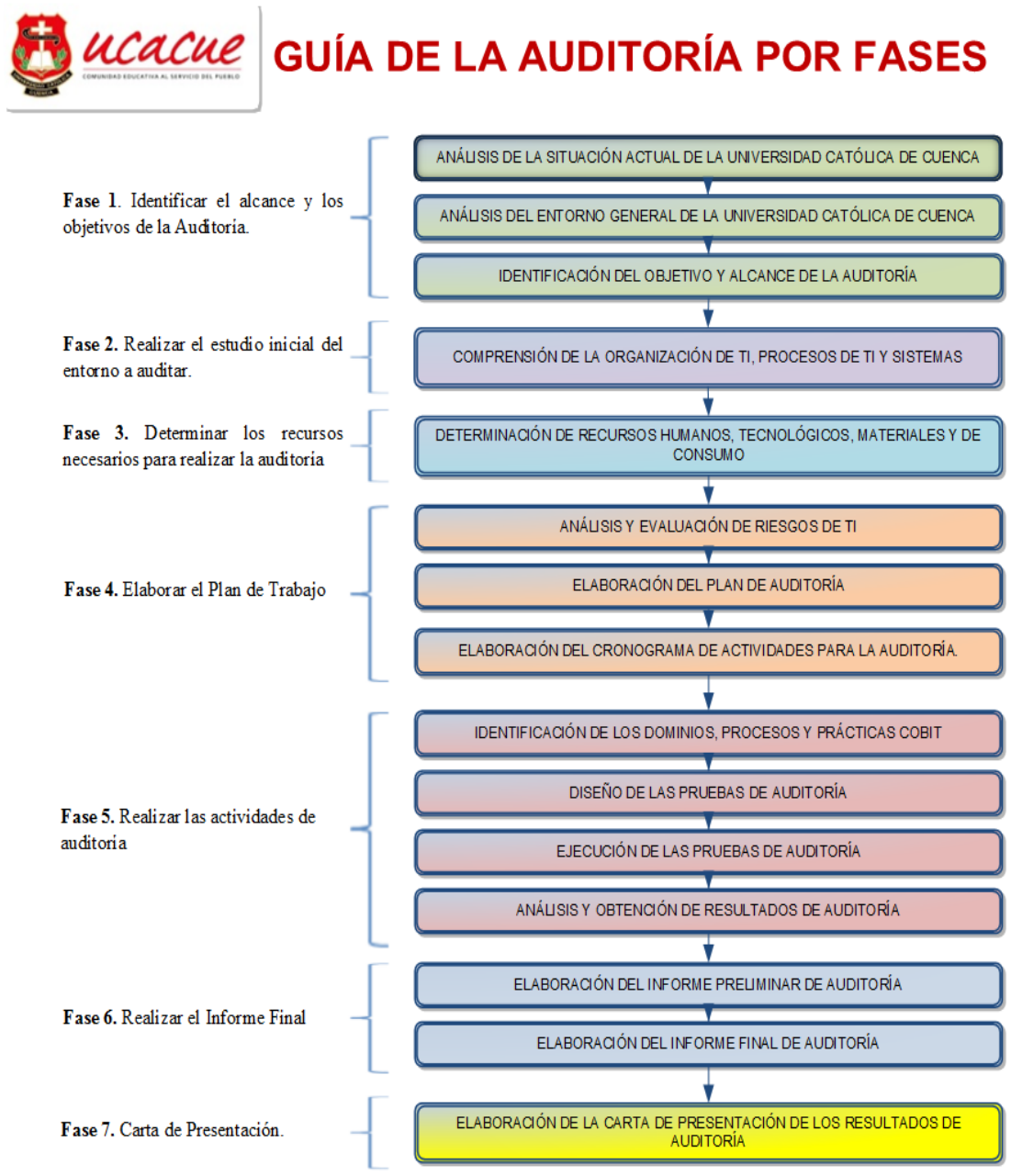


Figura 3. Guía de auditoría por fases
Fuente: Autores (Adaptado de Kuna, 2006)

2.2.1 Planeación Previa

Para el desarrollo de la "Guía de Auditoría para la Evaluación del Control Interno de Seguridad de la Información", es importante conocer el entorno de la UCACUE y del área de Tecnología de la Información y Comunicación tales como: procesos sistematizados, organización del área de tecnología de información y comunicaciones, planes estratégicos de TI, planes operativos, planes de contingencia y/o continuidad del negocio relacionado con la Seguridad de la Información, plataforma tecnológica con la que cuenta la institución. De esta manera se obtiene una adecuada planificación del trabajo a realizar. El conocimiento como producto del análisis da como resultado un marco conceptual, que permite evaluar si la UCACUE sigue un enfoque estructurado de gestión de la seguridad información y si éste es pertinente (ver Figura 3).

- **Situación actual de la Universidad Católica de Cuenca.**

La Universidad Católica de Cuenca nace como una respuesta al clamor de los pueblos de Azuay, Cañar y Morona Santiago, que no contaban con alternativas educativas de nivel Superior, el 7 de septiembre de 1970 por Decreto Presidencial del Doctor José María Velasco Ibarra, y al cabo de 4 décadas de fructífera labor, se encuentra inmersa en celoso proceso de ajustes legales y reglamentarios, fruto del marco jurídico cambiante y motivador, que tiene como fin el establecimiento del Sumak Kawsay o del Buen Vivir (UCACUE - PEDI, 2014).

Por tal motivo, la Universidad Católica de Cuenca se rige por la Constitución de la República del Ecuador y la Ley Orgánica de Educación Superior, su Reglamento, las normativas emitidas por el CES[17] y el CEAACES[18], que son los cuerpos legales y reglamentarios que regulan al sistema de Educación Superior (UCACUE - PEDI, 2014).

Misión

Es Misión de esta Universidad Católica, inspirada en los principios cristianos, la producción y difusión del conocimiento científico, cultural, artístico y tecnológico, y

17 CES.- Consejo de Educación Superior.
18 CEAACES.- Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior

la formación de profesionales e investigadores con sólida preparación científica y técnica, cuyas capacidades, valores y compromiso con la búsqueda de solución a los problemas del país, los vuelvan competentes para liderar el cambio social y el servicio a los pueblos (UCACUE - PEDI, 2014).

Visión

La Visión de esta Universidad, tiene por objeto constituir una Casa de Estudios Superiores defensora de los valores éticos y cristianos, debidamente acreditada, con excelencia académica para liderar los proyectos de docencia, investigación y vinculación con la sociedad, rescatar las culturas ancestrales y utilizar modernas tecnologías, con lo que contribuye participativamente al desarrollo de la comunidad ecuatoriana, americana y universal (UCACUE - PEDI, 2014).

- **Entorno general de la Universidad Católica de Cuenca**

La Universidad Católica de Cuenca considera necesario contar con herramientas de gestión sólidas, coherentes con el medio y que permitan a la Institución un análisis profundo de los factores internos y externos, así como la capacidad de enfrentar los retos que conlleva el cambio; tener claro la situación actual, poder establecer estrategias y superar las debilidades para alcanzar un crecimiento sostenible (UCACUE - PEDI, 2014).

Para lograr estas metas, es necesario conocer los Objetivos Estratégicos Institucionales, relacionados con el incremento de los niveles académicos en docencia de grado y posgrado conforme a los estándares de calidad. Incrementar los niveles de investigación. Mantener las actividades de Vinculación con la sociedad. Incrementar la infraestructura, así como la eficiencia e integración interna en la gestión institucional; y, la búsqueda de la excelencia de los estudiantes de esta Casa de Estudios Superiores; por lo que se establece de manera coherente y ordenada los pasos y estrategias a seguir, contar con indicadores que den a la dirección, elementos de evaluación respecto del avance, desviaciones y cambios oportunos (UCACUE - PEDI, 2014).

- **Orgánico funcional**

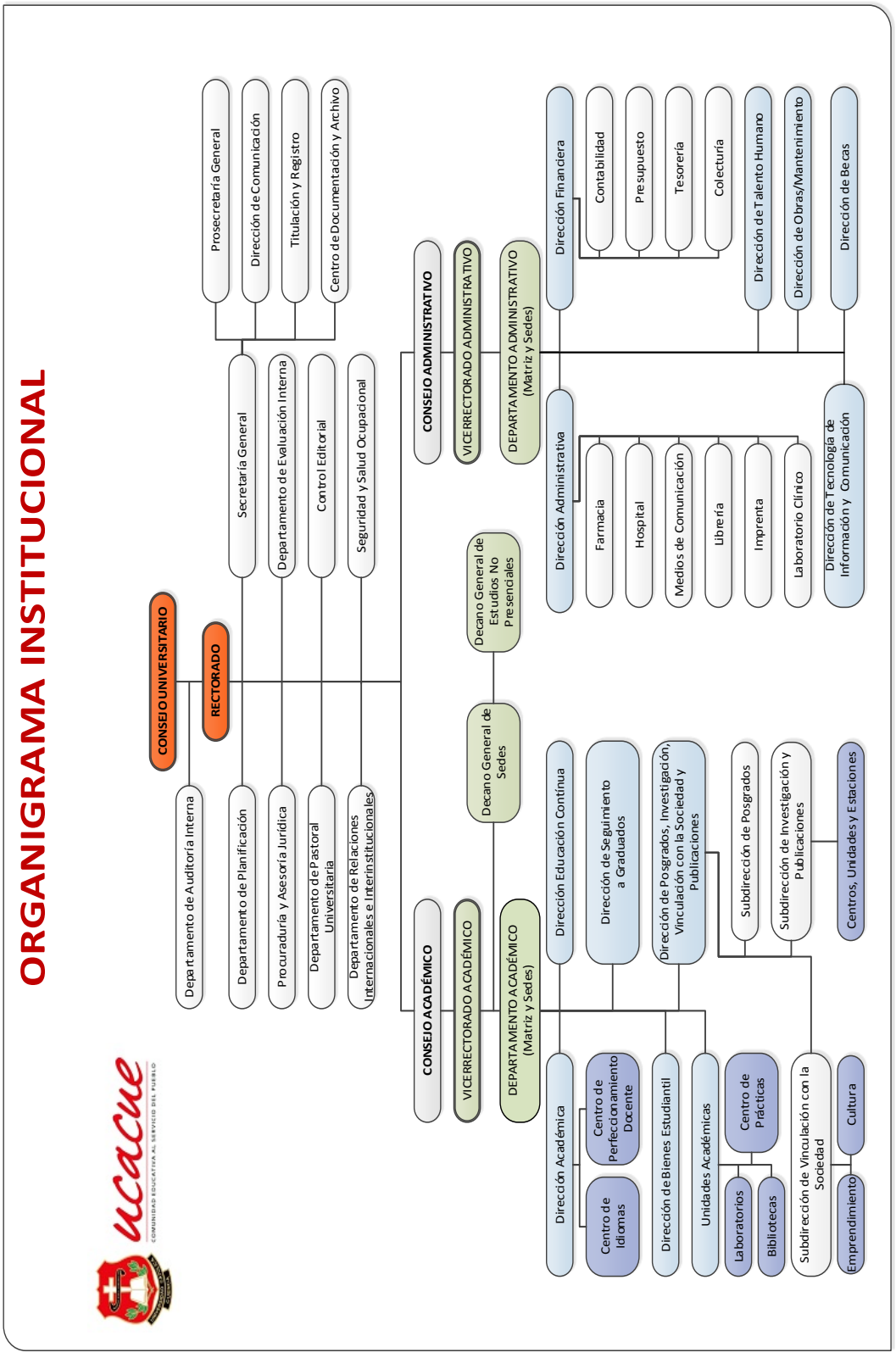


Figura 4. Organigrama Institucional de la UCACUE
Fuente: (UCACUE - PEDI, 2014)

Objetivos estratégicos en relación a TI

En la Tabla 1 y Tabla 2, se describen las estrategias en el área de TI que se implementan actualmente según se desprende del "Plan Estratégico Institucional 2011 - 2015" de la Universidad Católica de Cuenca.

Tabla 1.
Objetivo estratégico Institucional 4.

<table>
<tr><td colspan="6">Incrementar la Infraestructura, que propicie la eficiencia de integración de la comunidad universitaria en la gestión institucional.</td></tr>
<tr><th colspan="2">PROGRAMA</th><th colspan="2">PROYECTOS</th><th colspan="2">ESTRATEGIAS</th></tr>
<tr><td rowspan="8">4.2</td><td rowspan="8">Innovación e incremento de los recursos bibliográficos tecnológicos y laboratorios de la UCACUE</td><td>4.2.1</td><td>Adquisición de recursos bibliográficos físicos, digitales bibliotecas virtuales actualizados que fortalezcan las actividades académicas</td><td>4.2.1.2</td><td>Generar accesos remotos a las Bases de Datos digitales</td></tr>
<tr><td rowspan="7">4.2.3</td><td rowspan="7">Adquisición de recursos tecnológicos y laboratorios funcionales que fortalezcan las actividades académicas</td><td>4.2.3.2</td><td>Implementar infraestructura tecnológica de Data Center</td></tr>
<tr><td>4.2.3.3</td><td>Monitorear las conexiones de red existente</td></tr>
<tr><td>4.2.3.4</td><td>Implementar cobertura inalámbrica total</td></tr>
<tr><td>4.2.3.6</td><td>Elaborar e implementar planes de mantenimiento preventivo</td></tr>
<tr><td>4.2.3.8</td><td>Implementación de un Sistema de Mesa de Ayuda para soporte a las actividades académica-administrativa</td></tr>
<tr><td>4.2.3.10</td><td>Implementación de Factura Electrónica</td></tr>
</table>

Fuente: (UCACUE - PEDI, 2014)

Tabla 2.
Objetivo estratégico Institucional 5

Incrementar la eficiencia e integración interna en la gestión institucional, en la búsqueda de la excelencia de los estudiantes de la Universidad Católica de Cuenca					
PROGRAMA		**PROYECTOS**		**ESTRATEGIAS**	
5.1	Generación y mantenimiento de un sistema de gestión de calidad de la UCACUE que optimice la gestión del talento humano y su mejoramiento continuo en función de las necesidades institucionales	5.1.1	Implementación de un sistema de administración de procesos bajo la lógica de mejoramiento continuo	5.1.1.1	Diagnosticar la situación actual de los procesos institucionales
				5.1.1.2	Definir los procesos institucionales y por áreas
				5.1.1.4	Diseñar mecanismos de monitoreo y evaluación del sistema
5.4	Automatización de los procesos administrativos y académicos de la UCACUE	5.4.1	Implementación de un software que permita la automatización de los procesos administrativos y académicos	5.4.1.1	Adquirir un software que permita la automatización de los procesos administrativos y académicos
				5.4.1.2	Desarrollar e implementar el software para el proceso de titulación
				5.4.1.4	Capacitación para el uso del Sistema ERP
				5.4.1.5	Instalar el sistema ERP (Sistema Integrado de gestión SIG-UCC)

Fuente: (UCACUE - PEDI, 2014)

➢ Objetivo y alcance de la auditoría

Como resultado del análisis de la situación actual y del entorno general de la Universidad Católica de Cuenca se identifica el alcance y los objetivos de la auditoría, de tal forma que se determinan los límites y el entorno en el que se realizará la evaluación del control interno de la Seguridad de la Información:

- **Objetivo**: Evaluar el Control Interno de Seguridad de la Información en la Universidad Católica de Cuenca.
- **Alcance**: Identificar si existen controles que permitan validar y orientar si las acciones implementadas cumplen sus objetivos, para brindar Seguridad de la Información.

2.2.2 Estudio general de la Dirección de Tecnologías de la Información de la Universidad Católica de Cuenca.

El estudio general del área de TI de la Unidad de Sistemas de Información y Comunicación de la Universidad Católica de Cuenca, tiene por finalidad, describir la estructura orgánica interna, responsabilidad, coordinación, funciones de cada una de las unidades de la estructura interna; establecer perfiles del personal del cargo que ha sido asignado; descripción macro de sistemas de información implementados y en producción.

El estudio del área de TI es vital, como punto de partida de la revisión del entorno de seguridad existente e identificar la efectividad de los controles internos con el propósito de lograr que las tecnologías de información contribuyan considerablemente para que la Institución sea eficaz y eficiente, es necesario entonces que la información manejada sea utilizada en forma adecuada mediante el uso de controles de tipo preventivo y predictivo, una gestión de los recursos en forma ordenada, para que se pueda alcanzar las metas establecidas, la toma decisiones apropiadas y a tiempo; alineadas a la Ley Orgánica de Educación Superior (LOES).

