UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

Elaboración de una Auditoria de la Gestión de Tecnologías de Información aplicable en los centros desconcentrados de soporte informático de las diferentes unidades académicas de la Universidad de Costa Rica.

Trabajo final de graduación sometido a la consideración de la Comisión del Programa de Estudios del Posgrado en Administración y Dirección de Empresas para optar al grado y título de **Maestría Profesional en Auditoría de Tecnologías de Información**

SUSTENTANTE:

Esteban Valerio Rojas

Ciudad Universitaria Rodrigo Facio, Costa Rica
Abril 2018

DEDICATORIA

A mi esposa Ana María y a mi hija Sofía, porque su amor y compañía me hacen seguir adelante cada día. Este triunfo no es solo mío, es nuestro, ya que el esfuerzo para conseguir este objetivo lo hemos realizado todos.

A mi madre Lidiette, porque me enseñó el calor del trabajo y que siempre hay que esforzarse para cumplir con los objetivos que uno se plantea.

AGRADECIMIENTOS

A todos y cada uno de los profesores y profesoras que nos acompañaron en este proceso. Considero la experiencia muy enriquecedora y dentro de un ambiente muy cordial y respetuoso, gracias por todas sus enseñanzas y consejos.

A mis compañeros y compañeras, gracias a cada uno por ser como son, por hacernos el mejor grupo de la historia de la maestría. Cada uno aportó para construir un ambiente muy bonito, eso sin duda hizo que este proceso se tornara más sencillo.

HOJA DE APROBACIÓN (Proyecto Final)

Este trabajo final de investigación aplicada fue aceptado por la Comisión de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de Información.

Magister Gino Ramírez Solís

Profesor – Coordinador

Magister Alejandro Zúñiga Gómez (Profesor UCR)

Tutor-Lector

M.Sc. Teresita Ramellini Centella

Lectora–Empresa

M.Sc. Ridiguer Artavia Barboza

Director Programa de Posgrado en Administración y Dirección de Empresas

Esteban Valerio Rojas

Sustentante

TABLA DE CONTENIDOS

RESUMEN EN ESPAÑOL

Este trabajo final de graduación surge debido a la necesidad de una auditoría de los procesos sustantivos de la gestión informática en los diferentes centros desconcentrados que existen en la Universidad de Costa Rica.

El objetivo general del trabajo es realizar una auditoría a la gestión informática en un centro desconcentrado específico, con la finalidad de fortalecer los procesos que ahí se realizan y además verificar la suficiencia de la gestión realizada y brindar recomendaciones al respecto.

También, un objetivo es generar un instrumento de evaluación que sea aplicable a otros centros desconcentrados de la misma universidad. Se conoce de antemano que existen diferencias de personal e infraestructura en cada centro, pero se trató de crear los instrumentos de una manera genérica e incluyente.

Para la generación del instrumento se realizaron entrevistas al personal administrativo de la Unidad Académica para definir cuáles procesos sustantivos serían tomados en cuenta en este trabajo. Se entrevistó a varios administradores de otros centros desconcentrados para definir los puntos más convenientes de los procesos antes definidos. Una vez generados los instrumentos, se aplicaron en la Unidad Académica seleccionada y para los datos recopilados se generaron gráficos y tablas.

Como principales resultados, cabe resaltar que la unidad académica, en cuanto a cumplimiento, no tiene grandes problemas. No obstante, se identificaron incumplimientos en algunas buenas prácticas como consecuencia de la cantidad de personas que conforman la unidad de tecnologías de información y las deficiencias en infraestructura.

RESUMEN EN OTRA LENGUA DIFERENTE AL ESPAÑOL

This final graduation work arises due to the lack and the need for an audit of the substantive processes of computer management in the different decentralized centers that exist in the University of Costa Rica.

The general objective of the work is to perform an audit of the computerized management in a specific deconcentrated center, in order to strengthen the processes and also verify the adequacy of the management and provide recommendations in this regard.

Also, one objective is to generate an evaluation instrument that is applicable to other deconcentrated centers of the same University, it is known in advance that there are staff and infrastructure differences in each center, but the instruments were created in a generic way but that cover the most complete area possible.

For the generation of the instrument, interviews were first conducted with the administration of the Academic Unit to define which substantive processes would be taken into account in this work, and several administrators of other decentralized centers were interviewed to define the most convenient points of the previously defined processes.

Once the instruments were generated, they were executed in the selected Academic Unit, and graphs and tables contained in this report were generated.

As main results, it should be noted, that the academic unit in terms of compliance does not have major problems, but the number of people that make up the information technology unit and the deficiencies in infrastructure for carrying out some processes make it lack some good practices.

LISTA DE CUADROS, TABLAS, FIGURAS E ILUSTRACIONES

ÍNDICE DE HOJAS DE TRABAJO

NOMENCLATURA

Abreviatura	Definición
TI	Tecnologías de Información
PT	Papel de trabajo
BD	Base de datos
TFG	Trabajo Final de Graduación
UCR	Universidad de Costa Rica
CGR	Contraloría General de la República
NIA	Normas Internacionales de Auditoría
RID	Recurso informático desconcentrado
CI	Centro de Informática
MATI	Maestría en Auditoría de Tecnologías de Información
PEITI	Plan Estratégico Institucional de Tecnologías de Información.

CAPITULO 1 - INTRODUCCIÓN

1.1 Objetivos

1.1.1. Objetivo general

Realizar una Auditoría de la gestión de tecnologías de información a un centro desconcentrado de soporte informático con el fin de estandarizar, mantener y perfeccionar el sistema de control interno que aplican los responsables de gestionar y supervisar este tipo de servicios.

1.1.2. Objetivos específicos

1. Comprobar la suficiencia del control interno de la unidad de soporte para mejorar, agilizar y fortalecer la gestión informática no solo de la oficina auditada sino de todos los centros desconcentrados de soporte informático de la UCR.

2. Determinar la suficiencia de la gestión evaluada y emitir recomendaciones de los aspectos sujetos a mejora encontrados mediante un Informe de Auditoría.

3. Proveer un documento de referencia a los encargados de la gestión de tecnologías de información para su utilización como herramienta de autoevaluación de sus controles internos y como guía en su labor.

1.2 Alcance del proyecto

Este trabajo de graduación tiene como principal interés, el diseñar una herramienta general que facilite la realización de evaluaciones de la gestión de las TI en las unidades académicas pertenecientes a la Universidad de Costa Rica.

Las herramientas diseñadas para efectos de este trabajo se aplicarán mediante un proceso de Auditoría de la gestión actual en la Escuela de Psicología de la Universidad de Costa Rica, de enero a marzo de 2018. Sin embargo, los alcances del diseño de estas

herramientas permitirán a los encargados autoevaluarse, apoyar el trabajo de los auditores y servirán como punto de partida para supervisiones del desempeño.

1.3 Justificación

La seguridad informática en estos años donde cada día surgen nuevas vulnerabilidades es una necesidad para cualquier institución. Para ello es necesario contar con protocolos, controles, procedimientos, normativas, directrices y manuales que permitan cumplir con los objetivos de forma satisfactoria, uno de los cuales es la continuidad de los servicios ofrecidos por la Universidad. Por lo anterior, una evaluación de la gestión informática permite tomar las acciones correctivas oportunamente, brindar un servicio seguro y confiable, así como uniformar los criterios para trabajar y estandarizar las funciones.

Además, una auditoría como la planteada es un aporte a la labor de la Comisión Institucional de Gestión Informática (CIGI), ya que coadyuva a mejorar el cumplimiento de la normativa institucional en materia de tecnologías aprobada por esta comisión. Aunado a lo anterior, los resultados pueden extrapolarse a todas las sedes adaptando las herramientas a la realidad de cada una.

1.4 Marco metodológico

1.4.1 Clasificación de la investigación

El presente trabajo, según Barrantes Echeverría (1999) es una investigación **aplicada,** ya que se aplica el conocimiento adquirido durante la maestría a un caso real en una empresa costarricense, con la finalidad de detectar aspectos sujetos a mejora en el control interno al comprar una aplicación tecnológica. El estudio realizado no pretende aportar un conocimiento teórico nuevo al campo de la Auditoría, sino abordar potenciales problemas generadores de riesgo en el tema evaluado, que en este caso es la gestión informática en una unidad desconcentrada de TI en una institución pública.

Respecto a su **alcance temporal,** es una investigación **transversal o sincrónica**, ya que se realiza en un momento dado (noviembre 2017 hasta abril 2018) y los datos o situaciones analizadas también se observaron en un único momento (abril del 2016 a diciembre del 2017).

Según su **profundidad u objeto,** se puede catalogar como **descriptiva,** ya que describe una condición encontrada, que se valora contra unos criterios normativos establecidos que rigen el tema evaluado tanto en el nivel interno como en el externo.

En su enfoque o medición, se considera **cualitativa,** ya que se describirán situaciones de la gestión informática de la institución evaluada sin cuantificar o manipular datos numéricos específicos, más que los que se observan o responden en instrumentos cualitativos. Tiene lugar en el **campo** y no en un laboratorio, con situaciones naturales y libertad de acción de los observados.

La **validez** de la investigación se evalúa con base en la evidencia recabada por el postulante durante su trabajo de campo y en el debido proceso de ejecución. La **confiabilidad** se ampara en el diseño de los instrumentos denominados como *Papeles de Trabajo*, los cuales se basan en la normativa (interna y externa), estándares, criterio experto y mejores prácticas en el campo evaluado.

1.4.2 Aproximación al marco metodológico e instrumentos por utilizar

Para iniciar con el marco metodológico se considera pertinente definir dos conceptos:

Método: Manera de ordenar una actividad, orden sistemático que se impone en la investigación y camino para llegar a cierto resultado compuesto por varias técnicas (Barrantes Echeverría, 1999).

Técnica: Conjunto de instrumentos de medición elaborados con base en los conocimientos, los cuales pueden ser de medición o de recolección de la información (Barrantes Echeverría, 1999).

Con base en estos conceptos, es importante señalar que la institución autónoma en donde se realizó el trabajo no cuenta con un método propio para realizar auditorías de TI o no se tiene acceso a ella. Así pues, considerando que el campo de la Auditoría está normado por la Contraloría General de la República en sus *Normas generales de Auditoría para Sector Público* (CGR, 2014), se tomarán estas normas como base para diseñar un método que se adecue a la auditoría de este proyecto. A continuación se describen sus etapas.

ETAPA 1: Planificación

La auditoría de la evaluación de la gestión informática, como toda auditoría, se planifica para garantizar la realización de una labor de alta calidad de un modo económico, eficiente y eficaz, de acuerdo con los principios de la buena gestión en general (COBIT 5).

Para lo anterior, se debe tener claro el objetivo, naturaleza, alcance, oportunidad y plazo para llevar a cabo el trabajo en el tiempo establecido así como los recursos requeridos. Además, en esta etapa se obtiene un conocimiento de la entidad, la comprensión del sistema de control interno relacionado con el asunto objeto de auditoría, así como la identificación de los criterios de auditoría que serán aplicados.

Con los insumos de información y conocimiento, se realiza una evaluación del riesgo que conduzca a determinar las áreas de mayor exposición en la gestión que se evalúa. Asimismo, se busca que la evaluación del riesgo permita la elaboración de un programa de ejecución de la auditoría acorde a la realidad de la organización, para que esta obtenga un valor agregado a su operación.

En la actividad de planificación se debe preparar y aprobar el programa específico que el postulante ejecuta durante la actividad de examen.

Instrumentos diseñados en esta etapa

- **Cuestionarios.** Estos se aplican al personal encargado de la gestión informática de la Escuela de Psicología, del Centro de Informática y de la CIGI, así como a usuarios u otro tipo de personal, con el objetivo de evaluar su percepción del servicio.
- **Plantillas de trabajo.** Papeles de trabajo para evaluar o describir condiciones encontradas, listas de chequeo, cuadros resúmenes de información recopilada, resultados de pruebas, hojas de recolección de hallazgos, etc.
- **Guías de entrevistas.** Estas se realizaron al personal encargado de la gestión informática en los diferentes centros desconcentrados y a cualquier otro tipo de personal.
- **Mapa o Cuadro de Riesgo.** Herramienta para mostrar gráficamente el diagnóstico del proceso de evaluación de riesgos que se identificaron en esta etapa de

planificación. Se determina mediante la probabilidad o frecuencia del impacto de los tipos de riesgo en los diferentes procesos, actividades o funciones de un negocio.

- **Programa de ejecución del trabajo.** Documento formal que se utiliza como guía metodológica en la realización del trabajo. El programa indica la descripción de actividades por desarrollar de acuerdo con un orden, una lógica y un periodo determinado.

ETAPA 2: Examen o trabajo de campo

Durante la actividad de examen se debe ejecutar el programa realizado en la etapa de planificación. Se ejecuta en forma ordenada las actividades dispuestas, lo cual conlleva a realizar pruebas, evaluar controles y recolectar la evidencia necesaria mediante la utilización de técnicas y prácticas de auditoría para determinar, justificar y presentar apropiadamente los hallazgos de auditoría, con sus atributos de criterio, condición, causa y efecto.

Se aplican todos los papeles de trabajo diseñados en la etapa de planificación y cualquier otro requerido de acuerdo con los hallazgos encontrados. Lo anterior se lleva acabo siguiendo el debido proceso tanto de la ejecución como en la recolección de evidencia. Cabe señalar que se verifica la calidad y la trazabilidad de todo el proceso, desde el programa de trabajo hasta el último papel de trabajo diseñado y aplicado.

Instrumentos aplicados en esta etapa

- **Cuestionarios.** Se aplican al personal encargado de la gestión de TI de diferentes centros desconcentrados de cómputo y a cualquier otro personal de interés.
- **Plantillas de trabajo.** Papeles de trabajo para evaluar o describir condiciones encontradas, listas de chequeo, cuadros resúmenes de información recopilada, resultados de pruebas, hojas de recolección de hallazgos, etc.
- **Guías de entrevistas.** Se llevan a cabo con el personal encargado de la gestión informática en los diferentes centros desconcentrados y con cualquier otro personal de interés.

- **Programa de ejecución del trabajo.** Se completa el programa que sirve de guía metodológica en la realización del trabajo. El programa se asocia con las pruebas aplicadas, la evidencia recopilada y los hallazgos detectados. El auditor o postulante verifica que los hallazgos de auditoría contenidos en los informes estén debidamente sustentados en evidencia suficiente, competente y pertinente, obtenida por los medios legales y técnicos aplicables.
- **Diseño y aprobación del informe borrador.** Este debe ser aprobado por el tutor y por el profesor coordinador.

ETAPA 3: Comunicación de resultados

Una vez concluido el trabajo de campo y aprobado el informe borrador, se comunica a instancias correspondientes de la institución auditada los principales resultados, las conclusiones y las recomendaciones respectivas. Esta información constituirá la base para el mejoramiento de los asuntos examinados. El informe preliminar o borrador de auditoría se elabora en un lenguaje sencillo, objetivo, conciso, claro, completo, exacto e imparcial, basado en hechos y respaldado con evidencia suficiente, competente y pertinente.

El postulante efectúa una conferencia final con la administración de la institución y con los responsables de poner en práctica las recomendaciones o disposiciones antes de emitir el informe definitivo. Este paso se ejecuta con el fin de exponer los resultados, las conclusiones y las disposiciones o recomendaciones de la auditoría, de conformidad con lo establecido en los objetivos y alcance del proyecto, que ya conocen los interesados.

El informe de auditoría contiene un resumen ejecutivo de los principales resultados obtenidos, así como de las conclusiones, disposiciones o recomendaciones emitidas.

Las recomendaciones contemplan al menos lo siguiente:

a) Generar valor a la entidad;

b) Abordan las causas del problema o condición identificada;

c) Están dirigidas al nivel responsable de solventar la deficiencia y

d) Deben ser claras, específicas, convincentes y relevantes.

Entregables en esta etapa

- **Informe definitivo.** Debe incorporar las observaciones de la administración sobre cada hallazgo, observación o recomendación.
- **Acta de reunión de comunicación de resultados.** Contiene la fecha, hora de inicio y de finalización, participantes convocados y presentes (con firma), observaciones y comentarios con nombre completo y puesto.
- **Recibido conforme de la institución.** Documento emitido por la misma persona que autorizó la realización del evento con la firma de la persona contacto (cuando fuese diferente). Este documento debe indicar el cumplimiento de lo acordado y el grado de satisfacción con el trabajo.