- **Comprensión de la organización de TI, procesos de TI y sistemas**

La estructura departamental de la Universidad Católica de Cuenca está conformada por una matriz en la ciudad de Cuenca; dos sedes en las ciudades de: Azogues y Macas; dos extensiones: Cañar y San Pablo de La Troncal.

En la actualidad el departamento de Tecnología de la Información y Comunicación da el soporte a toda la estructura departamental de la Matriz incluida las Sedes y Extensiones, de una manera centralizada.

Estructura de la Dirección de Tecnología de Información y Comunicación.

La Unidad de Sistemas y Comunicaciones no cuenta con una estructura funcional, sin embargo existe personal que realiza diferentes actividades dentro del área, a nivel general en la Universidad Católica de Cuenca existe 38 funcionarios que forman parte de esta Unidad (ver Tabla 3).

Tabla 3.
Número de personal de TI de la UCACUE.

SEDE	CIUDAD	N. DE EM PLEADOS.
Matriz	Cuenca	27
Sede	Azogues	7
Extensión	Cañar	1
Extensión	La Troncal	2
Sede	Macas	1
Total		38

Funciones que desarrolla la Dirección de Tecnología de Información y Comunicación:

- Implementar el sistema ERP, se tiene documentado el manual de procesos administrativos y académicos para la implementación del ERP Académico.
- Mantener el sistema SIGEAC, análisis de la BD[19] y los módulos iniciales sobre gestión académica; desarrollo de aplicaciones a medida; mantener y administrar las bases de datos.
- Administrar el funcionamiento del sistema integral de conectividad de la Universidad.
- Asesorar, evaluar y brindar el soporte técnico de software y hardware a las dependencias de la Universidad.

Esquema de la Dirección de Tecnología de Información y Comunicación.

De acuerdo a las funciones se identificaron dentro de esta Dirección las áreas de: Desarrollo de Sistemas; Comunicaciones y Redes. En la actualidad no existe un orgánico funcional del área de TI.

[19] BD.- Base de datos.

Figura 5. Esquema de TIC de acuerdo a las actividades que desarrolla.
Fuente: Autores (Adaptado de UCACUE - PEDI, 2014)

Descripción de sistemas de información implementados

El sistema SIGEAC, es el que actualmente brinda el soporte tecnológico transaccional, se encuentra en la fase de migración al sistema ERP Académico adquirido por la Universidad como parte del cumplimiento de los Objetivos Estratégicos en relación a TI registrados en la Tabla 1 y Tabla 2, para el área administrativa y curricular.

Desde el departamento de TI ubicado en el Edifico Administrativo se ofrece el soporte para las Unidades Académicas; en los siguientes servicios implementados que están en producción:

- Sistema SIGEAC
- Sistema ERP Académico (en fase de implementación)
- Sistema de marcación de personal
- Sistema de comunicación visual institucional
- Aplicaciones web
- Aulas Virtuales
- D'Space
- Antivirus

Descripción del sistema de comunicación, topología lógica de la red.

La Administración de la Universidad Católica de Cuenca está formada por un edificio y centraliza sus comunicaciones a través del responsable de Comunicación y Redes. La LAN[20] y la red Wireless dan servicio a los distintos grupos de trabajo de personal administrativo y acceso desde las Unidades Académicas que se hallan ubicadas en diferentes lugares del centro histórico de la ciudad de Cuenca y sus alrededores. La división lógica se realiza mediante la implementación de VLAN's[21].

En el área de TI se encuentra el Centro de Datos, en el que se concentra una serie de servidores para automatizar todas las funciones administrativas, algunas funciones curriculares, el acceso a Internet y al sistema SIGEAC. Este sistema de información es accedido desde cualquier sede o extensión, a través de, conexiones seguras de Internet con el Servidor VPN[22], tal como se aprecia en el Diagrama de red.

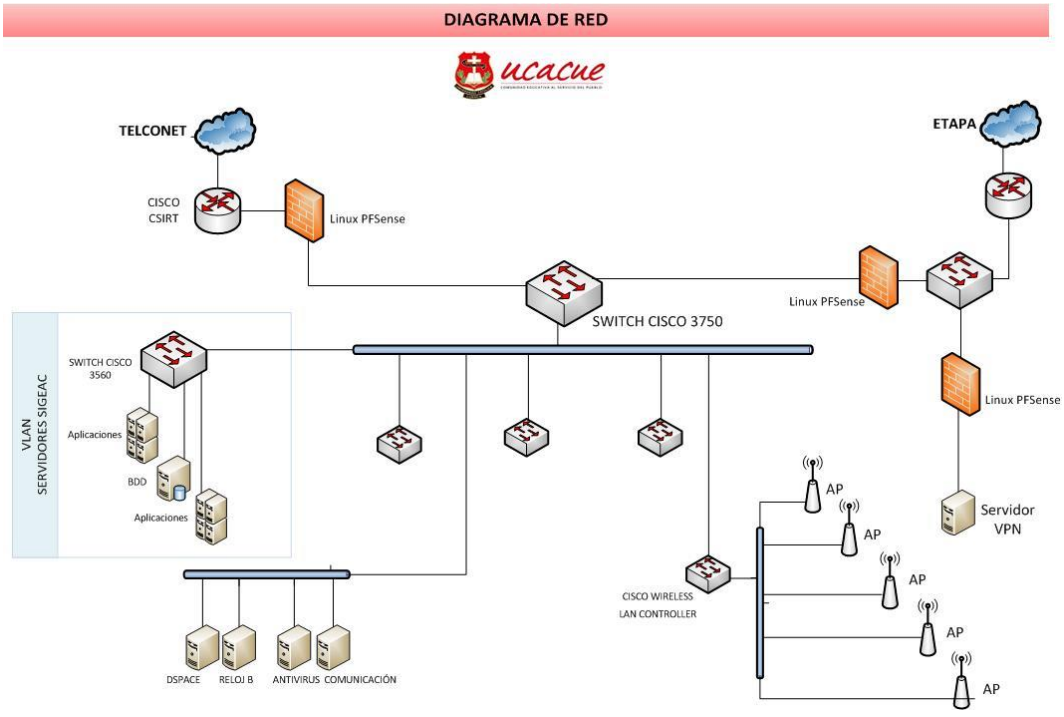


Figura 6. Diagrama de red de la UCACUE.

[20] LAN.- Red de área local.
[21] VLAN's.- Redes de área local virtuales.
[22] VPN.- Red privada virtual.

Descripción de la red de datos

El diseño actual de la red cableada está basado en un esquema de organización que cumple con las especificaciones mínimas de cableado estructurado según las normas TIA/EIA-568-B. Entre los puntos considerados durante el diseño de red se destacan:

- Una topología en estrella extendida, conformada por el MDF[23] y 3 IDF[24] adicionales, los que son requeridos por las distancias máximas que establecen los estándares para el cableado horizontal.
- El Tipo de cable para las conexiones horizontales y verticales es UTP[25] Categoría 6a.
- Las velocidades de transmisión para las conexiones horizontales es de 1000Mbps, y utiliza una interfaz de 1000BASE-TX.
- Para las conexiones verticales, las velocidades de transmisión es de 1Gbps, y utiliza una interfaz GBIT Ethernet.
- El MDF se halla ubicado en el cuarto piso del edificio, en el departamento de Comunicación y Redes. Se encuentra instalados armarios en los que están colocados los equipos activos y pasivos de la red. Estos armarios están directamente conectados al MDF o IDF más cercano mediante tendidos de cable UTP Categoría 6, cada uno de ellos para el área administrativa, SIGEAC y servicios de red.
- Las comunicaciones con las demás Unidades Académicas se realizan a través del ISP[26], el mismo que implementa con su estructura de red y configuración Túneles en los enlaces de última milla de cada locación, suministrada por los ISPs: ETAPA[27] y CEDIA[28].

Seguridad perimetral y de red

La seguridad perimetral está conformada por tres Firewalls PfSense Linux, esta es una plataforma libre de código abierto, robusta y segura que puede usarse como

[23] MDF.- Servicio de distribución principal para comunicación de redes de datos.
[24] IDF.- Servicio de distribución intermedia para comunicación de redes de datos.
[25] UTP.- Cable de par trenzado.
[26] ISP.- Proveedor de servicios de internet.
[27] ETAPA.- Empresa de Telecomunicaciones, Agua Potable, Alcantarillado y saneamiento de Cuenca
[28] CEDIA.- Red nacional de educación e investigación del Ecuador.

base para soluciones complejas de seguridad perimetral y seguridad de red. Para dar respuesta a las necesidades de seguridad de red y control de los canales de comunicación, se han establecido las siguientes funciones:

- Existen dos enlaces a Internet que pueden funcionar como respaldo de conectividad, además en el enlace a través de CEDIA se cuenta con el servicio de CSIRT[29], para la prevención de ataques desde el exterior mediante el envío de mensajes de correo de alerta en el que comunica que actividad se efectúa en un determinado puerto, los ajustes que se realizan son replicados al enlace a Internet de ETAPA, con esto se logra tener una defensa solida perimetral en la red de datos.
- FIREWALL sobre IPTables: políticas de acceso según direcciones IP, puertos origen, puertos destino, NAT[30] y PAT[31].
- VPN: Net-to-Net o Host-to-Net desde un cliente Windows, Mac o Linux, utiliza una solución libre de conectividad OpenVPN que permite la validación de usuario contra un directorio LDAP[32] y Active Directory mediante un servidor Radius.
- QoS: calidad de servicio para la priorización de tipos de tráfico en la red de la área administrativa.
- Proxy y control de contenido: acelerador de navegación web, en modalidad declarada o proxy transparente, activado el filtro de contenido para permitir acceso condicionado a la navegación de acuerdo a políticas establecidas por el Vicerrectorado Administrativo.

Seguridad red wireless.

La seguridad Wireless abarca dos elementos: el acceso a la red y la protección de los datos (autenticación y encriptación respectivamente).

En lo referente al acceso está controlado por el servicio Radius implementado en un servidor tipo Hotspot para controlar el ingreso a la red por tiempo limitado y

[29] CSIRT.- Equipo de Respuesta ante Incidencias de Seguridad)
[30] NAT.- Traducción de direcciones de red.
[31] PAT.- Traducción de direcciones de puerto.
[32] LDAP.- Protocolo ligero de acceso a directorios.

realizar un control del ancho de banda por cada conexión desde la red de: Administración e Invitados.

Mecanismos de seguridad implementados:

- SSID (Identificador de Servicio): Los clientes deben tener configurado el SSID correcto para acceder a la red inalámbrica.
- WPA2 (Wi-Fi Protected Access)Contiene los beneficios de encriptación del protocolo de integridad de llave temporal. Debido a que la tecnología Wireless se basa en transmisión sobre ondas de radio, con cobertura en áreas que pueden ser ambientes públicos o privados, se ha tomado en cuenta importantes consideraciones acerca de la seguridad en la red; las actividades están dirigidas por la especificación de seguridad WPA2 (Acceso de Protección Wi-Fi), esta especificación proporciona una mayor encriptación de datos para corregir las vulnerabilidades de seguridad WEP, además de añadir autenticación de usuarios, por lo que se encuentra implementado en los puntos de acceso (APs).

2.2.3 Determinación de recursos

- **Recursos humanos, tecnológicos, materiales y de consumo.**

Cumplidas las actividades correspondientes e identificado el alcance y los objetivos de la auditoría interna se obtiene un conocimiento general mediante el estudio inicial del entorno a auditar, entonces se procede a determinar los recursos necesarios para la ejecución de la auditoría, estos recursos abarcan tanto: humanos, tecnológicos, materiales y de consumo.

Para identificar el recurso humano necesario, se ha de considerar todo el personal que desarrollará la auditoría; en el caso de los recursos tecnológicos se deberá analizar en función del alcance de la auditoría las herramientas tanto de software como de hardware necesarias para la recolección de la evidencia de ser el caso y la elaboración de la documentación necesaria; los recursos materiales y de consumo han de ser considerados en función de la auditoría y el entorno a auditar; pueden

representar un rubro alto que se debe considerar. En la tabla 4 se observa el listado de recursos necesarios para realizar la auditoría del presente trabajo de titulación.

Tabla 4.
Recursos para el desarrollo de la auditoría.

TIPO DE RECURSO	DETALLE
Humano	Equipo Auditor: Auditor: Ing. Carlos Encalada L. Auditor: Ing. Aida Tenecela P. Director de Auditoría Interna: Eco. José Guzmán A Tutor del proyecto: Ing. Fernando Garrido
Tecnológico	Equipos de cómputo para la elaboración de documentación
Materiales y de consumo	Llamadas Telefónicas Movilización Alimentación Encuadernación Fotocopias e impresiones

2.2.4 Definición del programa y alcance de la auditoria.

- **Análisis y evaluación de riesgos de TI**

Se recomienda fuertemente que para el inicio de la Auditoria se realice previamente la identificación de riesgos y vulnerabilidades de seguridad mediante una evaluación de riesgos, esto permitirá a la alta dirección de la Universidad tener una idea clara y precisa de la situación actual en el tema de la Seguridad de la Información.

La Universidad Católica de Cuenca si cuenta con una evaluación de riesgos, pero en el caso de no existir, se deberá obligatoriamente realizar una evaluación de riesgos básica, que permitan identificar áreas críticas, en donde se analizarán los respectivos controles.

- **Plan de auditoría**

El encargado de elaborar la planificación de la auditoría es el auditor líder, en cuyas manos está coordinar todas las actividades referentes a la preparación y desarrollo de la auditoría.

En los criterios globales de un programa de auditoría debe basarse en objetivos, alcance y criterios documentados, los objetivos de la auditoría son los que definen qué se pretende alcanzar con su realización.

Tabla 5.
Plan de Auditoría.

PLAN DE AUDITORÍA	
INSTITUCIÓN:	Universidad Católica de Cuenca
DIRECCIÓN:	Av. de Las Américas s/n y Humbolt Edificio Administrativo
ALCANCE:	Identificar si existen controles que permitan validar y orientar si las acciones implementadas cumplen sus objetivos, para brindar Seguridad de la Información.
EQUIPO AUDITOR:	Auditor líder: Ing. Carlos Encalada L. Auditor: Ing. Aida Tenecela P. Director de Auditoría Interna: Eco. José Guzmán A
FECHA AUDITORÍA:	03-Febrero-2015
LUGAR:	Instalaciones Administrativas de la Universidad Católica de
DOCUMENTACIÓN DE REFERENCIA:	COBIT 5 Para la Seguridad de la Información ISO 27002 Guía para la Seguridad de la Información Plan Estratégico Institucional de la Universidad Católica de Cuenca.
OBJETIVO:	Evaluar el Control Interno de Seguridad de la Información en la Universidad Católica de Cuenca.
ACTIVIDADES:	1. Verificar si existe un sistema de Seguridad de la Información implementado. 2. Verificar si existe Estructuras Organizativas de Seguridad de la Información de acuerdo a las necesidades de la UCACUE. 3. Verificar si el personal de TI y el personal de Seguridad de la Información posee las habilidades y competencias requeridas. 4. Verificar si la información está debidamente catalogada. 5. Verificar si los servicios de Seguridad de la Información se gestionan adecuadamente. 6. Verificar la existencia de controles ante software malicioso 7. Verificar la aplicación de prácticas relacionadas con la seguridad de la red. 8. Verificar los controles para la seguridad de los usuarios finales a nivel de Servidores. 9. Verificar la existencia de controles para la identidad de usuarios y accesos lógicos. 10. Verificar los controles de acceso físico a los activos de TI. 11. Verificar los controles de administración de documentos sensibles. 12. Verificar que se gestionen los eventos de seguridad de la información críticos. 13. Verificar que se realiza el control interno de Seguridad de la Información.