Todo lo anterior se apega a la norma *Calidad en la Auditoría*, en la que se establece lo siguiente:

El aseguramiento de la calidad de la auditoría es una labor que debe ejecutarse durante cada una de las actividades del proceso de auditoría, con el propósito de asegurar que los insumos, las tareas realizadas y los productos generados cumplan oportunamente con los estándares profesionales y con los requerimientos establecidos en la normativa bajo un enfoque de efectividad y mejoramiento continuo. ***(CGR, 2014)***

CAPITULO 2 - PERSPECTIVAS TEÓRICAS

2.1 Estado de la cuestión en Costa Rica.

En nuestro país se podría decir que la Auditoría de Tecnologías de Información es una profesión joven, depende de la institución y de su normativa. En el sector público, la normativa que se utiliza es la que brinda la CGR; en el sector financiero, COBIT es la regla; y en la industria privada, se puede trabajar sobre el marco de ITIL o las normativas asociadas.

2.1.1 ¿Qué es un Recurso Informático Desconcentrado?

El personal designado como administrador de recursos informáticos desconcentrados es el encargado de la gestión y monitoreo de la plataforma de acceso, herramientas de trabajo informáticas, sistemas de telecomunicaciones y la administración del hardware y el software de cada entidad institucional (unidad, centro, facultad, escuela y afines). Deberá actuar conforme a las normas de ética profesional dictadas por sus colegios profesionales, las emitidas por organismos competentes y aquellas que disponga el Centro de Informática para garantizar la buena conducta, el respeto, la integridad, la confidencialidad y la calidad profesional en los productos y servicios que brinda a los usuarios.

2.2 Historia de la empresa donde se desarrollará el proyecto

Como institución autónoma de cultura superior, la Universidad de Costa Rica está constituida por una comunidad de profesores, estudiantes y administrativos, todos dedicados a la enseñanza, la investigación y la acción social.

Los esfuerzos de la Universidad de Costa Rica se dirigen a propiciar el avance del conocimiento en su máxima expresión y responder, de manera efectiva, a las necesidades que genera el desarrollo integral de la sociedad. Esta institución ofrece excelencia en la formación de profesionales que, a su vez, actúan como difusores y agentes de cambio.

Misión

La Universidad de Costa Rica es una institución de educación superior y cultura, autónoma constitucionalmente y democrática, constituida por una comunidad de profesores y profesoras, estudiantes y personal administrativo, dedicada a la enseñanza, la investigación, la acción social, el estudio, la meditación, la creación artística y la difusión del conocimiento.

Visión

Las aspiraciones de la institución son, en primer lugar, fortalecer la excelencia académica mediante el desarrollo y el cultivo permanente de una cultura de calidad, con una articulación estrecha entre docencia, acción social e investigación y por medio de la actualización de los planes de estudio en grado y posgrado en todas sus sedes universitarias, la generación de carreras innovadoras, el mejoramiento continuo y la formación de alto nivel del personal académico y administrativo, con el fin de atender, de manera pertinente, las necesidades de la sociedad costarricense y potenciar su liderazgo en el desarrollo de la educación nacional.

En segundo lugar, potenciar la generación de conocimiento científico, tecnológico, sociocultural e innovador en todas las unidades de la Universidad y entre disciplinas, así como incorporarse a redes académicas internacionales, basadas en el reconocimiento recíproco, el respeto y los beneficios compartidos, con miras a fortalecer la cultura académica.

En tercer lugar, promover la integración, las alianzas, el compromiso social, la cooperación, la relación solidaria, la difusión del quehacer universitario y la innovación en aras de forjar nuevos espacios, con el fin de transferir e intercambiar el conocimiento generado entre la Universidad y la sociedad.

En cuarto lugar, promover la democratización del ingreso a la educación superior mediante programas que favorezcan la equidad y la inclusión social y, al mismo tiempo, impulsar iniciativas para fortalecer los servicios de apoyo a la población estudiantil, con el fin de facilitar la permanencia y la culminación exitosa de sus estudios en la Institución.

Finalmente, impulsar la internacionalidad solidaria mediante el desarrollo de redes académicas y la movilidad de docentes, estudiantes y personal administrativo, así como actualizar los mecanismos y las plataformas de la gestión universitaria velando por la sostenibilidad ambiental, el liderazgo tecnológico y la modernidad de la infraestructura física, para potenciar la pertinencia, eficiencia y rendición de cuentas.

Sobre el departamento de TI

El administrador RID se rige por la normativa, procesos técnicos, especificaciones de diseño y de desarrollo, relativos a tecnologías de la información y las comunicaciones, emitidas por el Centro de Informática. Sin embargo, los administradores RID dependen jerárquicamente de manera directa de cada una de las entidades institucionales en las cuales han sido nombrados.

Los lineamientos y marcos de trabajo que el CI desarrolla son del conocimiento y aplicación obligatoria para los administradores de recursos informáticos desconcentrados. Para ello debe cumplir con las capacitaciones y el desarrollo de conocimiento que este mismo centro determine.

Las actividades que se desarrollan en cada entidad institucional y que están relacionadas con la administración de servicios y recursos informáticos son muy diversas. Estas actividades incluyen el manejo básico de instalación de sistemas operativos y aplicaciones, la configuración de la salida externa a redes y la navegación por Web, el control de tráfico de usuarios, la asignación de cuentas y el desarrollo de aplicaciones en servidores propios de la entidad, entre otras.

La gestión de TI de la Escuela de Psicología inicia en el año 2008, con la incorporación de su propio administrador RID para cubrir las necesidades tecnológicas de dicha entidad. Cabe destacar que antes de contar con su propia gestión, dichas necesidades eran cubiertas por el equipo de informáticos del Decanato de la Facultad de Ciencias Sociales.

2.3 Normativa asociada

En el caso de la Universidad de Costa Rica, al ser una institución autónoma, se rige por la normativa brindada por la CGR. Además el CI genera estándares y procedimientos que deben seguir los administradores RID de cada unidad académica.

2.4 Estudio preliminar

Una vez realizada una visita a uno de los centros desconcentrados de gestión informática en la UCR, se determinó la necesidad de estandarizar la actividad de los encargados de dichos centros. Por ejemplo, fue posible observar la ejecución de prácticas alejadas de los mejores procedimientos para respaldo de información, donde en caso de un siniestro, la capacidad de recuperar los resultados de la actividad de las oficinas no es el óptimo.

Es por esto que se toma la decisión de realizar este estudio y poner en práctica los conocimientos adquiridos en la MATI, con el afán de mejorar la gestión en estos centros para mejorar la calidad de la gestión informática en general.

CAPÍTULO 3 - DESARROLLO

3.1 Actividades del proyecto

Tal como se planteó en la metodología, la investigación abarca tres grandes macro-etapas: Planificación, ejecución y comunicación de resultados.

A continuación, se describe cada una de ellas.

3.1.1 Etapa 1 - Planificación

Esta etapa inició con un estudio preliminar para clarificar el objetivo de este y la naturaleza de la institución. En esta etapa se pretende conocer las necesidades y el ambiente de control donde se desarrolla la auditoría. Producto de esta indagación, se determinó la oportunidad y la posibilidad real de llevar a cabo el trabajo con el alcance y en el tiempo establecido, así como los recursos requeridos.

Una vez establecida la viabilidad de cumplir con los objetivos del proyecto y de la empresa, se preparó el programa de ejecución del trabajo, para que una vez aprobado se comience a determinar las áreas de riesgo, diseñar las herramientas para poder atender de extremo a extremo todo el programa de ejecución, diseñar el mapa de riesgos, diseñar las pruebas, los cuestionarios, las guías de entrevista y todas las plantillas de trabajo para evidenciar la ejecución del mismo.

3.1.1.1 Programa de examen del proyecto

Según lo establece el ente contralor en la norma 203.03, el auditor (en este caso el postulante) debe elaborar el programa para la actividad de planificación, en el que se definan los procedimientos de auditoría que se requiere aplicar para cumplir con los objetivos correspondientes a esta actividad, así como el objetivo, naturaleza, alcance, oportunidad, plazo y responsables (CGR, 2014).

En virtud de lo anterior se describe a continuación el programa para ejecutar la evaluación de la gestión de TI.

Proceso a Auditar	Gestión Informática en los Centros Desconcentrados de TI en la Universidad de Costa Rica		
Responsable:	Esteban Valerio Rojas		
Aprobado por			
	Magister Alejandro Zúñiga G.	**Firma**	**Fecha**
	Magister Ana P. Porras Solano	**Firma**	**Fecha**
Plazo de ejecución	De enero a marzo de 2018		

1. **Objetivos de la auditoria**
   Comprobar la calidad de la gestión de TI en los centros desconcentrados de soporte informático para mejorar la ejecución de las tareas y procesos concernientes al quehacer del centro donde se va a ejecutar la auditoria.

2. **Naturaleza**

   La presente auditoría se realiza como proyecto de graduación para obtener el grado de Magister en Auditoría de Tecnologías de Información del Programa de Posgrado en Administración y dirección de Empresas de la Universidad de Costa Rica.

3. **Alcance**

   Centro Desconcentrado de Gestión Informática de la Escuela de Psicología de la Universidad de Costa Rica, etapa comprendida en los meses de enero a marzo del 2018

4. **Procedimientos de trabajo**

Procedimientos a ejecutar			
ID	Detalle	Ref. PT	Tiempo estimado
1	Identificar los procesos sustantivos de la gestión informática que se llevan a cabo en dichos centros desconcentrados, esto por medio de entrevistas dirigidas al personal clave del departamento	Enlace al papel de trabajo o evidencia	Ene 08 a Ene 21
2	Determinar por medio de dichas entrevistas, cuáles procesos son los que presentan un mayor reto o problemática para los administradores de TI de los centros desconcentrados.	Enlace al papel de trabajo o evidencia	Ene 22 a Feb 04
3	Realizar encuestas a los encargados de diferentes centros desconcentrados para conocer las prácticas de gestión de TI utilizadas en sus centros.	Enlace al papel de trabajo o evidencia	Feb 05 a Feb 25
4	Analizar las opiniones recolectas para encontrar hallazgos y realizar recomendaciones a las prácticas.	Enlace al papel de trabajo o evidencia	Feb 26 a Mar 18
5	Realizar un informe de auditoría donde se generen recomendaciones de mejora y se documenten los hallazgos encontrados.	Enlace al papel de trabajo o evidencia	Mar 19 a Abr 01

CAPÍTULO 4 - MACHOTES DEL TRABAJO

Definición de los procesos sustantivos en la gestión informática por tomar en cuenta en el estudio

Luego de realizadas las entrevistas y procesada la información recolectada mediante estas, se decidió en conjunto con la administración (en este caso la jefatura administrativa y la dirección de la unidad académica), concentrar la realización de los papeles de trabajo en cinco (5) grandes procesos o gestiones que se llevan a cabo dentro de la unidad académica. Dichos procesos son los siguientes:

Procesos sustantivos evaluados en el estudio
Política y estrategia de respaldos y recuperación de información
Gestión de usuarios de la Unidad Académica
Utilización de un criterio técnico para la realización de compras en la Unidad Académica
Política y estrategia de administración de sitio web de la Unidad Académica
Utilización de un criterio técnico para el desecho de activos de la Unidad Académica

Tabla 1. Procesos sustantivos evaluados en el estudio.

La continuación de este capítulo comprende los planes generales de auditoría para cada proceso y su correspondiente papel de trabajo desarrollado para evaluar el porcentaje de cumplimiento de la unidad académica en su gestión informática.

PLAN GENERAL DE AUDITORÍA

1-	Marco de referencia de la Auditoría Interna (NGASP 203-05-a)
1.1 Nombre auditoría: Gestión de Tecnologías de Información - Evaluar la política y estrategia de Respaldos y Recuperación de Información	
1.2 Origen: Trabajo final de graduación MATI 2018	
1.3 Instancias auditadas: Departamento de TI	
1.4 Criterios de Auditoría: Internacional COBIT 5, ITIL, Estándares de Seguridad de la Información (ISO 27000) como la ISO 27001 e ISO 27002 Nacional Ley General de Control Interno 8292, Normas Generales de Control Interno 2014. Entidad PEITI 2016-2020 Plan Estratégico Institucional en Tecnologías de Información	

2-	Viabilidad de la Auditoría: (NGASP 203-05-b)
	La viabilidad de esta auditoría se determina por tres aspectos primordiales como la disponibilidad de: -La información suficiente y apropiada para planificar la auditoría. -Cooperación del área auditada. -Tiempo y recursos necesarios. Se determina que sí es viable y permite el cumplimiento del objetivo de la auditoría.

3-	Relevancia de la Auditoría: (NGASP 203-05-c)
	La auditoría de la política y estrategia de Respaldos y Recuperación de Información tiene como principal finalidad, que se cumpla los siguientes objetivos: Integridad: garantizar que los datos que se respaldan sean los indispensables para el correcto funcionamiento de la unidad académica. Confidencialidad: asegurar que sólo los usuarios autorizados tengan acceso a los recursos con la información respaldada debido al posible almacenamiento de información sensible en dichos datos. Disponibilidad: garantizar la correcta obtención y recuperación de datos ante una eventualidad.

4-	**Objetivos: (NGASP 203-05-d)**
	Objetivo: Determinar la efectividad y eficacia de la Política y Estrategia de Respaldo y Recuperación de Información establecidos en la Unidad Académica en la que se está ejecutando el proceso.
5-	**Alcance y período objeto de examen: (NGASP 203-05-e**
	5.1 Alcance Se evaluarán la efectividad y eficacia de la Política y Estrategia de Respaldo de Información establecidos en la Unidad Académica. Se verificará el cumplimiento de dicha política, la correcta ejecución de la estrategia de respaldo, la realización de pruebas de verificación de los respaldos realizados y la generación y contenido de los informes concernientes al proceso.
	5.2 Período: Primer trimestre 2018

Hoja de Trabajo Cuestionario
Política y Estrategia de Respaldo de Información de la Unidad Académica

Elaborado por: Esteban Valerio Rojas

Revisado por: Alejandro Zúñiga Gómez

Fecha: 03-03-2018

Versión: 1.0

N°	Pregunta	Si	No	Comentario	Pond
1	**Política de Respaldo**				
1.1	¿Existe dentro del PIETI de la UCR, un apartado que se refiera puntualmente a los respaldos de información de cada unidad académica?				
1.2	¿Dicho apartado es conocido por la Dirección y Jefatura de la Unidad Académica?				
1.3	¿Dicho apartado es conocido por el personal de TI?				
1.4	¿Este documento se actualiza periódicamente?				
2	**Estrategia de Respaldo**				
2.1	¿Existe una estrategia creada por el personal de TI para satisfacer los requerimientos de la política de respaldo institucional?				
2.2	¿Se tiene un documento donde se indique cuándo (fecha) y el tipo de respaldo que se realizó?				
2.3	¿Con respecto al respaldo, se utiliza un medio físico para realizarlos?				
2.4	¿El medio o medios utilizados para los respaldos, se mantienen en un ambiente controlado para prevenir el deterioro?				

2.5	¿El medio o medios utilizados para los respaldos, se almacena en un lugar externo a la unidad académica para proteger su integridad ante un evento?				
2.6	¿El acceso a dichos medios, está restringido solamente a personal autorizado?				
2.7	¿Existe un tiempo determinado para conservar dicho respaldo?				
2.8	¿Se cuenta con automatización para realizar estos respaldos?				
2.9	¿Existe personal asignado puntualmente para realizar la ejecución y control de los respaldos?				
3	**Realización de Pruebas**				
3.1	¿Una vez realizado el respaldo, se verifica que se haya realizado correctamente?				
3.2	¿Se crea un documento con la información sobre dicha verificación?				
3.3	¿Se realizan pruebas sobre el tiempo de obtención y recuperación de información contenida en los respaldos?				
3.4	¿Se crea un documento con la información sobre dichas pruebas?				
4	**Generación de informes**				
4.1	¿Se emiten informes relativos a las actividades de respaldo?				
4.2	¿Estos informes se ponen a disposición de la Dirección y Jefatura de la Unidad Académica?				

Totales

Porcentaje de cumplimiento

Criterio	Nivel de Riesgo
De 0% a menos de 20%	Muy Alto
De 21% a menos de 40%	Alto
De 41% a menos de 60%	Medio Alto
De 61% a menos de 80%	Medio Bajo
De 81% a 100%	Bajo

PLAN GENERAL DE AUDITORÍA

1-	**Marco de referencia de la Auditoría Interna (NGASP 203-05-a)**
1.4 Nombre auditoría: Gestión de Tecnologías de Información – Gestión de Usuarios de la Unidad Académica.	
1.5 Origen: Trabajo final de graduación MATI 2018	
1.6 Instancias auditadas: Departamento de TI	
1.4 Criterios de Auditoría: Internacional COBIT 5, ITIL, Estándares de Seguridad de la Información (ISO 27000) como la ISO 27001 e ISO 27002 Nacional Ley General de Control Interno 8292, Normas Generales de Control Interno 2014. Entidad PEITI 2016-2020 Plan Estratégico Institucional en Tecnologías de Información	
2-	**Viabilidad de la Auditoría: (NGASP 203-05-b)**
	La viabilidad de esta auditoría se determina por tres aspectos primordiales como la disponibilidad de: -La información suficiente y apropiada para planificar la auditoría. -Cooperación del área auditada. -Tiempo y recursos necesarios. Se determina que sí es viable y permite el cumplimiento del objetivo de la auditoría.
3-	**Relevancia de la Auditoría: (NGASP 203-05-c)**
	La auditoría de la Gestión de Usuarios de la Unidad Académica tiene como principal finalidad, que se cumpla los siguientes objetivos: Integridad: garantizar que los usuarios tengan su correspondiente cuenta y contraseña para obtener el acceso a los equipos pertenecientes a la unidad académica, verificar que no existan cuentas duplicadas ni usuarios genéricos, además de la correcta asignación de roles para cada cuenta. Confidencialidad: asegurar que sólo los usuarios autorizados tengan acceso a los recursos con la información correspondiente a la unidad académica. Disponibilidad: garantizar el acceso a los equipos por parte de los diferentes usuarios pertenecientes a la unidad académica correspondiente.