La Tabla 5 representa la planificación en la que se presentan las principales actividades a realizar en esta guía de Auditoría:

- Analizar y diagnosticar la actual gestión de Seguridad de la Información en la red de datos de la Universidad Católica de Cuenca.
- Plantear las mejoras para la gestión de la seguridad de la red de datos.
- Proponer nuevos procesos y actividades que ayudaran a identificar los controles que se requieren para garantizar la Seguridad de la Información

Para dar cumplimiento al programa de auditoría, los integrantes del equipo auditor deben proceder de la siguiente manera:

- Definir el alcance de la auditoría: Se describe la extensión y los límites de la auditoría, tales como ubicación, unidades de la organización, actividades y procesos a ser auditados, así como el periodo de tiempo cubierto por la auditoría.
- Solicitar la documentación necesaria. Antes de desarrollar las actividades de la auditoría in-situ, la documentación del auditado debe ser revisada para determinar la conformidad del sistema con los criterios de auditoría.
- Preparar la lista de verificación. Los miembros del equipo auditor deben revisar la información pertinente de las tareas asignadas y preparar los documentos de trabajo que sean necesarios como referencia y registro del desarrollo de la auditoría.
- Elaboración del plan de auditoría. El líder del equipo auditor debe preparar un plan de auditoría que proporcione la base para cumplir el objetivo acordado previamente.
- Comunicar el plan de auditoría. El líder del equipo auditor debe comunicar al auditado el correspondiente plan de auditoria, con la antelación suficiente, para que, tanto el auditado como su equipo de trabajo estén a entera disposición (Ver Tabla 5).

- **Cronograma de actividades para la auditoría**

Tabla 6.
Cronograma de actividades para la auditoría

N°	Actividad	Duración	Comienzo	Fin
1	Cronograma de Trabajo	118 días	lun 24/11/14	jue 14/05/15
1.1	Definición de alcance y objetivos de la auditoria	3 días	lun 24/11/14	mie 26/11/14
1.1.1	Definición del alcance	1 día	lun 24/11/14	lun 24/11/14
1.1.2	Definición de los objetivos	1 día	lun 24/11/14	lun 24/11/14
1.1.3	Aprobación de los interesados	2 días	mar 25/11/14	mie 26/11/14
1.2	Estudio preliminar del entorno a auditar	7 días	lun 01/12/14	mar 09/12/14
1.2.1	Preparación de la visita preliminar	4 días	mar 02/12/14	vie 05/12/14
1.2.2	Visita preliminar	3 días	lun 08/12/14	mie 10/12/14
1.3	Determinación de recursos	1 día	vie 12/12/14	vie 12/12/14
1.3.1	Determinación de recursos humanos	1 día	vie 12/12/14	vie 12/12/14
1.3.2	Determinación de recursos tecnológicos	1 día	vie 12/12/14	vie 12/12/14
1.3.3	Determinación de recursos materiales y de consumo	1 día	vie 12/12/14	vie 12/12/14
1.4	Elaboración del plan de trabajo	32 días	lun 05/01/15	mar 17/02/15
1.4.1	Determinación de los aspectos a ser evaluados	1 día	lun 05/01/15	lun 05/01/15
1.4.2	Elaboración del documento formal del plan de trabajo	8 días	mar 06/01/15	jue 15/01/15
1.4.3	Elaboración de los programas de actividades	3 días	vie 16/01/15	mar 20/01/15
1.4.4	Determinación de herramientas	2 días	mie 21/01/15	jue 22/01/15
1.4.5	Elaboración de los documentos necesarios	5 días	vie 23/01/15	jue 29/01/15
1.5	Ejecución de las actividades de auditoría	20 días	lun 02/02/15	vie 27/02/15
1.5.1	Aplicación de los instrumentos y herramientas	10 días	lun 02/02/15	vie 13/02/15
1.5.2	Identificación y elaboración de los documentos de desviaciones	5 días	lun 16/02/15	vie 20/02/15
1.5.3	Elaboración del dictamen preliminar y presentación para discusión	5 días	lun 23/02/15	vie 27/02/15
1.6	Elaboración del informe final de auditoría.	9 días	lun 02/03/15	jue 12/03/15
1.6.1	Elaboración del informe final	8 días	lun 02/03/15	mie 11/03/15
1.6.2	Presentación del informe de auditoría	1 día	jue 12/03/15	jue 12/03/15

2.2.5 Evaluación de controles y seguridades (COBIT – UCACUE)

- **Identificación de los dominios, procesos y prácticas COBIT aplicables**

Para la evaluación del control interno de la Seguridad de la Información en la Universidad Católica de Cuenca basada en COBIT 5, es necesario identificar claramente los dominios, procesos y prácticas de gestión aplicables. Para lo que se debe realizar un mapeo minucioso entre los objetivos de la Institución y los objetivos del área auditada, posteriormente se procederá a relacionar los objetivos del área con los procesos de COBIT 5 principales, es decir, que aportan significativamente a la

consecución de los objetivos y requieren ser evaluados. Para llevar a cabo esta actividad el marco de referencia COBIT 5 proporciona tanto la tabla de mapeo entre objetivos institucionales y los objetivos de TI, así como, los objetivos de TI con los procesos, que constituyen una guía pero que deben ser analizadas y utilizadas de acuerdo a la realidad de cada institución.

En el presente trabajo de titulación 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 lo que se ha utilizado 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 7 se puede apreciar los procesos identificados para evaluar la Seguridad de la Información en la UCACUE.

Identificados y seleccionados los procesos tanto principales como secundarios (ver tabla 7), 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 8 se tiene las prácticas identificadas para evaluar la Seguridad de la Información en la UCACUE, cada una de las cuales pertenece a un proceso seleccionado y que a su vez corresponde a un dominio.

Tabla 7.
Mapeo de los procesos de TI con el objetivo correspondiente a Seguridad de la Información

		Meta relacionada con las TI																
		Alineamiento de TI y la estrategia de negocio.	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con	Riesgos de negocio relacionados con las TI gestionados.	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI.	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones.	Optimización de activos, recursos y capacidades de las TI.	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones.	Cumplimiento de las políticas internas por parte de las TI.	Personal del negocio y de las TI competente y motivado.	Conocimiento, experiencia e iniciativas para la innovación de negocio.
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
PROCESOS DE COBIT		**Financiera**						**Cliente**		**Interna**							**Aprendizaje**	
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							

Fuente: (ISACA-COBIT 5, 2012)

Tabla 8.
Dominios, Procesos y Prácticas de Seguridad de Información identificados

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

Fuente: Adaptación de (ISACA - COBIT 5 para Seguridad de la Información, 2012)

- **Diseño de las pruebas de auditoría**

Al utilizar COBIT 5 como marco de referencia para la evaluación del control interno de la Seguridad de la Información de la Universidad Católica de Cuenca, el diseño de las pruebas de auditoría consiste en la elaboración de checklist que serán aplicados al personal identificado como responsable de los procesos a evaluar.

Para cada uno de los procesos identificados y listados en la Tabla 8, se debe elaborar los checklist necesarios que permitan evaluar las prácticas de gestión correspondientes. De esta manera se han determinado 15 checklist 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 8, esto permitió generar el formato AUD-FOR-TIC-001 (ver Tabla 9), en base al que se realizaron los checklist para evaluar el control interno (ver tabla 10 hasta la tabla 24).

Tabla 9.
Formato AUD-FOR-TIC-001 – Evaluación de controles

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

- **Checklist desarrollados para la evaluación del control sobre la Seguridad de la Información.**

Tabla 10.
Checklist para evaluación de controles de estructuras organizativas.

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-01				
EVALUACIÓN DE CONTROLES DE ESTRUCTURAS ORGANIZATIVAS				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO01 Gestionar el Marco de Gestión de TI			
PRÁCTICA:	APO01.01 Definir la estructura organizativa			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe una estructura orgánico funcional de TI?	☐	☐	☐	
¿La estructura orgánica funcional de la UCACUE incluye una estructura específica para seguridad de la información?	☐	☐	☐	
¿Existe un ISSC (Comité de dirección de la seguridad de la información) o su equivalente?	☐	☐	☐	

Tabla 11.
Checklist para evaluación de controles acerca de roles y responsabilidades.

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-02				
EVALUACIÓN DE CONTROLES DE ESTRUCTURAS ORGANIZATIVAS				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO01 Gestionar el Marco de Gestión de TI			
PRÁCTICA:	APO01.02 Establecer roles y responsabilidades.			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Las funciones y responsabilidades del personal han sido, correctamente establecidas, formalizadas, documentadas y aprobadas con respecto a seguridad de la información?	☐	☐	☐	
¿Se entrega formalmente a los funcionarios sus funciones y responsabilidades sobre seguridad de la información?	☐	☐	☐	
¿Existe un manual de cargos y funciones acorde a la estructura orgánico funcional que tome en cuenta la seguridad de la información?	☐	☐	☐	
¿Existe definidos los puestos de director de la seguridad de la Información (CISO) y de gerente de la seguridad de la información?	☐	☐	☐	

Tabla 12.
Checklist para evaluación de controles de políticas de seguridad

UNIVERSIDAD CATÓLICA DE CUENCA

AUD-FOR-TIC-001-03

EVALUACIÓN DE CONTROLES DE POLÍTICAS DE SEGURIDAD				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO01 Gestionar el Marco de Gestión de TI			
PRÁCTICA:	APO01.03 Mantener los catalizadores del sistema de gestión			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
Principios, políticas y marcos				
¿Existe el marco de políticas establecido sobre la seguridad de la información?	☐	☐	☐	
¿Están definidos los principios seguridad de la información que den soporte a la institución y promuevan un comportamiento responsable en seguridad de la información?	☐	☐	☐	
¿Existe una política de seguridad de la información?	☐	☐	☐	
¿Existe una política de control de accesos?	☐	☐	☐	
¿Existe una política de seguridad de la información del personal?	☐	☐	☐	
¿Existe una política de gestión de incidentes de seguridad?	☐	☐	☐	
¿Existe una política de gestión de riesgos, sobre la seguridad de la información?	☐	☐	☐	
¿Se comunica las políticas sobre seguridad de la información a las partes interesadas?	☐	☐	☐	
¿Las políticas sobre seguridad de la información se actualizan periódicamente de acuerdo a los requerimientos de la institución?	☐	☐	☐	
¿Existe procedimientos de Seguridad de Información?	☐	☐	☐	

Continúa →

Cultura, Ética y comportamiento				
¿Las personas respetan la importancia de las políticas y principios de la seguridad de la información?	☐	☐	☐	
¿Las personas poseen un nivel detallado y suficiente de orientación en seguridad de la información y se los anima a participar y cuestionar la situación actual de seguridad de la información?	☐	☐	☐	
¿Todo el personal es responsable de que se proteja la información de la empresa?	☐	☐	☐	
¿Las Partes Interesadas están informadas de cómo identificar y responder a las amenazas de seguridad de la información en el contexto de la Universidad?	☐	☐	☐	
¿La Dirección respalda y anticipa las innovaciones en seguridad de la información de manera proactiva?	☐	☐	☐	
¿La Dirección comunica a toda la Universidad las innovaciones en seguridad de la información?	☐	☐	☐	
¿La UCACUE es receptiva para tener en cuenta y manejar nuevos retos en materia de seguridad de la información?	☐	☐	☐	
¿La alta dirección reconoce el valor para la UCACUE de la seguridad de la información?	☐	☐	☐	
¿Se influye en el comportamiento del personal mediante comunicaciones, disposiciones, reglas y normas sobre la seguridad de la información?	☐	☐	☐	

Tabla 13.

Checklist para evaluación de controles acerca de la gestión del personal de seguridad de la información

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-001-04				
EVALUACIÓN DE CONTROLES ACERCA DE LA GESTIÓN DEL PERSONAL DE SEGURIDAD DE LA INFORMACIÓN				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO07 Gestionar los Recursos Humanos			
PRÁCTICA:	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			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe personal con funciones específicas correspondientes a seguridad de la información?	☐	☐	☐	
¿Se ha definido las habilidades y competencias para el personal de seguridad de la información?	☐	☐	☐	
¿El personal tiene habilidades y competencias en Gobierno de la Seguridad de la Información?	☐	☐	☐	
¿El personal tiene habilidades y competencias en Formulación de estrategia de seguridad de información?	☐	☐	☐	
¿El personal tiene habilidades y competencias en Gestión de riesgos de la información?	☐	☐	☐	
¿El personal tiene habilidades y competencias en desarrollo de la arquitectura de seguridad de la información?	☐	☐	☐	
¿El personal tiene habilidades y competencias en Operaciones de Seguridad de la Información?	☐	☐	☐	
¿El personal tiene habilidades y competencias en Evaluación, pruebas y cumplimiento de la información?	☐	☐	☐	
¿Existe programas de capacitación y desarrollo profesional en seguridad de información?	☐	☐	☐	
¿Existe programas de capacitación, certificación y desarrollo profesional en seguridad de información?	☐	☐	☐	

Tabla 14.

Checklist para evaluación de controles de los servicios, infraestructura y aplicaciones

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-001-05				
EVALUACIÓN DE CONTROLES DE LOS SERVICIOS, INFRAESTRUCTURA Y APLICACIONES				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO09 Gestionar los acuerdos de servicio			
PRÁCTICA:	APO09.01 Identificar servicios TI APO09.02 Catalogar los servicios de TI			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se han identificado los servicios de TI relacionados con seguridad de información?	☐	☐	☐	
¿Se ha definido el portafolio de servicios de seguridad de la información?	☐	☐	☐	
¿Se cuenta con un catálogo de servicios de seguridad de la información?	☐	☐	☐	

Tabla 15.

Checklist para evaluación de controles para la gestión de la seguridad de la información

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-001-06				
EVALUACIÓN DE CONTROLES PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO13 Gestionar la seguridad			
PRÁCTICA:	APO13.01 Establecer un SGSI			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe un Sistema de Gestión de Seguridad de la Información que esté de acuerdo con las políticas de la UCACUE?	☐	☐	☐	
¿Existe una política de implementación del Sistema de Gestión de Seguridad de la Información?	☐	☐	☐	
¿Están definidos y comunicados los roles y responsabilidades de la gestión de la seguridad de la información?	☐	☐	☐	

Tabla 16.

Checklist para evaluación de controles de información relacionada con seguridad de la información

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-001-07	

EVALUACIÓN DE CONTROLES DE INFORMACIÓN RELACIONADA CON SEGURIDAD DE LA INFORMACIÓN				
DOMINIO:	Construir, Adquirir e Implementar (BAI)			
PROCESO:	BAI08 Gestionar el conocimiento			
PRÁCTICA:	BAI08.02 Identificar y clasificar las fuentes de información			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se ha definido los tipos de información relacionados con la seguridad de la información?	☐	☐	☐	
¿Se ha identificado los grupos de interés o partes interesadas de los diferentes tipos de información?	☐	☐	☐	
¿Los diferentes tipos de información están debidamente almacenados y son de acceso únicamente para las partes interesadas?	☐	☐	☐	
¿Están definidos los requisitos de configuración de la seguridad?	☐	☐	☐	

Tabla 17.
Checklist para evaluación de controles contra software malicioso

UNIVERSIDAD CATÓLICA DE CUENCA

AUD-FOR-TIC-001-08

EVALUACIÓN DE CONTROLES CONTRA SOFTWARE MALICIOSO				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.01 Proteger contra software malicioso			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe una política de prevención de software malicioso?	☐	☐	☐	
¿Existe una cultura de concienciación sobre: software malicioso, cómo proceder frente a los mismos y responsabilidades de prevención?	☐	☐	☐	
¿Se ha instalado y activado herramientas de protección frente a software malicioso?	☐	☐	☐	
¿Los ficheros de definición de software malicioso se actualizan: periódicamente, automática o semiautomáticamente?	☐	☐	☐	
¿Se distribuye el software de protección de forma centralizada?	☐	☐	☐	
¿Se utiliza una configuración centralizada del software de protección?	☐	☐	☐	
¿Se realiza gestión de cambios en la configuración del software de protección?	☐	☐	☐	
¿Se revisa y evalúa regularmente la información sobre nuevas posibles amenazas?	☐	☐	☐	
¿Se realiza filtrado del tráfico entrante para protegerse frente a información no solicitada?	☐	☐	☐	
¿Se realiza capacitación periódica sobre software malicioso?	☐	☐	☐	
¿Se realiza capacitación periódica sobre el uso de correo electrónico, internet e instalación de software no autorizado?	☐	☐	☐	
¿Existe un listado de software autorizado por la institución?	☐	☐	☐	
¿Se prohíbe el uso de software no autorizado por la institución?	☐	☐	☐	
¿Se establece procedimientos para evitar obtención o descarga de archivos y software de procedencia dudosa?	☐	☐	☐	
¿Los sistemas operativos y sistemas de procesamiento de información están actualizados con las últimas versiones de seguridad disponibles?	☐	☐	☐	

Tabla 17.
Checklist para evaluación de controles contra software malicioso

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-08				
EVALUACIÓN DE CONTROLES CONTRA SOFTWARE MALICIOSO				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.01 Proteger contra software malicioso			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se revisa periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la institución?	☐	☐	☐	
¿Se verifica antes de su uso, la presencia de virus en archivos de medios electrónicos?	☐	☐	☐	
¿Existen procedimientos para verificar toda la información relativa a software malicioso?	☐	☐	☐	
¿Se emiten boletines informativos de alerta con información precisa acerca de software malicioso?	☐	☐	☐	
¿Se ha contratado con el proveedor de Internet o del canal de datos los servicios de filtrado de: virus, spam y programas maliciosos (malware), en el perímetro externo?	☐	☐	☐	

Tabla 18.