4-	**Objetivos: (NGASP 203-05-d)**
	Objetivo: Garantizar la correcta ejecución de la Gestión de Usuarios de la Unidad Académica.
5-	**Alcance y período objeto de examen: (NGASP 203-05-e**
	5.1 Alcance Se evaluarán la efectividad y eficacia de la Gestión de Usuarios de la Unidad Académica. Se verificará el cumplimiento de dicha gestión, la correcta asignación de roles a los diferentes usuarios, y la no existencia de usuarios duplicados o genéricos.
	5.2 Período: Primer trimestre 2018

Hoja de Trabajo Cuestionario
Política y Estrategia de Gestión de Cuentas de Usuarios de la Unidad Académica

Elaborado por: Esteban Valerio Rojas

Revisado por: Alejandro Zúñiga Gómez

Fecha: 03-03-2018

Versión: 1.0

N°	Pregunta	Si	No	Comentario	Pond
1	**Política de Cuentas**				
1.1	¿Existe dentro del PETI de la UCR, un apartado que se refiera puntualmente a la gestión de cuentas de usuarios de cada unidad académica?				
1.2	¿Dicho apartado es conocido por la Dirección y Jefatura de la Unidad Académica?				
1.3	¿Dicho apartado es conocido por el personal de TI?				
1.4	¿Este documento se actualiza periódicamente?				
2	**Estrategia de Gestión**				
2.1	¿Existe una estrategia creada por el personal de TI para satisfacer los requerimientos de la política de gestión de usuarios?				
2.2	¿Existe un formulario de comunicación para realizar la creación/habilitación de una cuenta?				
2.3	¿Existe un formulario de comunicación para realizar una modificación sobre una cuenta?				
2.4	¿Existe un formulario de comunicación para realizar el borrado/cancelación de una cuenta?				

2.5	¿Sobre las contraseñas de las cuentas, existe una política con las características que deben cumplir las mismas?				
2.6	¿Está indicado si la contraseña debe tener una cantidad de caracteres específica?				
2.7	¿Está indicado si la contraseña debe tener una combinación de caracteres específica?				
2.8	¿Está indicado si la contraseña caduca y debe ser cambiada cada cierto periodo de tiempo?				
2.9	¿Sobre las cuentas de usuarios, está indicado si las cuentas caducan?				
2.10	¿Las cuentas de usuarios tienen diferentes permisos/roles?				
3	**Generación de informes**				
3.1	¿Se emiten informes relativos a las actividades de gestión de cuentas de usuarios en la Unidad Académica?				
3.2	¿Estos informes se ponen a disposición de la Dirección y Jefatura de la Unidad Académica?				

Totales

Porcentaje de cumplimiento

Criterio	Nivel de Riesgo
De 0% a menos de 20%	Muy Alto
De 21% a menos de 40%	Alto
De 41% a menos de 60%	Medio Alto
De 61% a menos de 80%	Medio Bajo
De 81% a 100%	Bajo

PLAN GENERAL DE AUDITORÍA

1-	**Marco de referencia de la Auditoría Interna (NGASP 203-05-a)**
1.7 Nombre auditoría: Gestión de Tecnologías de Información – Utilización de un criterio técnico para la realización de compras en la Unidad Académica	
1.8 Origen: Trabajo final de graduación MATI 2018	
1.9 Instancias auditadas: Departamento de TI	
1.4 Criterios de Auditoría: Internacional COBIT 5, ITIL, Estándares de Seguridad de la Información (ISO 27000) como la ISO 27001 e ISO 27002 Nacional Ley General de Control Interno 8292, Normas Generales de Control Interno 2014. Entidad PEITI 2016-2020 Plan Estratégico Institucional en Tecnologías de Información	
2-	**Viabilidad de la Auditoría: (NGASP 203-05-b)**
	La viabilidad de esta auditoría se determina por tres aspectos primordiales como la disponibilidad de: -La información suficiente y apropiada para planificar la auditoría. -Cooperación del área auditada. -Tiempo y recursos necesarios. Se determina que sí es viable y permite el cumplimiento del objetivo de la auditoría.
3-	**Relevancia de la Auditoría: (NGASP 203-05-c)**
	La revisión del uso de un criterio técnico para la realización de compras en una unidad académica tiene como principal finalidad, que se cumpla los siguientes objetivos: Integridad: garantizar que el proceso se realiza de manera confiable, que se siguen las mejores prácticas en cuanto a reputación y calidad del vendedor, y que siempre sea considerada la mejor opción para realizar la compra. Disponibilidad: garantizar la generación de informes con la correcta documentación de los datos utilizados para la realización de la compra.

4-	**Objetivos: (NGASP 203-05-d)**
	Objetivo: Garantizar la transparencia y el buen suceso del proceso de compras institucionales, asegurando el uso de buenas prácticas y una correcta gestión de compras.
5-	**Alcance y período objeto de examen: (NGASP 203-05-e**
	5.1 Alcance Se evaluará el proceso de emisión de un criterio técnico para la ejecución de una compra institucional y el uso de las buenas prácticas y recomendaciones para la gestión de compras durante este proceso.
	5.2 Período: Primer trimestre 2018

Hoja de Trabajo Cuestionario
Criterio Técnico para la realización de compras de la Unidad Académica

Elaborado por: Esteban Valerio Rojas

Revisado por: Alejandro Zúñiga Gómez

Fecha: 03-03-2018

Versión: 1.0

N°	Pregunta	Si	No	Comentario	Pond
1	**Política de Compras**				
1.1	¿Existe dentro del PETI de la UCR, un apartado que se refiera puntualmente a los compras de equipo de cada unidad académica?				
1.2	¿Dicho apartado es conocido por la Dirección y Jefatura de la Unidad Académica?				
1.3	¿Dicho apartado es conocido por el personal de TI?				
1.4	¿Este documento se actualiza periódicamente?				
2	**Estrategia de Compra**				
2.1	¿Existe una estrategia creada por el personal de TI para satisfacer los requerimientos de la política de compras institucionales?				
2.2	¿Sobre los proveedores, antes de emitir el criterio técnico, se evalúa el tiempo del proveedor en el mercado?				
2.3	¿Sobre los proveedores, antes de emitir el criterio técnico, se evalúa la capacidad de reacción ante inconvenientes por parte del proveedor?				

2.4	¿Sobre los proveedores, antes de emitir el criterio técnico, se toman en cuenta proveedores con empresas radicadas fuera del país?				
2.5	¿Sobre las compras, se pueden realizar compras en monedas que no son la oficial del país?				
2.6	¿Sobre las compras, se define claramente el plazo de entrega del producto?				
2.7	¿Sobre las compras, se define claramente el plazo de garantía del producto?				
2.8	¿Existen sanciones hacia los proveedores por atrasos en entrega de productos?				
2.9	¿Existen sanciones hacia los proveedores por atrasos en revisiones por garantía?				
3	**Generación de informes**				
3.1	¿Se emiten informes con el criterio técnico del personal de TI para la realización de compras?				
3.2	¿Estos informes se ponen a disposición de la Dirección y Jefatura de la Unidad Académica?				