Checklist para evaluación de controles de seguridad de la red

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-09				
EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA RED				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.02 Gestionar la seguridad de la red y las conexiones			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe una política de seguridad en la conectividad basada en el análisis de riesgos y los requerimientos del negocio?	☐	☐	☐	
¿El acceso a la información y a la red está restringido sólo a dispositivos autorizados?	☐	☐	☐	
¿Los dispositivos que tienen acceso a la red están configurados a fin de que soliciten contraseña de acceso a la red?	☐	☐	☐	
¿Se ha implementado mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones?	☐	☐	☐	
¿Existen reglas apropiadas para controlar el tráfico entrante y saliente a nivel de firewall?	☐	☐	☐	
¿Se aplica los protocolos de seguridad aprobados a las conexiones de red?	☐	☐	☐	
¿Se configura los equipamientos de red de forma segura?	☐	☐	☐	
¿Se establece mecanismos de confianza para dar soporte a la transmisión y recepción segura de información?	☐	☐	☐	
¿Se realiza pruebas de ajustes periódicas para determinar la adecuación de la protección de la red?	☐	☐	☐	
¿Se establecen procedimientos y responsabilidades para la gestión de equipos remotos como el caso de re-direccionamiento de puertos y accesos por VPNs, se incluye el área de operaciones y el área de usuarios finales?	☐	☐	☐	
¿Se dispone de un esquema de red de los enlaces de datos, Internet y redes locales, así como la documentación respectiva?	☐	☐	☐	
¿Se incorpora tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red?	☐	☐	☐	
¿Se definen procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red cuando sea necesario?	☐	☐	☐	

Tabla 19.

Checklist para evaluación de controles de seguridad de los usuarios

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-001-10				
EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LOS USUARIOS				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.03 Gestionar la seguridad de los puestos de usuarios finales			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe una política de seguridad para dispositivos de usuarios finales?	☐	☐	☐	
¿Se configura los sistemas operativos de forma segura?	☐	☐	☐	
¿Se implementa mecanismos de bloqueo de los dispositivos no autorizados para acceso a la red?	☐	☐	☐	
¿Se utilizan mecanismos para cifrado de la información almacenada de acuerdo a su clasificación y a su criticidad?	☐	☐	☐	
¿Se gestiona el acceso y control remoto entre las estaciones de los usuarios?	☐	☐	☐	
¿Se gestiona la configuración de la red de forma segura?	☐	☐	☐	
¿Se implementa filtrado del tráfico de la red en dispositivos de usuario finales?	☐	☐	☐	
¿Se provee de protección física a los dispositivos de usuario finales?	☐	☐	☐	
¿Se identifica los medios de almacenamiento de información que requieran eliminación segura?	☐	☐	☐	
¿Se desecha (donación/desecho) los dispositivos de usuario finales de forma segura a fin de que la información sea eliminada completamente?	☐	☐	☐	
¿Se almacena de forma segura los medios que contienen información sensible?	☐	☐	☐	
¿Se registra la eliminación de los medios de almacenamiento para mantener pruebas de auditoría?	☐	☐	☐	
¿Se ha establecido un procedimiento para la gestión de todos los medios removibles?	☐	☐	☐	
¿Se ha establecido permisos para la conexión de los medios removibles y se registra la conexión y retiro, para pruebas de auditoría?	☐	☐	☐	
¿Se almacena los medios removibles en un ambiente seguro, según las especificaciones de los fabricantes?	☐	☐	☐	

Tabla 20.
Checklist para evaluación de controles de accesos lógicos

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-001-11				
EVALUACIÓN DE CONTROLES DE ACCESOS LÓGICOS				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.04 Gestionar la identidad del usuario y el acceso lógico			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se establecen permisos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio?	☐	☐	☐	
¿Se alinea los permisos de acceso a los roles y responsabilidades definidos, basándose en los principios de menos privilegio, necesidad de tener y necesidad de conocer?	☐	☐	☐	
¿Se autentican todos los accesos a los activos de información basándose en su clasificación de seguridad?	☐	☐	☐	
¿Se administra todos los cambios de permisos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno mediante un proceso formal de autorización?	☐	☐	☐	
¿Se verifica que los controles de autenticación han sido administrados adecuadamente?	☐	☐	☐	
¿Existe segregación y gestión de cuentas de usuarios privilegiadas?	☐	☐	☐	
¿Se realiza regularmente revisiones de la gestión de todas las cuentas y privilegios relacionados?	☐	☐	☐	
¿Se mantiene un registro de auditoría de los accesos a la información clasificada como altamente sensible?	☐	☐	☐	
¿Existe un procedimiento formal para la gestión de usuarios y accesos lógicos?	☐	☐	☐	
¿Se tiene definido el administrador de accesos que debe controlar los perfiles y roles?	☐	☐	☐	
¿Existe acuerdos de confidencialidad y responsabilidad de los usuarios?	☐	☐	☐	

Tabla 20.

Checklist para evaluación de controles de accesos lógicos

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-001-11				
EVALUACIÓN DE CONTROLES DE ACCESOS LÓGICOS				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.04 Gestionar la identidad del usuario y el acceso lógico			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se valida que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden y completos?	☐	☐	☐	
¿Se suspende temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, permisos temporales?	☐	☐	☐	
¿Se otorga accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados?	☐	☐	☐	
¿Se firma un convenio de confidencialidad para los usuarios externos o terceros?	☐	☐	☐	
¿Se tiene un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso?	☐	☐	☐	
¿Se tiene un registro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones?	☐	☐	☐	

Tabla 21.
Checklist para evaluación de controles de acceso físico

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-12				
EVALUACIÓN DE CONTROLES DE ACCESO FÍSICO				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.05 Gestionar el acceso físico a los activos de TI			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se gestiona adecuadamente las peticiones de acceso a las instalaciones físicas del área de Servidores?	☐	☐	☐	
¿Las peticiones formales de acceso al área de TI son autorizadas?	☐	☐	☐	
¿Se ha establecido el responsable para autorizar las peticiones de acceso a las ubicaciones de TI?	☐	☐	☐	
¿Se encuentras especificadas las áreas a las cuales el individuo tiene acceso autorizado?	☐	☐	☐	
¿Los perfiles de acceso a las ubicaciones de TI están definidos?	☐	☐	☐	
¿Se registra y supervisa todos los puntos de entrada a los emplazamientos del área de TI?	☐	☐	☐	
¿Se registra todos los visitantes a las dependencias, se incluyen contratistas y proveedores con fecha y hora de entrada y salida?	☐	☐	☐	
¿Se instruye a todo el personal para mantener visible la identificación en todo momento?	☐	☐	☐	
¿Se restringe el acceso a ubicaciones de TI sensibles mediante restricciones en el perímetro, tales como dispositivos de seguridad en puertas interiores y exteriores?	☐	☐	☐	
¿Se realiza regularmente formación de concienciación de seguridad física?	☐	☐	☐	
¿Se controla y limita el acceso a las instalaciones de procesamiento de información exclusivamente a personal autorizado?	☐	☐	☐	
¿Se prohíbe el uso de equipos de grabación, cámaras, equipos de vídeo y audio, dispositivos móviles, etc. a menos de que estén autorizados en las ubicaciones de TI?	☐	☐	☐	
¿Se prohíbe comer, beber y fumar dentro de las instalaciones de procesamiento de la información?	☐	☐	☐	

Tabla 22.
Checklist para evaluación de controles sobre información sensible

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-13				
EVALUACIÓN DE CONTROLES SOBRE INFORMACIÓN SENSIBLE				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.06 Gestionar documentos sensibles y dispositivos de salida			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existen procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida hacia dentro y fuera de la Universidad?	☐	☐	☐	
¿Se cuenta con un inventario de documentos sensibles y dispositivos de salida?	☐	☐	☐	
¿Existe el inventario de documentos sensibles y dispositivos de salida?	☐	☐	☐	
¿Se asigna privilegios de acceso a documentos sensibles y dispositivos de salida basándose en el principio del menor privilegio, para equilibrar riesgo y requerimientos del negocio?	☐	☐	☐	
¿Se designa responsables de los documentos sensibles?	☐	☐	☐	
¿Se designa responsables de los dispositivos de salida?	☐	☐	☐	
¿Se establece salvaguardas física apropiadas sobre formularios especiales y dispositivos sensibles?	☐	☐	☐	
¿Se destruye, borra o sobrescribe la información sensible y se protege los dispositivos de salida mediante técnicas que permitan la no recuperación de la información original?	☐	☐	☐	
¿Se evalúa los dispositivos deteriorados que contengan información sensible antes de enviar a reparación o darlos de baja?	☐	☐	☐	

Tabla 23.

Checklist para evaluación de controles para detección de eventos de seguridad de la información

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-001-14				
EVALUACIÓN DE CONTROLES PARA DETECCIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.07 Supervisar la Infraestructura para detectar eventos relacionados con seguridad			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se utilizan herramientas de detección de intrusiones?	☐	☐	☐	
¿Se guardan los registros de eventos críticos de seguridad de información?	☐	☐	☐	
¿Se revisa regularmente los registros de eventos para detectar incidentes potenciales?	☐	☐	☐	
¿Se define y comunica la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocidos?	☐	☐	☐	
¿Se define y comunica el impacto de los incidentes para permitir una respuesta acorde?	☐	☐	☐	
¿Se verifica que los tiques de incidentes de seguridad de la información se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales?	☐	☐	☐	
¿Se registra los eventos relacionados con la seguridad de la información, reportados por las herramientas de monitorización de la seguridad de la infraestructura?	☐	☐	☐	

Tabla 24.
Checklist para evaluación de controles para el sistema de control interno

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-15				
EVALUACIÓN DE CONTROLES PARA EL SISTEMA DE CONTROL INTERNO				
DOMINIO:	Supervisar, Evaluar y Valorar (MEA)			
PROCESO:	MEA02 Supervisar, evaluar y valorar el sistema de control interno			
PRÁCTICA:	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			
Auditor:				
Responsable:	**Fecha:**			
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se revisa de manera periódica el cumplimiento de las políticas y procedimientos de seguridad de la información?	☐	☐	☐	
¿Se determina el alcance del aseguramiento mediante la definición de controles de seguridad de la información a evaluar?	☐	☐	☐	
¿Se mide la eficacia de los controles de seguridad de la información?	☐	☐	☐	
¿Se realiza revisiones regulares sobre seguridad de la información sobre: aplicaciones, sistemas y redes?	☐	☐	☐	
¿Se realiza evaluaciones del aseguramiento de seguridad de la información para identificar debilidades de los controles?	☐	☐	☐	
¿Se revisa los informes de incidentes de seguridad de la información para identificar deficiencias de los controles?	☐	☐	☐	
¿Se informa y aborda las deficiencias detectadas sobre seguridad de la información?	☐	☐	☐	

- **Ejecución de las pruebas de auditoría**

Concluido el diseño de las pruebas de auditoría se procede con su aplicación. Para el efecto se identificará apropiadamente al personal a auditar, este personal es el responsable del proceso a evaluar.

Es importante coordinar con el personal a ser auditado, la fecha y hora para la aplicación de los checklist, es necesario considerar que las respuestas que proporcionen deben estar apropiadamente sustentadas, para esto se deberá planificar un periodo de tiempo adecuado. El auditado tendrá que responder a las preguntas con una de las tres opciones: SI, NO o PARCIAL y en el campo observaciones especificará el por qué no se cumple, si es el caso o indicará la evidencia del cumplimiento total o parcial. Los funcionarios que intervinieron en la Auditoría se listan a continuación: Directora de TI, Responsable de Redes y Comunicaciones, Auditor Interno.

En las tablas desde la 25 hasta la 39 se evidencia como se aplicó la Guía de Auditoria.

- **Checklist aplicados**

Tabla 25.
Evaluación de controles de estructuras organizativas

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-001-01				
EVALUACIÓN DE CONTROLES DE ESTRUCTURAS ORGANIZATIVAS				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO01 Gestionar el Marco de Gestión de TI			
PRÁCTICA:	APO01.01 Definir la estructura organizativa			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**02/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe una estructura orgánico funcional de TI?	☐	☐	☑	Existe una estructura de TI organizada informalmente como: la Dirección de TI, el responsable de Redes y Comunicaciones.
¿La estructura orgánica funcional de la UCACUE incluye una estructura específica para seguridad de la información?	☐	☐	☑	La Seguridad de la Información es considerada en la defensa perimetral de la Red de Datos solamente
¿Existe un ISSC (Comité de dirección de la seguridad de la información) o su equivalente?	☐	☑	☐	

Tabla 26.
Evaluación de controles de estructuras organizativas – roles y responsabilidades

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-001-02	

EVALUACIÓN DE CONTROLES DE ESTRUCTURAS ORGANIZATIVAS				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO01 Gestionar el Marco de Gestión de TI			
PRÁCTICA:	APO01.02 Establecer roles y responsabilidades.			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**02/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Las funciones y responsabilidades del personal han sido correctamente: establecidas, formalizadas, documentadas y aprobadas con respecto a seguridad de la información?	☐	☐	☑	Se han establecido pero informalmente
¿Se entrega formalmente a los funcionarios sus funciones y responsabilidades sobre seguridad de la información?	☐	☑	☐	
¿Existe un manual de cargos y funciones acorde a la estructura orgánico funcional que tome en cuenta la seguridad de la información?	☐	☑	☐	
¿Existe definidos los puestos de director de la seguridad de la Información (CISO) y de gerente de la seguridad de la información (ISM)?	☐	☑	☐	

Tabla 27.
Evaluación de controles de políticas de seguridad

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-03				
EVALUACIÓN DE CONTROLES DE POLÍTICAS DE SEGURIDAD				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO01 Gestionar el Marco de Gestión de TI			
PRÁCTICA:	APO01.03 Mantener los catalizadores del sistema de gestión			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**03/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
Principios, políticas y marcos				
¿Existe el marco de políticas establecido sobre la seguridad de la información?	☐	☑	☐	
¿Están definidos los principios seguridad de la información que den soporte a la institución y promuevan un comportamiento responsable en seguridad de la información?	☐	☑	☐	
¿Existe una política de seguridad de la información?	☐	☑	☐	
¿Existe una política de control de accesos?	☐	☑	☐	
¿Existe una política de seguridad de la información del personal?	☐	☐	☑	Las Políticas de TI para el uso de la información se encuentran en los servidores de datos y aplicaciones., pero no están documentadas.
¿Existe una política de gestión de incidentes de seguridad?	☐	☑	☐	
¿Existe una política de gestión de riesgos sobre la seguridad de la información?	☐	☑	☐	
¿Se comunica las políticas sobre seguridad de la información a las partes interesadas?	☐	☑	☐	
¿Las políticas sobre seguridad de la información se actualizan periódicamente de acuerdo a los requerimientos de la institución?	☐	☑	☐	
¿Existe procedimientos de Seguridad de Información?	☐	☑	☐	
Cultura, Ética y comportamiento				
¿Las personas respetan la importancia de las políticas de la seguridad de la información?	☐	☑	☐	No existen políticas sobre Seguridad de la Información.