Totales

Porcentaje de cumplimiento

Criterio	Nivel de Riesgo
De 0% a menos de 20%	Muy Alto
De 21% a menos de 40%	Alto
De 41% a menos de 60%	Medio Alto
De 61% a menos de 80%	Medio Bajo
De 81% a 100%	Bajo

PLAN GENERAL DE AUDITORÍA

1-	**Marco de referencia de la Auditoría Interna (NGASP 203-05-a)**
1.10 Nombre auditoría: Gestión de Tecnologías de Información – Política y Estrategia de Administración de Sitio Web de la Unidad Académica.	
1.11 Origen: Trabajo final de graduación MATI 2018	
1.12 Instancias auditadas: Departamento de TI	
1.4 Criterios de Auditoría: Internacional COBIT 5, ITIL, Estándares de Seguridad de la Información (ISO 27000) como la ISO 27001 e ISO 27002 Nacional Ley General de Control Interno 8292, Normas Generales de Control Interno 2014. Entidad PEITI 2016-2020 Plan Estratégico Institucional en Tecnologías de Información	
2-	**Viabilidad de la Auditoría: (NGASP 203-05-b)**
	La viabilidad de esta auditoría se determina por tres aspectos primordiales como la disponibilidad de: -La información suficiente y apropiada para planificar la auditoría. -Cooperación del área auditada. -Tiempo y recursos necesarios. Se determina que sí es viable y permite el cumplimiento del objetivo de la auditoría.
3-	**Relevancia de la Auditoría: (NGASP 203-05-c)**
	La auditoría de la Política y Estrategia de Administración de Sitio Web de la Unidad Académica tiene como principal finalidad, que se cumpla los siguientes objetivos: Integridad: garantizar que el acceso y la información contenida en el sitio web sean fidedigna y acorde a los principios de la unidad académica. Confidencialidad: asegurar que sólo los usuarios autorizados tengan acceso a la consola de administración del sitio web de la unidad. Disponibilidad: garantizar el acceso a los usuarios y administrados del sitio.

4-	**Objetivos: (NGASP 203-05-d)**
	Objetivo: Garantizar la correcta ejecución de la Política y Estrategia de Administración de Sitio Web de la Unidad Académica.
5-	**Alcance y período objeto de examen: (NGASP 203-05-e**
	5.1 Alcance Se evaluarán la efectividad y eficacia de la Política y Estrategia de Administración de Sitio Web de la Unidad Académica. Se verificará el cumplimiento de dicha política, la estrategia de actualización y gestión del sitio web, el control de accesos al mismo y la integridad de los datos del mismo.
	5.2 Período: Primer trimestre 2018

Hoja de Trabajo Cuestionario
Política y Estrategia de Administración de Sitio Web de la Unidad Académica

Elaborado por: Esteban Valerio Rojas

Revisado por: Alejandro Zúñiga Gómez

Fecha: 03-03-2018

Versión: 1.0

N°	Pregunta	Si	No	Comentario	Pond
1	**Política de Gestión**				
1.1	¿Existe dentro del PETI de la UCR, un apartado que se refiera puntualmente a la administración de sitios web de cada unidad académica?				
1.2	¿Dicho apartado es conocido por la Dirección y Jefatura de la Unidad Académica?				
1.3	¿Dicho apartado es conocido por el personal de TI?				
1.4	¿Este documento se actualiza periódicamente?				
2	**Estrategia de Administración**				
2.1	¿Existe una estrategia creada por el personal de TI para satisfacer los requerimientos de la política de administración de sitios web a nivel institucional?				
2.2	¿Se encuentra todo el software necesario actualizado a sus últimas versiones?				
2.3	¿Se realizan escaneos de vulnerabilidades regularmente?				
2.4	¿Se cuenta con una copia de seguridad de los datos y de todo el sitio web?				
2.5	¿Se cuenta con un servidor duplicado listo para funcionar en caso de una eventualidad?				

2.6	¿Se realizan limpiezas de datos del sitio (borrado de datos archivos, plugins, etc.) que ya no se utilicen en el mismo?				
2.7	¿Se utilizan solamente conexiones seguras para acceder a la administración del sitio?				
2.8	¿Se cuenta con una política de contraseñas robustas para acceder al sitio web?				
3	**Estrategia de Actualización**				
3.1	¿Las comunicaciones sobre la necesidad de cambios y/o actualizaciones se realizan de manera formal?				
3.2	¿Se crea un documento con la información sobre dichos cambios y/o actualizaciones?				
3.3	¿La Dirección o la Jefatura Administrativa se encargan de verificar la correctitud de dichos cambios y/o actualizaciones?				
4	**Generación de informes**				
4.1	¿Se emiten informes relativos a las actividades de administración del sitio web de la Unidad Académica?				
4.2	¿Estos informes se ponen a disposición de la Dirección y Jefatura de la Unidad Académica?				

Totales

Porcentaje de cumplimiento

Criterio	Nivel de Riesgo
De 0% a menos de 20%	Muy Alto
De 21% a menos de 40%	Alto
De 41% a menos de 60%	Medio Alto
De 61% a menos de 80%	Medio Bajo
De 81% a 100%	Bajo

PLAN GENERAL DE AUDITORÍA

1-	**Marco de referencia de la Auditoría Interna (NGASP 203-05-a)**
1.13 Nombre auditoría: Gestión de Tecnologías de Información – Utilización de un criterio técnico para el desecho de activos de la Unidad Académica.	
1.14 Origen: Trabajo final de graduación MATI 2018	
1.15 Instancias auditadas: Departamento de TI	
1.4 Criterios de Auditoría: Internacional COBIT 5, ITIL, Estándares de Seguridad de la Información (ISO 27000) como la ISO 27001 e ISO 27002 Nacional Ley General de Control Interno 8292, Normas Generales de Control Interno 2014. Entidad PEITI 2016-2020 Plan Estratégico Institucional en Tecnologías de Información	
2-	**Viabilidad de la Auditoría: (NGASP 203-05-b)**
	La viabilidad de esta auditoría se determina por tres aspectos primordiales como la disponibilidad de: - La información suficiente y apropiada para planificar la auditoría. - Cooperación del área auditada. - Tiempo y recursos necesarios. Se determina que sí es viable y permite el cumplimiento del objetivo de la auditoría.
3-	**Relevancia de la Auditoría: (NGASP 203-05-c)**
	La auditoría de la utilización de un criterio técnico para le desecho de activos de la Unidad Académica tiene como principal finalidad, que se cumpla los siguientes objetivos: Integridad: garantizar que el criterio emitido este fundamentado en informes técnicos que respalden la decisión de desechar un activo institucional. Confidencialidad: asegurar que la información contenida en los dispositivos de almacenamiento de los activos a desechar, sea correctamente respaldada y luego eliminada del mismo para evitar su utilización por usuarios ajenos a la unidad académica correspondiente. Disponibilidad: garantizar la realización de informes correspondientes al proceso de desecho, y la recuperación de datos ante una eventual necesidad de la información respaldada.

4-	**Objetivos: (NGASP 203-05-d)**
	Objetivo: Determinar la efectividad y eficacia de la utilización de un criterio técnico para el desecho de activos de la Unidad Académica.
5-	**Alcance y período objeto de examen: (NGASP 203-05-e**
	5.1 Alcance Se evaluarán la efectividad y eficacia de la utilización de un criterio técnico para le desecho de activos de la Unidad Académica. Se verificará el cumplimiento y pertinencia de dicho criterio técnico, además del aseguramiento de la información contenida en los activos a desechar.
	5.2 Período: Primer trimestre 2018

Hoja de Trabajo Cuestionario
Criterio técnico para el desecho de activos de la Unidad Académica

Elaborado por: Esteban Valerio Rojas

Revisado por: Alejandro Zúñiga Gómez

Fecha: 03-03-2018

Versión: 1.0

N°	Pregunta	Si	No	Comentario	Pond
1	**Política de desecho de activos**				
1.1	¿Existe dentro del PETI de la UCR, un apartado que se refiera puntualmente al desecho de activos de cada unidad académica?				
1.2	¿Dicho apartado es conocido por la Dirección y Jefatura de la Unidad Académica?				
1.3	¿Dicho apartado es conocido por el personal de TI?				
1.4	¿Este documento se actualiza periódicamente?				
2	**Estrategia de ejecución del desecho**				
2.1	¿Existe una estrategia creada por el personal de TI para satisfacer los requerimientos de la política de desecho de activos institucional?				
2.2	¿Se tiene un documento donde se indiquen los criterios válidos para realizar el desecho de activos?				
2.3	¿Se realiza un informe técnico con la justificación para el desecho de los activos?				
3	**Sobre la información contenida en los activos**				

3.1	¿Existe alguna política creada por el personal de TI sobre la información contenida en los activos por desechar?				
3.2	¿Se realiza un respaldo de la información contenida en los activos desechados?				
3.3	¿Se realiza un borrador de la información contenida en los activos desechados antes de la ejecución del proceso de desecho?				
4	**Generación de informes**				
4.1	¿Se emiten informes relativos a las actividades de desecho de activos?				
4.2	¿Estos informes se ponen a disposición de la Dirección y Jefatura de la Unidad Académica?				