Tabla 27.
Evaluación de controles de políticas de seguridad

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-03				
EVALUACIÓN DE CONTROLES DE POLÍTICAS DE SEGURIDAD				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO01 Gestionar el Marco de Gestión de TI			
PRÁCTICA:	APO01.03 Mantener los catalizadores del sistema de gestión			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**03/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Las personas poseen un nivel detallado y suficiente de orientación en seguridad de la información y se los anima a participar y cuestionar la situación actual de seguridad de la información?	☐	☑	☐	No existe capacitación en términos de Seguridad de la Información.
¿Todo el personal es responsable de que se proteja la información de la empresa?	☐	☐	☑	No existen políticas definidas para el control de cumplimiento, se realiza informalmente.
¿Las Partes Interesadas están informadas de cómo identificar y responder a las amenazas de seguridad de la información en el contexto de la Universidad?	☐	☑	☐	
¿La Dirección respalda y anticipa las innovaciones en seguridad de la información de manera proactiva?	☐	☑	☐	
¿La Dirección comunica a toda la Universidad las innovaciones en seguridad de la información?	☐	☑	☐	
¿La UCACUE es receptiva para tener en cuenta y manejar nuevos retos en materia de seguridad de la información?	☐	☑	☐	
¿La alta dirección reconoce el valor para la UCACUE de la Seguridad de la Información?	☐	☑	☐	No se da la importancia del tema de la Seguridad de la Información.
¿Se influye en el comportamiento del personal mediante comunicaciones, disposiciones, reglas y normas sobre la seguridad de la información?	☐	☑	☐	

Tabla 28.

Evaluación de controles acerca de la gestión del personal de seguridad de la información.

UNIVERSIDAD CATÓLICA DE CUENCA

AUD-FOR-TIC-001-04

EVALUACIÓN DE CONTROLES ACERCA DE LA GESTIÓN DEL PERSONAL DE SEGURIDAD DE LA INFORMACIÓN				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO07 Gestionar los Recursos Humanos			
PRÁCTICA:	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.			
Auditor:	**Ing. Carlos Encalada Loja, Ing. Aída Tenecela**			
Responsable: Ing. Mireya Calderón	**Fecha:**	**03/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe personal con funciones específicas correspondientes a seguridad de la información?	☐	☑	☐	
¿Se ha definido las habilidades y competencias para el personal de seguridad de la información?	☐	☑	☐	
¿El personal tiene habilidades y competencias en Gobierno de la Seguridad de la Información?	☐	☑	☐	
¿El personal tiene habilidades y competencias en Formulación de estrategia de seguridad de información?	☐	☑	☐	
¿El personal tiene habilidades y competencias en Gestión de riesgos de la información?	☐	☑	☐	
¿El personal tiene habilidades y competencias en desarrollo de la arquitectura de seguridad de la información?	☐	☐	☑	A nivel perimetral se realizan actualizaciones de seguridad pero no documentadas. Solamente un funcionario está capacitado en "Seguridad de la Información" pero no cumple estas funciones específicas.
¿El personal tiene habilidades y competencias en Operaciones de Seguridad de la Información?	☐	☐	☑	Solamente un funcionario, pero cumple funciones de administrador de red
¿El personal tiene habilidades y competencias en Evaluación, pruebas y cumplimiento de la información?	☐	☐	☑	Solamente un funcionario, pero cumple funciones de administrador de red
¿Existe programas de capacitación y desarrollo profesional en seguridad de información?	☐	☑	☐	
¿Existe programas de capacitación, certificación y desarrollo profesional en seguridad de información?	☐	☑	☐	

Tabla 29.
Evaluación de controles de los servicios, infraestructura y aplicaciones.

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-05				
EVALUACIÓN DE CONTROLES DE LOS SERVICIOS, INFRAESTRUCTURA Y APLICACIONES				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO09 Gestionar los acuerdos de servicio			
PRÁCTICA:	APO09.01 Identificar servicios TI APO09.02 Catalogar los servicios de TI			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**04/02/203**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se han identificado los servicios de TI relacionados con seguridad de información?	☐	☑	☐	
¿Se ha definido el portafolio de servicios de seguridad de la información?	☐	☑	☐	
¿Se cuenta con un catálogo de servicios de seguridad de la información?	☐	☑	☐	

Tabla 30.
Evaluación de controles para la gestión de la seguridad de la información

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-06				
EVALUACIÓN DE CONTROLES PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
DOMINIO:	Alinear, Planificar y Organizar (APO)			
PROCESO:	APO13 Gestionar la seguridad			
PRÁCTICA:	APO13.01 Establecer un SGSI			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**04/02/2013**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe un Sistema de Gestión de Seguridad de la Información que esté de acuerdo con las políticas de la UCACUE?	☐	☑	☐	
¿Existe una política de implementación del Sistema de Gestión de Seguridad de la Información?	☐	☑	☐	
¿Están definidos y comunicados los roles y responsabilidades de la gestión de la Seguridad de la Información?	☐	☑	☐	

Tabla 31.
Evaluación de controles de información relacionada con seguridad de la información

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-001-07	

EVALUACIÓN DE CONTROLES DE INFORMACIÓN RELACIONADA CON SEGURIDAD DE LA INFORMACIÓN		
DOMINIO:	Construir, Adquirir e Implementar (BAI)	
PROCESO:	BAI08 Gestionar el conocimiento	
PRÁCTICA:	BAI08.02 Identificar y clasificar las fuentes de información	
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela	
Responsable: Ing. Mireya Calderón	**Fecha:**	**04/02/2015**

VERIFICACIÓN	SI	NO	PARCIAL	OBSERVACIONES
¿Se ha definido los tipos de información relacionados con la seguridad de la información?	☑	☐	☐	Políticas de tecnologías a nivel de servidores de archivos
¿Se ha identificado los grupos de interés o partes interesadas de los diferentes tipos de información?	☑	☐	☐	Políticas de tecnologías a nivel de servidores de archivos
¿Los diferentes tipos de información están debidamente almacenados y son de acceso únicamente para las partes interesadas?	☐	☐	☑	Solo a nivel de los servidores de archivos
¿Están definidos los requisitos de configuración de la seguridad?	☐	☑	☐	

Tabla 32.
Evaluación de controles contra software malicioso.

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-08				
EVALUACIÓN DE CONTROLES CONTRA SOFTWARE MALICIOSO				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.01 Proteger contra software malicioso			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Andrés Torres S	**Fecha:**	**05/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe una política de prevención de software malicioso?	☐	☐	☑	Implementado en el antivirus para el control de software malintencionado, definición de reglas para control de spam, análisis de un nuevo virus, actualización de la BD contra ataques de día cero.
¿Existe una cultura de concienciación sobre: software malicioso, cómo proceder frente a los mismos y responsabilidades de prevención?	☐	☑	☐	No existe, tuvieron problemas de encriptación de la información en una PC, el personal no está advertido de este tipo de problemas de seguridad.
¿Se ha instalado y activado herramientas de protección frente a software malicioso?	☑	☐	☐	McAfee, tiene licenciamiento
¿Los ficheros de definición de software malicioso se actualizan periódicamente automática o semiautomáticamente?	☑	☐	☐	Se actualiza automáticamente
¿Se distribuye el software de protección de forma centralizada?	☑	☐	☐	Mediante el servicio de Antivirus McAfee
¿Se utiliza una configuración centralizada del software de protección?	☑	☐	☐	Mediante el servicio de Antivirus MacAfee
¿Se realiza gestión de cambios en la configuración del software de protección?	☑	☐	☐	Mediante solicitud de protección a determinadas carpetas dirigida al director de TI
¿Se revisa y evalúa regularmente la información sobre nuevas posibles amenazas?	☑	☐	☐	La información enviada por el CSIRT de CEDIA, Microsoft MacAfee, Kapersky.
¿Se realiza filtrado del tráfico entrante para protegerse frente a información no solicitada?	☑	☐	☐	El acceso a servidores está bloqueado a usuarios no registrado mediante reglas en el firewall perimetral
¿Se realiza capacitación periódica sobre software malicioso?	☐	☑	☐	

Tabla 32.
Evaluación de controles contra software malicioso.

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-08				
EVALUACIÓN DE CONTROLES CONTRA SOFTWARE MALICIOSO				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.01 Proteger contra software malicioso			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Andrés Torres S	**Fecha:**	**05/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se realiza capacitación periódica sobre el uso de correo electrónico, internet e instalación de software no autorizado?	☐	☑	☐	
¿Existe un listado de software autorizado por la institución?	☑	☐	☐	Existe el listado de software que posee licenciamiento y está autorizado a instalarse en todas la dependencias de la Universidad
¿Se prohíbe el uso de software no autorizado por la institución?	☑	☐	☐	Existe un documento de prohibición
¿Se establece procedimientos para evitar obtención o descarga de archivos y software de procedencia dudosa?	☐	☑	☐	
¿Los sistemas operativos y sistemas de procesamiento de información están actualizados con las últimas versiones de seguridad disponibles?	☐	☐	☑	No existe un registro de actualizaciones, la mayoría se realiza automáticamente pero no se revisa
¿Se revisa periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la institución?	☐	☐	☑	A nivel de Servidores
¿Se verifica antes de su uso, la presencia de virus en archivos de medios electrónicos?	☑	☐	☐	Está aplicado la revisión de los pendrive cuando se conectan
¿Existen procedimientos para verificar toda la información relativa a software malicioso?	☐	☑	☐	
¿Se emiten boletines informativos de alerta con información precisa acerca de software malicioso?	☐	☑	☐	
¿Se ha contratado con el proveedor de Internet o del canal de datos los servicios de filtrado de: virus, spam, programas maliciosos (malware), en el perímetro externo?	☑	☐	☐	Mediante el CSIRT de CEDIA

Tabla 33.
Evaluación de controles de seguridad de la red

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-09				
EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA RED				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.02 Gestionar la seguridad de la red y las conexiones			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Andrés Torres Soto	**Fecha:**	**06/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe una política de seguridad en la conectividad basada en el análisis de riesgos y los requerimientos del negocio?	☐		☑ ☐	
¿El acceso a la información y a la red está restringido sólo a dispositivos autorizados?	☑	☐	☐	Mediante la implementación de reglas como el acceso de la información desde la red Wireless a la red de datos, a través de una solitud, se da permiso mediante filtrado por Mac para que acceda a la rede de datos
¿Los dispositivos que tienen acceso a la red están configurados a fin de que soliciten contraseña de acceso a la red?	☑	☐	☐	Mediante el servicio RADIUS
¿Se ha implementado mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones?	☐	☐	☑	No se cuenta con IDS (Sistema de detección de intrusos).
¿Existen reglas apropiadas para controlar el tráfico entrante y saliente a nivel de firewall?	☐	☐	☑	No están documentadas
¿Se aplica los protocolos de seguridad aprobados a las conexiones de red?	☑	☐	☐	Si se aplica mediante el servicio OpenVPN
¿Se configura los equipamientos de red de forma segura?	☐	☐	☑	Se aplica pero no está documentado el proceso
¿Se establece mecanismos de confianza para dar soporte a la transmisión y recepción segura de información?	☑	☐	☐	Si se aplica mediante el servicio OpenVPN
¿Se realiza pruebas de ajustes periódicas para determinar la adecuación de la protección de la red?	☐	☐	☑	Se aplica pero no está documentado el proceso

Tabla 33.
Evaluación de controles de seguridad de la red

UNIVERSIDAD CATÓLICA DE CUENCA

AUD-FOR-TIC-001-09

EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA RED				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.02 Gestionar la seguridad de la red y las conexiones			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Andrés Torres Soto	**Fecha:**	**06/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se establecen procedimientos y responsabilidades para la gestión de equipos remotos como el caso de re-direccionamiento de puertos y accesos por VPNs, se incluye el área de operaciones y el área de usuarios finales?	☑	☐	☐	Si se aplica y el instructivo está en la página web para conexiones remotas autorizadas
¿Se dispone de un esquema de red de los enlaces de datos, Internet y redes locales, así como la documentación respectiva?	☐	☐	☑	Están desarrollados pero no documentadas
¿Se incorpora tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red?	☐	☐	☑	No está documentado
¿Se definen procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red cuando sea necesario?	☐	☐	☑	No se tiene definido ningún procedimiento se realiza directamente en las configuraciones de los firewalls

Tabla 34.
Evaluación de controles de seguridad de los usuarios

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-10				
EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LOS USUARIOS				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.03 Gestionar la seguridad de los puestos de usuarios finales			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**09/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existe una política de seguridad para dispositivos de usuarios finales?	☐	☑	☐	
¿Se configura los sistemas operativos de forma segura?	☑	☐	☐	Se activa el firewall de los sistemas operativos Windows, antivirus se dan de baja los clientes de servicios que no están utilizados
¿Se implementa mecanismos de bloqueo de los dispositivos no autorizados para acceso a la red?	☐	☑	☐	
¿Se utilizan mecanismos para cifrado de la información almacenada de acuerdo a su clasificación y a su criticidad?	☐	☑	☐	
¿Se gestiona el acceso y control remoto entre las estaciones de los usuarios?	☐	☑	☐	
¿Se gestiona la configuración de la red de forma segura?	☑	☐	☐	Mediante la activación del firewall local de la estación de trabajo
¿Se implementa filtrado del tráfico de la red en dispositivos de usuario finales?	☑	☐	☐	Mediante VLANs
¿Se provee de protección física a los dispositivos de usuario finales?	☐	☐	☑	A nivel de UPS solamente
¿Se identifica los medios de almacenamiento de información que requieran eliminación segura?	☐	☑	☐	
¿Se desecha (donación/desecho) los dispositivos de usuario finales de forma segura a fin de que la información sea eliminada completamente?	☐	☐	☑	Se reutilizan los equipos en función de la capacidad del equipo que se disponga.
¿Se almacena de forma segura los medios que contienen información sensible?	☐	☑	☐	

Tabla 34.
Evaluación de controles de seguridad de los usuarios

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-10				
EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LOS USUARIOS				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.03 Gestionar la seguridad de los puestos de usuarios finales			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**09/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se registra la eliminación de los medios de almacenamiento para mantener pruebas de auditoría?	☐	☑	☐	
¿Se ha establecido un procedimiento para la gestión de todos los medios removibles?	☐	☑	☐	
¿Se ha establecido permisos para la conexión de los medios removibles y se registra la conexión y retiro, para pruebas de auditoría?	☐	☑	☐	
¿Se almacena los medios removibles en un ambiente seguro, según las especificaciones de los fabricantes?	☐	☑	☐	

Tabla 35.
Evaluación de controles de accesos lógicos.

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-11				
EVALUACIÓN DE CONTROLES DE ACCESOS LÓGICOS				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.04 Gestionar la identidad del usuario y el acceso lógico			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**10/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se establecen permisos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio?	☐	☐	☑	No está documentado
¿Se alinea los permisos de acceso a los roles y responsabilidades definidos, basándose en los principios de menos privilegio, necesidad de tener y necesidad de conocer?	☐	☐	☑	No está documentado
¿Se autentican todos los accesos a los activos de información basándose en su clasificación de seguridad?	☐	☑	☐	No existen políticas definidas sobre la seguridad de la información.
¿Se administra todos los cambios de permisos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno mediante un proceso formal de autorización?	☐	☑	☐	
¿Se verifica que los controles de autenticación han sido administrados adecuadamente?	☐	☑	☐	
¿Existe segregación y gestión de cuentas de usuarios privilegiadas?	☐	☑	☐	No está implementado el Directorio Activo con la definición de roles para la autenticación
¿Se realiza regularmente revisiones de la gestión de todas las cuentas y privilegios relacionados?	☐	☑	☐	
¿Se mantiene un registro de auditoría de los accesos a la información clasificada como altamente sensible?	☐	☑	☐	
¿Existe un procedimiento formal para la gestión de usuarios y accesos lógicos?	☐	☑	☐	

Tabla 35.
Evaluación de controles de accesos lógicos.

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-11				
EVALUACIÓN DE CONTROLES DE ACCESOS LÓGICOS				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.04 Gestionar la identidad del usuario y el acceso lógico			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**10/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se tiene definido el administrador de accesos que debe controlar los perfiles y roles?	☐	☑	☐	
¿Existe acuerdos de confidencialidad y responsabilidad de los usuarios?	☐	☑	☐	
¿Se valida que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden y completos?	☐	☑	☐	No está implementado Directorio Activo
¿Se suspende temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales?	☐	☑	☐	No está implementado Directorio Activo
¿Se otorga accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados?	☐	☑	☐	No está implementado Directorio Activo
¿Se firma un convenio de confidencialidad para los usuarios externos o terceros?	☐	☑	☐	
¿Se tiene un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso?	☐	☑	☐	
¿Se tiene un registro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones?	☐	☑	☐	

Tabla 36.
Evaluación de controles de acceso físico

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-001-12				
EVALUACIÓN DE CONTROLES DE ACCESO FÍSICO				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.05 Gestionar el acceso físico a los activos de TI			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Andrés Torres Soto	**Fecha:**	**11/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se gestiona adecuadamente las peticiones y concesiones de acceso a las instalaciones físicas del área de Servidores?	☐	☑	☐	
¿Las peticiones formales de acceso al área de TI son autorizadas?	☐	☑	☐	
¿Se ha establecido el responsable para autorizar las peticiones de acceso a las ubicaciones de TI?	☐	☑	☐	
¿Se encuentras especificadas las áreas a las cuales el individuo tiene acceso autorizado?	☐	☑	☐	
¿Los perfiles de acceso a las ubicaciones de TI (salas de servidores) están definidos?	☐	☑	☐	
¿Se registra y supervisa todos los puntos de entrada a los emplazamientos del área de TI?	☐	☑	☐	
¿Se registra todos los visitantes a las dependencias, se incluye contratistas y proveedores con fecha y hora de entrada y salida?	☐	☑	☐	
¿Se instruye a todo el personal para mantener visible la identificación en todo momento?	☐	☐	☑	Si se instruye pero el personal no lo utiliza
¿Se restringe el acceso a ubicaciones de TI sensibles mediante el establecimiento de restricciones en el perímetro, tales como dispositivos de seguridad en puertas interiores y exteriores?	☐	☑	☐	

Tabla 36.
Evaluación de controles de acceso físico

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-12				
EVALUACIÓN DE CONTROLES DE ACCESO FÍSICO				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.05 Gestionar el acceso físico a los activos de TI			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Andrés Torres Soto	**Fecha:**	**11/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se realiza regularmente formación de concienciación de seguridad física?	☐	☑	☐	
¿Se controla y limita el acceso a las instalaciones de procesamiento de información exclusivamente a personal autorizado?	☐	☑	☐	
¿Se prohíbe el uso de equipos de grabación, cámaras, equipos de vídeo y audio, dispositivos móviles, etc. a menos de que estén autorizados en las ubicaciones de TI?	☐	☑	☐	
¿Se prohíbe comer, beber y fumar dentro de las instalaciones de procesamiento de la información?	☐	☐	☑	Si existe la política pero a nivel de todo el edifico no solamente de las áreas de TI mediante oficio al personal desde la Dirección Administrativa

Tabla 37.
Evaluación de controles sobre información sensible.

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-13				
EVALUACIÓN DE CONTROLES SOBRE INFORMACIÓN SENSIBLE				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.06 Gestionar documentos sensibles y dispositivos de salida			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Mireya Calderón	**Fecha:**	**11/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Existen procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida hacia dentro y fuera de la Universidad?	☐	☑	☐	Solamente se formatea los discos y se respalda nada mas
¿Se cuenta con un inventario de documentos sensibles y dispositivos de salida?	☐	☐	☑	Existe un inventario de reglamentación, facturas electrónicas. Si esta normado la protección
¿Existe el inventario de documentos sensibles y dispositivos de salida?	☐	☑	☐	
¿Se asigna privilegios de acceso a documentos sensibles y dispositivos de salida basándose en el principio del menor privilegio, equilibrando riesgo y requerimientos del negocio?	☐	☑	☐	No está implementado el Directorio Activo
¿Se designa responsable de los documentos sensibles?	☐	☑	☐	
¿Se designa responsable de los dispositivos de salida?	☐	☑	☐	
¿Se establece salvaguardas física apropiadas sobre formularios especiales y dispositivos sensibles?	☐	☑	☐	
¿Se destruye, borra o sobrescribe la información sensible y se protege los dispositivos de salida mediante técnicas que permitan la no recuperación de la información original?	☐	☐	☑	Se hace pero no está reglamentado
¿Se evalúa los dispositivos deteriorados que contengan información sensible antes de enviar a reparación o darlos de baja?	☐	☐	☑	Se analiza los equipos del personal que renuncia o para darlos de baja, no está documentado el procedimiento

Tabla 38.
Evaluación de controles para detección de eventos de seguridad de la información

UNIVERSIDAD CATÓLICA DE CUENCA				
AUD-FOR-TIC-001-14				
EVALUACIÓN DE CONTROLES PARA DETECCIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN				
DOMINIO:	Entrega, Servicio y Soporte (DSS)			
PROCESO:	DSS05 Gestionar Servicios de Seguridad			
PRÁCTICA:	DSS05.07 Supervisar la Infraestructura para detectar eventos relacionados con seguridad			
Auditor:	Ing. Carlos Encalada Loja, Ing. Aída Tenecela			
Responsable: Ing. Andrés Torres Soto	**Fecha:**	**12/02/2015**		
VERIFICACIÓN	**SI**	**NO**	**PARCIAL**	**OBSERVACIONES**
¿Se utilizan herramientas de detección de intrusiones?	☐	☑	☐	
¿Se guardan los registros de eventos críticos de seguridad de información?	☐	☐	☑	En los archivos LOG de los servidores firewall, no está documentado el procedimiento.
¿Se revisa regularmente los registros de eventos para detectar incidentes potenciales?	☐	☐	☑	Se revisa constantemente los archivos de tipo LOG de los servidores firewall, no existe un procedimiento para informar y documentar los hallazgos
¿Se define y comunica la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocidos?	☐	☑	☐	
¿Se define y comunica el impacto de los incidentes para permitir una respuesta acorde?	☐	☑	☐	
¿Se verifica que los tiques de incidentes de seguridad de la información se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales?	☐	☑	☐	No se tiene implementado el servicio de mesa de ayuda
¿Se registra los eventos relacionados con la seguridad de la información, reportados por las herramientas de monitorización de la seguridad de la infraestructura?	☐	☑	☐	No se documenta

Tabla 39.
Evaluación de Controles para el Sistema de Control Interno

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-001-15	

EVALUACIÓN DE CONTROLES PARA EL SISTEMA DE CONTROL INTERNO		
DOMINIO:	Supervisar, Evaluar y Valorar (MEA)	
PROCESO:	MEA02 Supervisar, evaluar y valorar el sistema de control interno	
PRÁCTICA:	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	
Auditor:	**Ing. Carlos Encalada Loja, Ing. Aída Tenecela**	
Responsable: Eco. José Guzmán	**Fecha:**	**12/02/2015**

VERIFICACIÓN	SI	NO	PARCIAL	OBSERVACIONES
¿Se revisa de manera periódica el cumplimiento de las políticas y procedimientos de seguridad de la información?	☐	☑	☐	No se tiene definido políticas de seguridad de la información
¿Se determina el alcance del aseguramiento mediante la definición de controles de seguridad de la información a evaluar?	☐	☑	☐	
¿Se mide la eficacia de los controles de seguridad de la información?	☐	☑	☐	No se realizan acciones de control interno
¿Se realiza revisiones regulares sobre seguridad de la información sobre: aplicaciones, sistemas y redes?	☐	☑	☐	No se tiene registro de las revisiones
¿Se realiza evaluaciones del aseguramiento de seguridad de la información para identificar debilidades de los controles?	☐	☑	☐	
¿Se revisa los informes de incidentes de seguridad de la información para identificar deficiencias de los controles?	☐	☑	☐	
¿Se informa y aborda las deficiencias detectadas sobre seguridad de la información?	☐	☑	☐	

2.2.6 Determinación de resultados y productos de la Auditoría

- **Análisis de información y determinación de resultados.**

Aplicado los checklist al personal correspondiente se procede con el levantamiento de hallazgos de auditoría, los que para un mejor entendimiento y presentación se han establecido mediante un formato identificado como **AUD-FOR-TIC-002**. 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, que son: 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 identificados. Todos los hallazgos identificados, las conclusiones y recomendaciones formarán parte del informe preliminar de auditoría (ver Tabla 40).

Tabla 40.
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.	

- **Informe preliminar de Auditoría**

El informe preliminar de auditoría comprende los hallazgos identificados así como las conclusiones y recomendaciones que el auditor plantea, dicho informe constituye la base para la elaboración del informe final.

El informe preliminar de auditoría debe ser validado con los todos los auditados, quienes aprobarán el contenido de los hallazgos, sus conclusiones y recomendaciones, solamente cuando este informe preliminar haya sido validado podrá emitirse el informe final de auditoría.

A partir de la tabla 41 a la 57, se detallan los hallazgos identificados como implementación de la presente "Guía de Auditoría". Estos documentos han sido validados por el personal auditado de la Universidad Católica de Cuenca.

- **Hallazgos identificados**

Tabla 41.
Hallazgo respecto a definir la estructura organizativa

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-002-01	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Alinear, Planificar y Organizar (APO)
Proceso:	APO01 Gestionar el Marco de Gestión de TI
Práctica:	APO01.01 Definir la estructura organizativa
Evidencia:	AUD-FOR-TIC-001-01
Condición	
La UCACUE tiene una estructura orgánica definida en la que consta el Departamento de TIC cuya participación y apoyo a las decisiones de la institución es tomada en cuenta en las reuniones de directorio. No existe un área de Seguridad de la Información como tampoco personal encargado de dichas funciones.	
Criterio	
De acuerdo a COBIT 5 para Seguridad de la Información se recomienda establecer una estructura orgánica interna que refleje las necesidades del negocio y las prioridades de TI, implementar estructuras de dirección necesarias para permitir que la toma de decisiones de gestión se lleve a cabo de la forma más eficaz y eficiente posible, establecer un ISSC (Comité de dirección de la Seguridad de la Información) o su equivalente.	
Causa	
No se ha gestionado la creación en la estructura orgánica de la UCACUE de un área específica para Seguridad de la Información.	
Efecto	
Poca o nula actividad para implementación de iniciativas de Seguridad de la Información lo que convierte a la UCACUE en vulnerable ante situaciones que afecte la Seguridad de la Información.	
Conclusión	
La UCACUE no tiene una estructura orgánico funcional de TI definida, que corresponda a los procesos que actualmente ejecuta, no posee un Comité de Dirección de la Seguridad de la Información para asegurar que se implemente y controle las buenas prácticas en relación a Seguridad de la Información.	
Recomendación.	
A la Directora de Tecnologías de Información y Comunicación: • Gestionar la creación y aprobación de la estructura orgánico funcional de TI en coordinación con el Departamento de Planificación, que contenga cómo mínimo las siguientes áreas funcionales: * Redes y Comunicaciones * Desarrollo de software * Soporte * Seguridad de la Información, con funciones de gestión y ejecución desagregadas, lo que permita una adecuada toma de decisiones. • Gestionar la creación del Comité de dirección de la Seguridad de la Información que permita administrarla correctamente.	

Tabla 42.

Hallazgo respecto a establecer roles y responsabilidades

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-002-02	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Alinear, Planificar y Organizar (APO)
Proceso:	APO01 Gestionar el Marco de Gestión de TI
Práctica:	APO01.02 Establecer roles y responsabilidades.
Evidencia:	AUD-FOR-TIC-001-02
Condición	
La UCACUE, no cuenta con el cargo y manual de funciones en los que se haya establecido los roles y responsabilidades del personal y sus perfiles con relación a la Seguridad de la Información.	
Criterio	
De acuerdo a COBIT 5 para Seguridad de la Información se recomienda establecer, acordar y comunicar roles y responsabilidades del personal de TI que reflejen claramente las necesidades generales del área, los objetivos de TI, así como la autoridad y la rendición de cuentas.	
Causa	
La Universidad Católica no cuenta con personal específico para el cargo de: Director de la Seguridad de la Información y Gerente de Seguridad de la Información.	
Efecto	
No se realiza ninguna gestión y ejecución que corresponda a la Seguridad de la Información lo que provoca que la Universidad sea vulnerable a cualquier ataque interno o externo	
Conclusión	
La UCACUE al no disponer de una estructura orgánico funcional en el que conste el departamento de la Seguridad de la Información, imposibilita establecer nuevas contrataciones que se requieran producto del análisis del personal disponibles a las funciones que estos deberán asumir en términos de Seguridad.	
Recomendación.	
Al Vicerrector Administrativo: • Asegurar y Gestionar la definición de puestos para la Seguridad de la Información: • Director de la Seguridad de la Información (CISO) • Gerente de la Seguridad de la Información (ISM) **A la Directora de Tecnologías de Información y Comunicación:** • Gestionar el desarrollo del manual de funciones y operaciones, establecer roles y responsabilidades de Seguridad de la Información. Determinar el grado en que otros roles organizativos tiene obligaciones en Seguridad de la Información y añadirlas a las descripciones de puesto correspondiente.	

Tabla 43.

Hallazgo respecto a mantener los catalizadores del sistema de gestión

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-03	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Alinear, Planificar y Organizar (APO)
Proceso:	APO01 Gestionar el Marco de Gestión de TI
Práctica:	APO01.03 Mantener los catalizadores del sistema de gestión
Evidencia:	AUD-FOR-TIC-001-03
Condición	
La UCACUE no cuenta con políticas relacionadas con Seguridad de la Información, marcos de referencia o buenas prácticas para la gestión de la Seguridad de la Información por lo que tampoco se fomenta una cultura, ética y comportamiento adecuados en cuanto a Seguridad de la Información se refiere.	
Criterio	
Según COBIT 5 para Seguridad de la Información se debe mantener los catalizadores del sistema de gestión y del entorno de control para las TI de la Institución que incluyan una comunicación clara de expectativas o requisitos. El sistema de gestión debe fomentar la cooperación interdepartamental, el trabajo en equipo y promover el cumplimiento de la mejora continua basada siempre alcanzar la Seguridad de la Información	
Causa	
No están establecidos los principios, políticas, directrices y marcos de gestión de Seguridad de la Información.	
Efecto	
Desprotección de los recursos de información de la Universidad y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, lo que afecta el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.	
Conclusión	
La UCACUE no ha definido una Política de Seguridad de la Información que sirva de base y directriz para alinear a las estrategias empresariales y lograr el cumplimiento de las metas y objetivos propuesto en lo relacionado a Seguridad de la Información, lo que incrementa innecesariamente el riesgo de alteración, pérdida o fuga de la información institucional	
Recomendación.	
Al Vicerrector Administrativo: • Asegurar que el Responsable de Seguridad de la Información defina e implemente políticas, directrices que forme parte de la cultura organizacional de la UCACUE. Entre las políticas más relevantes deben constar: • Política de Seguridad de la Información* • Política de control de acceso* • Política de Seguridad de la Información del personal* • Política de gestión de incidentes sobre Seguridad de la Información* • Política de gestión de riesgos de Seguridad de la Información. **A la Directora de Tecnología de Información y Comunicaciones:** • Elaborar los procedimientos para aplicar y hacer cumplir las políticas y normas sobre Seguridad de la Información mediante un manifiesto compromiso de todos los funcionarios que de una u otra manera están vinculados a la gestión, lo que contribuirá la difusión, consolidación y cumplimiento. • Asegurar la implementación de las medidas de seguridad comprendidas en estas políticas y directrices mediante comunicaciones o disposiciones.	

Tabla 44.

Hallazgo respecto a mantener la dotación de personal suficiente y adecuado.

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-04	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Alinear, Planificar y Organizar (APO)
Proceso:	APO07 Gestionar los Recursos Humanos
Práctica:	APO07.01 Mantener la dotación de personal suficiente y adecuado
Evidencia:	AUD-FOR-TIC-001-04
Condición	
Además de la Directora de TI no existen otras direcciones o jefaturas encargadas de la Seguridad de la Información.	
Criterio	
Según COBIT 5 para seguridad de la información se debe evaluar las necesidades de personal de forma regular ante cambios importantes en la Institución o en los entornos operativos o de TI, para asegurar que la Institución tiene suficientes recursos humanos para apoyar las metas y objetivos de seguridad de la información de la UCACUE	
Causa	
El personal de TI en las condiciones que opera actualmente, no cubre las necesidades para la implementación de Seguridad de la Información en la UCACUE.	
Efecto	
Desorganización en el departamento de TI lo que imposibilita el cumplimiento de actividades y objetivos del área menos aún el alcance de Seguridad de la Información.	
Conclusión	
No se ha realizado una estudio para establecer una adecuada segregación de funciones que incluya roles específicos para seguridad de la información.	
Recomendación.	
Al Vicerrector Administrativo: • Asegurar que se tome en cuenta los requisitos de Seguridad de la Información asociados a dotar el personal adecuado para los procesos de seguridad y que éstos sean incorporados en los procesos de contratación de TI para empleados, subcontratistas y proveedores.	