Totales

Porcentaje de cumplimiento

Criterio	Nivel de Riesgo
De 0% a menos de 20%	Muy Alto
De 21% a menos de 40%	Alto
De 41% a menos de 60%	Medio Alto
De 61% a menos de 80%	Medio Bajo
De 81% a 100%	Bajo

CAPÍTULO 5 - ANÁLISIS DE RESULTADOS

Tabla comparativa de porcentajes de cumplimiento de cada proceso sustantivo evaluado

Una vez ejecutados los papeles de trabajo generados con las entrevistas a los otros administradores de centros desconcentrados de tecnologías de información y seleccionados los procesos sustantivos por evaluar por parte de la dirección y jefatura administrativa de la unidad académica, se obtuvieron los siguientes resultados.

Procesos sustantivos evaluados en el estudio	**Porcentaje de cumplimiento obtenido**
Respaldos y recuperación de información	37%
Gestión de usuarios de la Unidad Académica	25%
Utilización de un criterio técnico para la realización de compras en la Unidad Académica	100%
Administración de sitio web de la Unidad Académica	47%
Utilización de un criterio técnico para el desecho de activos de la Unidad Académica	92%

Tabla 2. Porcentaje de complimiento obtenido en los procesos evaluados.

Gráficos de completitud de cada uno de los procesos del estudio

Política y estrategia de respaldo de información de la Unidad Académica

Porcentaje de completitud de 37% a la fecha de realización del estudio.

Papel de trabajo realizado mediante entrevistas a otros encargados de centros desconcentrados de tecnologías de información.

Gráfico 1. Proceso sustantivo #1

Política y estrategia de gestión de cuentas de usuarios de la Unidad Académica

Porcentaje de completitud de 25% a la fecha de realización del estudio.

Papel de trabajo realizado mediante entrevistas a otros encargados de centros desconcentrados de tecnologías de información.

Gráfico 2. Proceso sustantivo #2

Criterio técnico para la realización de compras de la Unidad Académica

Porcentaje de completitud de 100% a la fecha de realización del estudio.

Papel de trabajo realizado mediante entrevistas a otros encargados de centros desconcentrados de tecnologías de información.

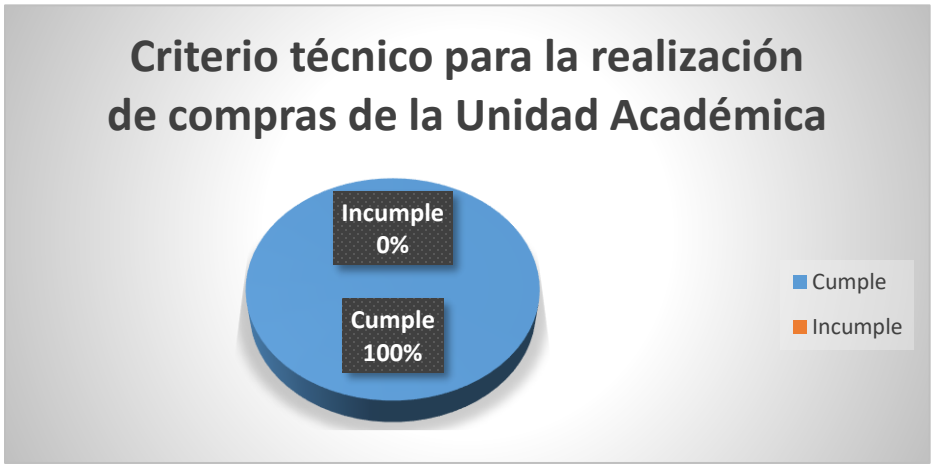

Gráfico 3. Proceso sustantivo #3

Política y estrategia de administración de sitio web de la Unidad Académica

Porcentaje de completitud de 47% a la fecha de realización del estudio.

Papel de trabajo realizado mediante entrevistas a otros encargados de centros desconcentrados de tecnologías de información.

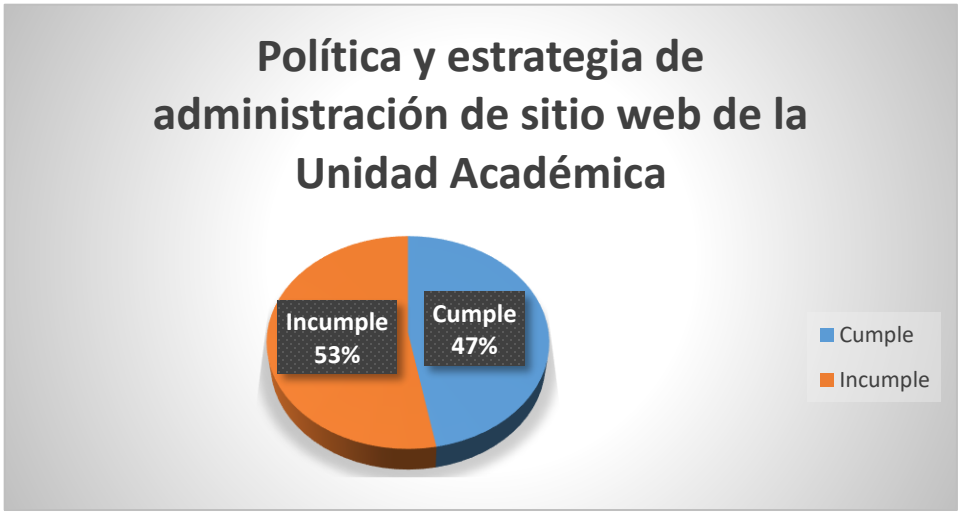

Gráfico 4. Proceso sustantivo #4

Criterio técnico para el desecho de activos de la Unidad Académica

Porcentaje de completitud de 92% a la fecha de realización del estudio.

Papel de trabajo realizado mediante entrevistas a otros encargados de centros desconcentrados de tecnologías de información.

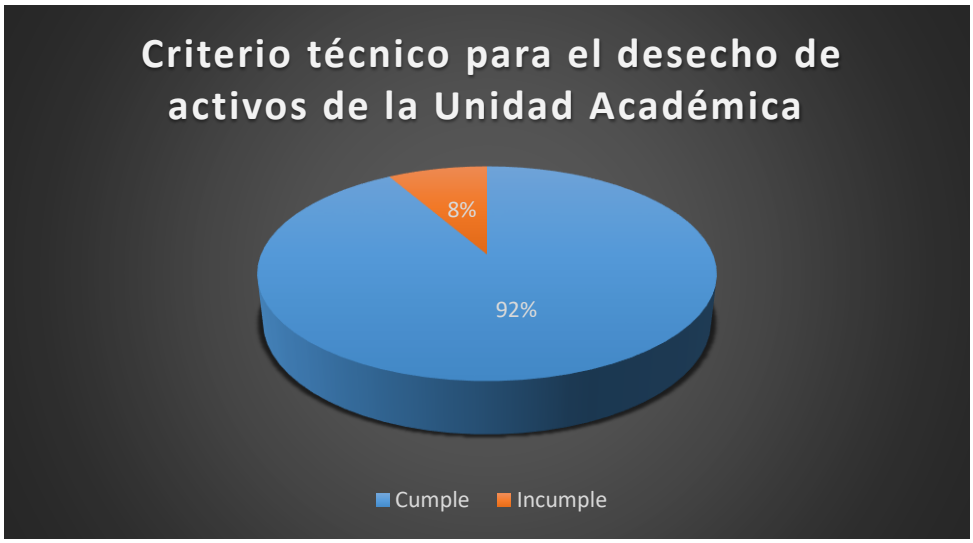

Gráfico 5. Proceso sustantivo #5

CAPÍTULO 6 - CONCLUSIONES Y RECOMENDACIONES

Como parte final de este estudio, a continuación se ofrecen una serie de conclusiones y recomendaciones basadas en los resultados obtenidos con la ejecución de los papeles de trabajo. Estas conclusiones y recomendaciones se presentan de la misma manera en que están organizados los papeles de trabajo. Cada proceso sustantivo evaluado fue desglosado en partes para su evaluación. De la misma manera se presentan las conclusiones, con uno o varios párrafos sobre cada una de las partes de los procesos, en aras de ser lo más puntual posible y que la administración pueda tomar las medidas correspondientes de una manera ordenada y enfocada en el problema o la carencia evidenciada.