Tabla 45.
Hallazgo respecto a identificar el personal clave de TI

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-05	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Alinear, Planificar y Organizar (APO)
Proceso:	APO07 Gestionar los Recursos Humanos
Práctica:	APO07.02 Identificar personal clave de TI
Evidencia:	AUD-FOR-TIC-001-04
Condición	
No se ha identificado el personal clave para las actividades de Seguridad de la Información.	
Criterio	
Conforme a COBIT 5 para Seguridad de la Información se debe Identificar al personal clave de TI para reducir al mínimo las dependencias unipersonales en la realización de una función crítica de trabajo, mediante la captura de conocimiento, intercambio de conocimiento y la planificación de la sucesión y el respaldo del personal.	
Causa	
No existe una estructura funcional para la Seguridad de la Información, en consecuencia, no se puede establecer una adecuada segregación de funciones.	
Efecto	
Dependencia en cierto personal sobre el que radica todo el conocimiento y la responsabilidad en términos de Seguridad de la Información.	
Conclusión	
La UCACUE no dispone de personal calificado que se haga cargo de la Seguridad de la Información a nivel de: Confidencialidad, Integridad y Disponibilidad; causados por fallas intencionales o accidentales a nivel de: Usuarios, Software o Hardware.	
Recomendación.	
Al Vicerrector Administrativo: • Asegurar la segregación de funciones en los puestos críticos del área de TI y de Seguridad de la Información. • Identificar al personal clave y de TI y Seguridad de la Información y elaborar planes de sucesión del mismo.	

Tabla 46.

Hallazgo respecto a mantener las habilidades y competencias del personal

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-06	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Alinear, Planificar y Organizar (APO)
Proceso:	APO07 Gestionar los Recursos Humanos
Práctica:	APO07.03 Mantener las habilidades y competencias del personal
Evidencia:	AUD-FOR-TIC-001-04
Condición	
El departamento de TI de la UCACUE cuanta con el plan de capacitación para el personal de TI, pero no está alineado a la segregación de funciones, no cuenta con un plan de capacitación para actividades específicas en temas de Seguridad de la Información.	
Criterio	
COBIT 5 para seguridad de la información sugiere definir y gestionar las habilidades y competencias necesarias del personal, verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones y/o experiencia. Verificar que estas competencias se mantienen mediante programas de capacitación y certificación que correspondan; proporcionar a los empleados formación continua y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas planteadas.	
Causa	
Falta de planificación de capacitaciones en áreas específicas y acordes a las requerimientos de seguridad de la información.	
Efecto	
La UCACUE es vulnerable ante la posible pérdida y/o robo de información o mal uso de la misma, principalmente por la no existencia de personal suficiente que cumplan con actividades para la protección de la información.	
Conclusión	
No existe personal suficiente con las habilidades y competencias para asumir los roles de dirección y operación del área de Seguridad de la Información.	
Recomendación.	
Al Vicerrector Administrativo: • Establecer las competencias y habilidades de los encargados del área de Seguridad, que incluyan competencias y habilidades en: * Gobierno, Formulación de estrategia, Gestión de riesgo, Desarrollo de arquitectura de Seguridad de la Información. * Operaciones de Seguridad de la Información * Evaluación, pruebas y cumplimiento de la información. **A la Directora de TI** • Gestionar el plan de capacitación en concordancia con la creación del área de Seguridad de la Información así como las competencias y habilidades establecidas necesarias, considerar el uso de programas de certificación del personal que aseguren un conjunto de habilidades profesionales de calidad en Seguridad de la Información	

Tabla 47.
Hallazgo respecto a catalogar los servicios de TI

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-07	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Alinear, Planificar y Organizar (APO)
Proceso:	APO09 Gestionar los acuerdos de servicio
Práctica:	APO09.01 Identificar servicios TI APO09.02 Catalogar los servicios de TI
Evidencia:	AUD-FOR-TIC-001-05
Condición	
El departamento de TIC de la UCACUE no cuenta con un portafolio de servicios específicos de las áreas funcionales establecidas.	
Criterio	
COBIT 5 para seguridad de la información sugiere analizar los requisitos del negocio y el modo en que los servicios de TI y los niveles de servicio soportan los procesos de negocio; discutir y acordar los servicios potenciales y niveles de servicio con el negocio y compararlos con el vigente portafolio de servicios para identificar servicios nuevos o modificarlos. Definir y mantener uno o más catálogos de servicios para grupos destinatarios relevantes.	
Causa	
Falta de gestión de la Dirección de TI en analizar los requisitos de la UCACUE que determinen los servicios de TI y los niveles de servicios que den soporte a los procesos de protección de la información.	
Efecto	
La UCACUE está expuesta a todo riesgo de Seguridad de la Información internos.	
Conclusión	
No existe gestión de servicios.	
Recomendación.	
A la Directora de Tecnología de Información y Comunicaciones: • Realizar la planeación estratégica del área de TI en el que se establezca como prioridad la definición de los servicios de TI que ofrece, en base a un estudio de necesidades y objetivos de la UCACUE. • Definir el portafolio de servicios de seguridad de la información en coordinación con el responsable del área de seguridad a crearse.	

Tabla 48.
Hallazgos con respecto a establecer un SGSI

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-08	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Alinear, Planificar y Organizar (APO)
Proceso:	APO13 Gestionar la seguridad
Práctica:	APO13.01 Establecer un SGSI
Evidencia:	AUD-FOR-TIC-001-06
Condición	
La UCACUE no cuenta con 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.	
Criterio	
COBIT 5 para seguridad de la información sugiere establecer y mantener un Sistema de Gestión de Seguridad de la Información que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineado con los requerimientos de la Institución.	
Causa	
Falta de gestión de la Dirección de TI para la implementación de un sistema de gestión de la seguridad de la Información (SGSI).	
Efecto	
La UCACUE está sujeta a riesgos y amenazas que pueden generarse desde dentro de la propia UCACUE o desde el exterior.	
Conclusión	
No existe un área de Seguridad de la información que defina, administre y supervise el SGSI	
Recomendación.	
A la Directora de Tecnología de Información y Comunicaciones: • Gestionar la implementación del Sistema de Gestión de Seguridad de la Información, basado en la norma ISO/IEC 27001 que debe ser establecido y mantenido por el Responsable de Seguridad de la Información.	

Tabla 49.
Hallazgo respecto a identificar y clasificar las fuentes de información

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-09	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Construir, Adquirir e Implementar (BAI)
Proceso:	BAI08 Gestionar el conocimiento
Práctica:	BAI08.02 Identificar y clasificar las fuentes de información
Evidencia:	AUD-FOR-TIC-001-07
Condición	
De manera formal no se ha identificado y clasificado las fuentes de información sino que existe una clasificación a nivel de servidores de archivos.	
Criterio	
COBIT 5 para seguridad de la información recomienda identificar, validar y clasificar las diversas fuentes de información interna y externa necesarias para posibilitar el uso y la operación efectivos de los procesos de negocio de los servicios de TI	
Causa	
No se han definido políticas de prioridad y criticidad de la información	
Efecto	
Puede existir información crítica que no esté debidamente protegida y custodiada.	
Conclusión	
La UCACUE está expuesta a la fuga o pérdida de información crítica de la Institución.	
Recomendación.	
A la Directora de Tecnología de Información y Comunicaciones: • Gestionar y asegurar la creación de políticas para la clasificación de la información de acuerdo a la sensibilidad de la misma como de su uso e intercambio entre los usuarios internos y externos de la UCACUE. • Desarrollar una estructura para la clasificación de la información no solamente a nivel de los servidores de archivos sino a nivel de Institución.	

Tabla 50.
Hallazgo respecto a proteger contra software malicioso

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-10	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Entrega, Servicio y Soporte (DSS)
Proceso:	DSS05 Gestionar Servicios de Seguridad
Práctica:	DSS05.01 Proteger contra software malicioso
Evidencia:	AUD-FOR-TIC-001-08
Condición	
En la UCACUE se ha implementado medidas para proteger los sistemas de información y la tecnología contra código malicioso sin embargo no se ha enfocado en concientización a los usuarios que constituyen uno de los medios más potenciales para propagación de software malicioso.	
Criterio	
COBIT 5 para seguridad de la información sugiere Implementar y mantener efectivas medidas preventivas, de detección y correctivas a lo largo de la organización, para proteger los sistemas de información y tecnología de software malicioso como: virus, gusanos, software espía, y correo basura entre otros.	
Causa	
No se realiza programas de capacitación y concientización sobre temas relacionados a software malicioso que ayuden a la prevención.	
Efecto	
Incremento de las vulnerabilidades de infección con software malicioso que afecten a la disponibilidad e integridad de la información.	
Conclusión	
La UCACUE ha realizado esfuerzos con respecto a la protección contra código malicioso con lo que cumple con la mayoría de los controles pero no ha considerado un factor importante que son las personas.	
Recomendación.	
Al Vicerrector Administrativo. • Asegurar que el responsable de seguridad de la información establezca políticas y procedimientos para la protección contra software malicioso. • Velar por el cumplimiento de las políticas y procedimientos establecidos. **A la Directora de Tecnologías de Información y Comunicación:** • Coordinar con la Dirección de Comunicación y Dirección de Talento Humano a fin de elaborar conjuntamente programas de concienciación y capacitación sobre protección ante software malicioso que minimice las vulnerabilidades de infección causadas por el factor personal.	

Tabla 51.
Hallazgo respecto a gestionar la seguridad de la red y las conexiones

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-11	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Entrega, Servicio y Soporte (DSS)
Proceso:	DSS05 Gestionar Servicios de Seguridad
Práctica:	DSS05.02 Gestionar la seguridad de la red y las conexiones
Evidencia:	AUD-FOR-TIC-001-09
Condición	
El departamento de TIC de la UCACUE utiliza medidas de seguridad como la defensa perimetral que se encuentra implementa mediante software libre Linux PFSense, además cuenta con el apoyo de un centro de respuesta a incidentes de seguridad en tecnologías de la información (CSIRT) suministrado por CEDIA (Red de Investigación de Universidades del Ecuador), el que alerta mediante mensajes de vulnerabilidades en tiempo real. Sin embargo, no cuenta con 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.	
Criterio	
Según COTIB 5 para seguridad de la información se debe utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	
Causa	
No existe un responsable formalmente designado, personal debidamente capacitado; como tampoco procedimientos y políticas de seguridad de la información implementada.	
Efecto	
La UCACUE está expuesta a cualquier tipo de incidente interno o externo que vulneren la seguridad de las redes y conexiones	
Conclusión	
Es necesario tomar las medidas que transformen las esfuerzos realizados de manera empírica en la UCACUE se implementa medidas de seguridad a la red de manera informal, puesto que, no existe políticas que definan las medidas de seguridad que se deben implementar ni los procedimientos que establezcan las actividades sus respectivos responsables.	
Recomendación.	
Al Vicerrector Administrativo • Asegurar que el Responsable de Seguridad de la Información establezca las políticas y procedimientos para la gestión de la seguridad de las redes y conexiones. **A la Directora de Tecnología de Información y Comunicaciones:** • Gestionar los recursos necesarios a fin de que se implementen mecanismos de seguridad como software de detección de intrusos, cifrado de la información en tránsito, de acuerdo a los requerimientos de seguridad de la Institución. **Al Responsable de Redes y Comunicaciones:** • Implementar las políticas y procedimientos para la gestión de la seguridad de las redes y conexiones. • Gestionar las medidas de seguridad de manera documentada y de acuerdo a las políticas y procedimientos que incluyan controles de acceso a la red. • Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	

Tabla 52.

Hallazgo respecto a gestionar la seguridad de los puestos de usuarios finales

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-002-12	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Entrega, Servicio y Soporte (DSS)
Proceso:	DSS05 Gestionar Servicios de Seguridad
Práctica:	DSS05.03 Gestionar la seguridad de los puestos de usuarios finales
Evidencia:	AUD-FOR-TIC-001-10
Condición	
En la UCACUE se realiza una configuración mínima a nivel de puestos de usuarios finales, no se han definido los niveles de seguridad de acuerdo a los requerimientos de seguridad ni existe una política de seguridad para gestión de dispositivos de usuarios finales.	
Criterio	
COBIT 5 para seguridad de la información sugiere asegurar que los puestos de usuario finales (equipos portátiles, equipos sobremesa, servidor y otros), estén asegurados a un nivel que es igual o mayor al definido en los requerimientos de Seguridad de la Información procesada, almacenada o transmitida.	
Causa	
No existe una política de seguridad para la gestión de dispositivos de usuarios finales.	
Efecto	
Alta probabilidad de ataques internos deliberados o fortuitos.	
Conclusión	
La UCACUE está expuesta a ataques internos que pueden afectar a los usuarios finales, puesto que, no se ha implementado medidas para prevenirlos.	
Recomendación.	
Al Vicerrector Administrativo: • Asegurar el cumplimiento de las funciones del Responsable de Seguridad de la Información correspondientes a gestión de la seguridad de los puestos de usuarios finales, tales como: * Establecer políticas y procedimientos para la gestión de la seguridad de los dispositivos de usuarios finales. * Establecer el modelo de arquitectura de la información de acuerdo a las necesidades del negocio. * Establecer los requerimientos de seguridad de la información y validarlos con las partes interesadas. **Al Responsable de Redes y Comunicaciones:** • Implementar las políticas y procedimientos para la gestión de la seguridad de los dispositivos de usuarios finales. • Gestionar las medidas de seguridad de manera documentada y de acuerdo a las políticas y procedimientos. • Implementar mecanismos como: bloqueo de dispositivos no identificados que accedan a la red; gestión segura de uso de medios de almacenamiento de información removibles; eliminación de dispositivos y medios de almacenamiento de manera segura; y , almacenamiento seguro de los dispositivos y medios que contienen información crítica o importante para la Institución de acuerdo a los requerimientos de seguridad de la información establecidos por el área de Seguridad de la Información cuando este funcional.	

Tabla 53.

Hallazgo respecto a gestionar la identidad del usuario y el acceso lógico

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-13	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Entrega, Servicio y Soporte (DSS)
Proceso:	DSS05 Gestionar Servicios de Seguridad
Práctica:	DSS05.04 Gestionar la identidad del usuario y el acceso lógico
Evidencia:	AUD-FOR-TIC-001-11
Condición	
Para la creación de usuarios de los sistemas de la UCACUE no se ha definido documentos formales a partir de los que se pueda realizar una adecuada gestión de la identidad de los usuarios y su acceso lógico, entregándose permisos de acceso sin definir perfiles adecuados y acordes a los requerimientos de la institución.	
Criterio	
De acuerdo a COBIT 5 para seguridad de la información se debe asegurar que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de la institución	
Causa	
No existen políticas de gestión de usuarios, no se tiene implementado el servicio de directorio activo.	
Efecto	
La confidencialidad, integridad y disponibilidad de la información están altamente comprometidos.	
Conclusión	
Al no estar definidos roles y perfiles para los usuarios no existe una adecuada administración de privilegios en los sistemas y servicios, por lo que, el acceso lógico pone en riesgo la confidencialidad, integridad y disponibilidad de la información.	
Recomendación.	
Al Vicerrector Administrativo: • Asegurar que el Responsable de Seguridad de la Información establezca las políticas y procedimientos para la gestión de identidad de los usuarios y el acceso lógico. • Asegurar el cumplimiento de las funciones del Oficial de Seguridad de la Información correspondientes a gestión de identidad de los usuarios y el acceso lógico, como: • Coordinar y establecer con los dueños de los procesos los perfiles, roles y responsabilidades de los usuarios de acuerdo a las funciones de los mismos y niveles de autoridad. • Revisar periódicamente (cada 6 meses) la gestión de los perfiles, roles y responsabilidades. • Designar el Administrador de accesos de usuarios a los servicios y sistemas quien deberá cumplir con lo siguiente: • Implementar las políticas y procedimientos para la gestión del control de acceso. • Gestionar los permisos y roles de manera documentada y en función de la política y los procedimientos, verificar la autorización correspondiente y la existencia del acuerdo de confidencialidad firmado por el usuario. • Administrar los permisos de acceso que requieran cambios, modificaciones y eliminaciones de manera documentada y con las debidas autorizaciones. • Gestionar los permisos de accesos temporales a usuarios externos mediante la firma de acuerdos de confidencialidad. • Gestionar la suspensión temporal de los accesos de los usuarios en caso de vacaciones, comisiones, licencias (permisos temporales). • Mantener un registro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones	

Tabla 54.

Hallazgo respecto a gestionar el acceso físico a los activos de TI

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-002-14	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Entrega, Servicio y Soporte (DSS)
Proceso:	DSS05 Gestionar Servicios de Seguridad
Práctica:	DSS05.05 Gestionar el acceso físico a los activos de TI
Evidencia:	AUD-FOR-TIC-001-12
Condición	
En la UCACUE no se realiza controles de acceso físico a los activos de TI a excepción de la identificación de los funcionarios de la institución.	
Criterio	
De acuerdo a COBIT 5 para seguridad de la información se debe definir e implementar procedimientos para conceder, limitar y revocar el acceso a los locales, edificios y áreas de acuerdo con las necesidades de la Institución, incluye emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado o supervisado, esto aplicará a todas las personas incluidos empleados, personal temporal, clientes, proveedores y visitantes.	
Causa	
No se ha definido una política de control de acceso físico para la protección de los activos de la organización.	
Efecto	
Los activos de TI y de la institución están completamente desprotegidos se encuentran actualmente expuestos a hurto y daño.	
Conclusión	
La UCACUE no cuenta con mecanismos de protección física que garantice la seguridad de sus activos.	
Recomendación.	
Al Vicerrector Administrativo: • Asegurar que el Responsable de Seguridad de la Información establezca las políticas y procedimientos para la gestión del control de acceso físico y gestión de activos. • Asegurar que el Responsable de Seguridad de la información identifique el entorno de seguridad de la información y los controles que deben ser implementados para proteger los activos de la organización, tales como: * Verificación de los perfiles de acceso a las ubicaciones de TI (salas de servidores) estén definidos. * Gestión adecuada de las peticiones y concesiones de acceso a las instalaciones físicas de las ubicaciones de TI. * Revisar que las peticiones formales de acceso están completadas y autorizadas. * Designación de responsable para autorizar las peticiones de acceso. * Uso de formularios que especifican las áreas a las que el individuo tiene acceso autorizado. * Acceso a las instalaciones de procesamiento de información exclusivamente a personal autorizado. * Prohibición el uso de equipos de grabación, cámaras, equipos de vídeo y audio, dispositivos móviles, etc. a menos de que estén autorizados en las ubicaciones de TI.	

Tabla 55.

Hallazgo respecto a gestionar documentos sensibles y dispositivos de salida

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-15	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Entrega, Servicio y Soporte (DSS)
Proceso:	DSS05 Gestionar Servicios de Seguridad
Práctica:	DSS05.06 Gestionar documentos sensibles y dispositivos de salida
Evidencia:	AUD-FOR-TIC-001-13
Condición	
En la UCACUE actualmente no se realiza gestión de documentación sensible y dispositivos de salida, la información se ha clasificado en función de la jerarquía de los usuarios y no de una manera formal, tampoco se gestiona el inventario de activos de TI	
Criterio	
COBIT 5 para seguridad de la información sugiere establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles tales formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (tokens) de seguridad.	
Causa	
No se ha clasificado la información sensible; no se ha establecido procedimientos para gestionar documentos sensibles y dispositivos de salida.	
Efecto	
La información está accesible a cualquier tipo de usuario en cualquier dispositivo lo que afecta a la disponibilidad, confidencialidad e integridad de la información.	
Conclusión	
La falta de clasificación de la información pone en riesgo la seguridad de la información porque no se identifica la información sensible, por tanto no se busca mecanismos para salvaguardarla.	
Recomendación.	
Al Vicerrector Administrativo: • Asegurar que el Responsable de Seguridad de la Información establezca las políticas y procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida hacia dentro y fuera de la UCACUE. • Asegurar el cumplimiento de las funciones del Oficial de Seguridad de la Información correspondientes a gestión de identidad de los usuarios y el acceso lógico, tales como: * Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basándose en el principio del menor privilegio, equilibrar riesgo y requerimientos del negocio. * Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones. * Establecer salvaguardas física apropiadas sobre formularios especiales y dispositivos sensibles. * Destruir la información sensible y proteger los dispositivos de salida (por ejemplo, desmagnetización de los soportes magnéticos, destrucción físicamente los dispositivos de memoria, colocación de trituradoras o papeleras cerradas para destruir formularios especiales y otros documentos confidenciales.	

Tabla 56.
Hallazgo con respecto a supervisar la infraestructura para detectar eventos de seguridad

UNIVERSIDAD CATÓLICA DE CUENCA	
AUD-FOR-TIC-002-16	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Entrega, Servicio y Soporte (DSS)
Proceso:	DSS05 Gestionar Servicios de Seguridad
Práctica:	DSS05.07 Supervisar la Infraestructura para detectar eventos relacionados con seguridad
Evidencia:	AUD-FOR-TIC-001-14
Condición	
En la UCACUE se supervisa la infraestructura para detectar accesos no autorizados mediante los archivos LOG de los firewall pero de manera informal, no se usan herramientas de detección de intrusos y no se realiza gestión de incidentes mediante una mesa de ayuda.	
Criterio	
De acuerdo a COBIT 5 para seguridad de la información se debe utilizar herramientas de detección de intrusos, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la gestión de incidentes.	
Causa	
La falta de una política y procedimientos formales para la supervisión de la infraestructura para detectar eventos relacionados con seguridad. No existe gestión de incidentes sobre seguridad de la información.	
Efecto	
Imposibilidad de medir la efectividad del sistema de defensa perimetral de la UCACUE por lo que el grado de confianza de seguridad de la infraestructura es indeterminado.	
Conclusión	
Al no poseer un procedimiento y las debidas herramientas para la supervisión de la infraestructura existirá únicamente respuesta reactiva a los incidentes en lugar de acciones proactivas para impedir que se den incidentes de seguridad.	
Recomendación.	
Al Vicerrector Administrativo: • Asegurar que el Responsable de Seguridad de la Información establezca las políticas y procedimientos para Supervisar la Infraestructura para detectar eventos relacionados con seguridad. • Asegurar que el Responsable de Soporte verifique que todos los eventos de seguridad de la infraestructura estén integrados con la gestión de incidentes. • Gestionar la implementación de herramientas para detección de intrusos y mesa de ayuda en ambientes libres o propietarios. **Al Responsable de Redes y Comunicaciones:** • Utilizar herramientas de detección de intrusiones. • Guardar los registros de eventos críticos de seguridad de información. • Revisar regularmente los registros de eventos para detectar incidentes potenciales. • Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocidos. • Definir y comunicar el impacto de los incidentes para permitir una respuesta acorde. • Registrar los eventos relacionados con la seguridad, reportados por las herramientas de monitorización de la seguridad de la infraestructura.	

Tabla 57.
Hallazgo respecto a supervisar el control interno

UNIVERSIDAD CATÓLICA DE CUENCA AUD-FOR-TIC-002-17	
HALLAZGOS DE LA AUDITORÍA	
Dominio:	Supervisar, Evaluar y Valorar (MEA)
Proceso:	MEA02 Supervisar, evaluar y valorar el sistema de control interno
Práctica:	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
Evidencia:	AUD-FOR-TIC-001-15
Condición	
En la UCACUE no se realiza control interno al departamento de TI como tampoco de la seguridad de la información.	
Criterio	
COBIT 5 para seguridad de la información recomienda realizar de forma continua la supervisión, estudios comparativos y la mejora del entorno de control de TI y del marco de control para alcanzar los objetivos de la institución. Revisar la operación de controles inclusive la revisión de evidencias para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Estimular a la Dirección y a los propietarios de los procesos a tomar posesión del procedimiento de mejora del control. Identificar deficiencias de control y analizar e identificar las causas raíces subyacentes. Escalar las deficiencias de control y comunicarlas a las partes interesadas.	
Causa	
El departamento de Auditoría Interna no ha implementado control interno para TI. No está definida una política de control interno de TI y el reglamento que exprese su alcance y aplicabilidad	
Efecto	
No se puede plantear y aplicar mejoras por no existir una retroalimentación de la efectividad de los controles sobre seguridad de la información.	
Conclusión	
La ausencia de controles de TI y de Seguridad de la Información hace que no se identifiquen de manera adecuada las deficiencias de TI por lo que no se implementan acciones de mejora.	
Recomendación.	
Al Vicerrector Administrativo: • Gestionar la implementación de Control Interno para TI y para Seguridad de la Información ante el Departamento de Auditoría Interna de tal manera que se identifiquen las oportunidades de mejora del área. **Al Responsable del Departamento de Auditoría Interna:** Planificar con su equipo de trabajo actividades de control como: • Realizar una revisión periódica de las políticas y procedimientos de TI y de seguridad de la información. • Medir la eficacia de los controles de seguridad de la información. • Realizar revisiones regulares de aplicaciones, sistemas y redes. • Realizar evaluaciones del aseguramiento de la información para identificar debilidades de los controles. • Revisar los informes de incidentes de seguridad de la información. • Informar y abordar las deficiencias detectadas.	

- **Informe Final de Auditoría**

Se concluye con el informe final de auditoría, en base a los hallazgos obtenidos tanto positivos como negativos. Citado informe contendrá fundamentalmente el análisis final del cumplimiento o no cumplimiento del control interno de la Seguridad de la Información.

Luego de la validación del informe preliminar, el auditor elaborará de manera oficial el informe final de auditoría, en el que constarán los hallazgos encontrados, las conclusiones y recomendaciones. Este documento es expresado de manera clara y precisa, el auditor emite su dictamen y para ello debe tomar en cuenta todas las desviaciones, analizarlas y emitir su opinión acerca de la situación del área y procesos auditados, su opinión respecto a dichos hallazgos se expresarán con total objetividad, sinceridad e imparcialidad.

De la misma manera que, en el informe preliminar de auditoría se revisa y valida con los auditados, se presentará el informe final de auditoría a la alta dirección, según las políticas de auditoría de la Institución, de existir observaciones se procederá con las modificaciones a las que diera lugar.

En resumen este documento contendrá la información lo suficientemente clara, concreta y pertinente de los resultados obtenidos después de aplicar la Auditoría al control interno sobre Seguridad de la Información, además se expondrán las respectivas recomendaciones que es otro de los puntos importantes a tomar en cuenta para mejorar el área auditada.

El informe final realizado como aplicación de la presente Guía de Auditoría en la Universidad Católica de Cuenca, se puede observar en el Anexo 1

2.2.7 Elaboración de la carta de presentación

Finalmente, se elaborará la carta de presentación de los resultados de la auditoría, esta carta irá dirigida a un alto directivo que tenga la atribución para autorizar la ejecución del cumplimiento de las recomendaciones. Esta presentación se debe realizar de manera formal. El informe final de auditoría que se entrega

conjuntamente con la carta de presentación no tendrá lugar a comentarios ni modificaciones porque constituye una entrega de carácter protocolario.

2.2.8 Carta de presentación de los resultados de auditoría aplicada

Para el caso de la Universidad Católica de Cuenca y como etapa final de la evaluación al control interno de la Seguridad de la Información se elaboró la carta de presentación dirigida al Vicerrector Administrativo a quien se notificó de los hallazgos más críticos que requieren urgente atención (ver Anexo 2).

CAPÍTULO III

3 RESULTADOS

3.1 Aprobación.

Cumplida la elaboración del informe final de la evaluación del control interno de la Seguridad de la Información, es revisado por la instancia de normatividad (Auditoria Interna de la UCACUE), para su aprobación legal y posteriormente remitirlo al ente auditado para la respuesta a las observaciones que integra el mismo, con la intención de agotar el derecho de audiencia del auditado.

3.2 Informe final de auditoría aplicado

El informe final de Auditoría se presentó por escrito y en forma verbal al Vicerrector Administrativo (alta dirección) de la Universidad Católica de Cuenca; se hicieron las respectivas aclaraciones, para que, la interpretación del informe sea adecuada a la situación tanto en los resultados como en las recomendaciones (Ver Anexo 1).

CAPÍTULO IV

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Al término de este trabajo de titulación, se ha cumplido con los objetivos planteados que han generado las siguientes 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 facilita 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 en base 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 entendimiento del marco de referencia.
- 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.

4.2 Recomendaciones

- Se recomienda que la Guía de Auditoría desarrollada sea reconocida e implementada por el área de Auditoría Interna, puesto que, de acuerdo a la revisión de los expertos permitirá al auditor interno realizar las evaluaciones periódicas necesarias para alcanzar un nivel de Seguridad de la Información aceptable para la UCACUE.
- Instaurar las prácticas de gestión y actividades específicas para Seguridad de la Información evaluadas.
- Se recomienda comprometer a los niveles directivos para el cumplimiento de las recomendaciones emitidas en el informe final de auditoría.
- Se sugiere una adecuada capacitación del marco de referencia COBIT 5 para Seguridad de la Información de tal manera que su utilización sea adecuada a la Institución en la que se requiere implementar.
- Se recomienda tomar como referencia la presente Guía para auditorías internas basadas en COBIT 5 para otras Instituciones de Educación Superior.
- Se sugiere adoptar COBIT 5 para Seguridad de la Información como margo de referencia y buenas prácticas para la empresa de acuerdo a sus necesidades, a su realidad, su campo de acción, su tamaño y a los objetivos planteados.

REFERENCIAS BIBLIOGRÁFICAS

Cano Martínez, J. J. (2014). *V Encuesta Latinoamericana de Seguridad de la Información, Informe 2014.*

Cano, J. J. (2007). *Inseguridad Informática y Computación Anti-forense.* Information Systems Control Journal.

CEDIA. (2014). *Informe de resultados de la 1° Encuesta de Seguridad de la Información en Universidades Ecuatorianas miembros de CEDIA.* Loja.

CISCO. (2014). *Informe anual de seguridad de 2014.*

CISCO. (2015). *Informe anual de seguridad de CISCO.*

Computerworld Mexico. (2012). ISACA presenta COBIT 5 para Seguridad de la Información . *PCWorld Mexico*.

Deloitte. (06 de 2013). *http://webserver2.deloitte.com.co/.* Obtenido de http://webserver2.deloitte.com.co/Consultoria%20en%20riesgo/coso/Heads%20Up%20No%20%2017%20de%202013COSOMejorasuCI.pdf

Díaz, R. C. (2012). Marco de referencia para auditorías integrales de sistemas en las mipymes colombianas. *Publicación Semestral revista Gestión y Sociedad*, 15-29.

EAFIT Universidad. (2007). COBIT : MODELO PARA AUDITORIA Y CONTROL DE SISTEMAS DE INFORMACIÓN. *Boletín 54*, 1.

Echenique, J. A. (2003). *Auditoría en Informática.* Mexico: Mcgraw-Hill.

Espinoza Cruz, M. (2009). *http://www.upt.edu.pe/upt/web/index.php.* Obtenido de http://www.upt.edu.pe/ouci/archivo/090826_II%20Charla%20sobre%20Control%20Interno%20-%202009.pdf

Galán, L. (1996). *Informática y auditoría para las ciencias empresariales.* Bucaramanga: Universidad Autónoma de Bucaramanga.

Instituto de auditores internos de España. (2013). *Control Interno - Marco Integrado.* Madrid.

ISACA - COBIT 5 para Seguridad de la Información. (2012). *COBIT 5: para Seguridad de la Información.* Estados Unidos.

ISACA. (2012). *Glossary of Terms English-Spanish.* Estados Unidos.

ISACA-COBIT 5. (2012). *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Estados Unidos.

ISO org. (20 de Agosto de 2014). *ISO 27000.* Obtenido de www.iso27000.es: http://www.iso27000.es/download/doc_iso27000_all.pdf

Kuna, H. (2006). *Tesis de Magister en Ingeniería del Software.* Obtenido de http://laboratorios.fi.uba.ar/lsi/rgm/tesistas/kuna-tesisdemagister.pdf

Microsoft - Technet. (15 de octubre de 2004). *Guía de administración de riesgos de seguridad de Microsoft*. Obtenido de Microsoft - Technet: https://www.microsoft.com/spain/technet/recursos/articulos/srsgch01.mspx

Muñoz Razo, C. (2002). *Auditoría en sistemas computacionales.* Mexico: Pearson Educación.

SNAP, Secretaría Nacional de la Administración Pública. (13 de 09 de 2013). *http://www.planificacion.gob.ec/.* Obtenido de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%B3n.pdf

Soy i Aumatell, C. (06 de Octubre de 2002). Auditar la información... ¿para qué? *Clip, boletín de la Sedic, n. 38.*, 1-3. Obtenido de http://www.sedic.es/clip38.pdf

UCACUE - PEDI. (2014). *PEDI*. CUENCA.

ANEXOS