6.1 Conclusiones del estudio aplicado y sus recomendaciones

Hallazgos y recomendaciones sobre la Política y estrategia de respaldo de información

Sobre la política de respaldo

La falta de un apartado que hable sobre las políticas de respaldo de información, dentro del PEITI (Plan Estratégico Institucional en Tecnologías de Información) de la Universidad de Costa Rica es una debilidad crítica encontrada durante la realización de esta auditoría. La no ejecución de este procedimiento puede afectar la continuidad de las labores cotidianas de las diferentes unidades académicas, oficinas e institutos que conforman la Universidad y se recomienda elevar este hallazgo a instancias superiores para valorar la inclusión de un apartado sobre este procedimiento en el PEITI.

Sobre la estrategia de respaldo

La estrategia creada por el personal de TI para la realización de respaldos debe ser ejecutada con más frecuencia. La posibilidad de pérdida de información importante ante una eventualidad es muy grande debido a la periodicidad con qué se realizan los respaldos. Se debe documentar el proceso de respaldo, no solamente indicar la fecha en la cual se realizó,

sino también su tamaño, las carpetas que fueron respaldadas e indicar el tipo de respaldo que se realizó.

Realizar la ejecución de los respaldos en discos duros externos no es una buena práctica, ya que no es un medio de almacenamiento tan confiable como las cintas magnéticas. Se debe procurar la implementación de un servidor de respaldos o bien realizarlos en cintas magnéticas u otro medio, Otra opción es realizar los respaldos en la nube, pero este medio conlleva otras consideraciones de seguridad importantes.

El almacenamiento de los respaldos en el mismo lugar físico donde se encuentra la información atenta contra las buenas prácticas de gestión. Se debe analizar y buscar una solución satisfactoria para esta situación, visto desde el punto donde los dispositivos usados para los respaldos están plaqueados y no pueden ser almacenados fuera de la Universidad. Se debe definir otro lugar de almacenamiento dentro de la Universidad.

Sobre la realización de pruebas

Una vez ejecutados los respaldos correspondientes se deben realizar pruebas sobre la integridad de los datos respaldados, las cuales permitan tener certeza de que se respaldó toda la información necesaria, y pruebas sobre el tiempo de obtención y recuperación de la información respaldada. Además, se deben documentar, así como sus verificaciones realizadas.

Sobre la generación de informes

Como se evidencia en los papeles de trabajo, se realiza una comunicación sobre la ejecución de los respaldos, pero se recomienda utilizar medios oficiales y con posibilidad de verificar su trazabilidad, o bien la creación de un documento con la información del proceso realizado.

Hallazgos y recomendaciones sobre la política y estrategia de gestión de cuentas de usuario de la Unidad Académica

Sobre la política de cuentas

La falta de un apartado dentro del PEITI (Plan Estratégico Institucional en Tecnologías de Información) de la Universidad de Costa Rica es una debilidad crítica encontrada durante la realización de esta auditoría. La inadecuada gestión de cuentas de usuario puede conllevar consecuencias operacionales y legales, por lo que resulta imperativo la inclusión de este apartado en el PEITI.

Sobre la estrategia de gestión

Existe una estrategia de gestión de cuentas, pero se debe mejorar la forma en la que los superiores realizan las indicaciones de trabajo, fortalecer las comunicaciones y dejar por escrito los requerimientos solicitados.

Se debe implementar una política de contraseñas, en la que su robustez, extensión y caducidad sean tomadas en cuenta para fortalecer su seguridad.

Es conveniente que exista una diferenciación entre los usuarios y que la gran mayoría no posea cuentas con permisos de administrador.

Sobre la generación de informes

Como se evidencia en los papeles de trabajo, sí se realiza una comunicación sobre la ejecución de los respaldos, pero se recomienda utilizar medios oficiales y con posibilidad de verificar su trazabilidad, o bien la creación de un documento con la información del proceso realizado.

Hallazgos y recomendaciones sobre el criterio técnico para la realización de compras de la Unidad Académica

Sobre la política de compras

Los papeles de trabajo evidencian que se cumple con lo establecido en el sistema de compras institucionales.

Sobre la estrategia de compras

Los papeles de trabajo evidencian que se cumple con lo establecido en el sistema de compras institucionales y además el personal de TI tiene conocimientos y hace uso de las buenas prácticas de gestión de compra de bienes institucionales.

Sobre la generación de informes

Si bien el personal de TI debe comunicar su criterio de manera un poco más formal a la administración, se cumple con la generación de informes concernientes a este proceso.

Hallazgos y recomendaciones sobre la política y estrategia de administración de sitio web de la Unidad Académica

Sobre la política de gestión

La falta de un apartado dentro del PEITI (Plan Estratégico Institucional en Tecnologías de Información) de la Universidad de Costa Rica es una debilidad crítica encontrada durante la realización de esta auditoría. La inadecuada gestión de administración del sitio web de la Unidad Académica puede generar desinformación, pérdida de confianza y mala reputación a esta.

Sobre la estrategia de administración

Se cuenta con una buena ejecución de la estrategia sugerida por el CI para la correcta gestión de sitios web institucionales, se actualizan los motores del sitio y se realizan las pruebas de seguridad y respaldos adecuadamente. No se cuenta con y se recomienda la utilización de un servidor duplicado para garantizar la continuidad del sitio en línea ante una eventualidad.

Además, se cumple con utilizar solamente conexiones seguras y contraseñas robustas para acceder a los módulos de gestión del sitio.

Sobre la estrategia de actualización

Existe una estrategia de gestión de actualización de contenido, pero se debe mejorar la forma en la que los superiores realizan las indicaciones de trabajo, fortalecer las comunicaciones y dejar por escrito los requerimientos solicitados.

Además, el personal de TI debe llevar una bitácora con la información de los cambios realizados en el contenido del sitio.

Sobre la generación de informes

Como se evidencia en los papeles de trabajo, sí se realiza una comunicación sobre la ejecución de actualizaciones y cambios en el contenido del sitio, pero se recomienda utilizar medios oficiales y con posibilidad de verificar su trazabilidad, o bien la creación de un documento con la información del proceso realizado.

Hallazgos y recomendaciones sobre el criterio técnico para el desecho de activos de la Unidad Académica

Sobre la política de desecho de activos

Los papeles de trabajo evidencian que se cumple con lo establecido por la reglamentación universitaria y la Oficina de Administración Financiera referente a este proceso.

Sobre la estrategia de ejecución de desecho

Existe una estrategia implementada por el personal de TI, que cumple con lo estipulado en la normativa universitaria para el correcto desecho de los equipos.

Sobre la información contenida en los activos

La política y estrategia de respaldo y borrado de información implementada por el personal de TI es acorde con las buenas prácticas para esta gestión.

Sobre la generación de informes

Se realiza correctamente tanto la ejecución del proceso de desecho de activos, así como la elaboración de los correspondientes informes técnicos sobre los equipos.

6.2 Conclusiones del proyecto realizado

El autor del estudio considera que todo el proceso de realización de este trabajo final de graduación ha sido enriquecedor y una prueba de lo aprendido durante la MATI. Los conocimientos recibidos, aprendidos y desarrollados durante el proceso de estudio fueron de vital importancia para la consecución final de este estudio.

El autor además considera que se cumplieron los objetivos planteados antes de la realización del estudio y se ejecutó todo el proceso de auditoría planteado, que incluía la fase de entrevistas y la creación de los papeles de trabajo.

Se logró el objetivo de verificar los procesos de control interno existentes en la unidad académica, de hecho, prácticamente no hay faltas en cuanto a cumplimiento. Se encuentran faltas a las mejores prácticas en la gestión, por falta de personal o falta de infraestructura y cada uno de los procesos evaluados se verán fortalecidos por el conocimiento adquirido al ejecutar los papeles de trabajo.

Por último, los papeles de trabajo, al realizarse pensando en la utilización en diferentes centros desconcentrados, será una herramienta útil y sencilla de utilizar para que otros administradores puedan llevar a cabo sus tareas de manera óptima.

7 Bibliografía

Barrantes Echeverría, Rodrigo. (1999). *Investigación. Un camino al conocimiento: Un Enfoque Cuantitativo y Cualitativo. San José, Costa Rica: EUNED.*

CGR. (2014). *Normas Generales de Auditoría para l Sector Público.* San José: Contraloría General de la República de Costa Rica.

INCIBE. (2016). *Checklist para la seguridad de tu web.* 25/01/2018, de instituto Nacional de CiberSeguridad de España Sitio web: https://www.incibe.es/protege-tu-empresa/blog/checklist-para-la-seguridad-de-tu-web

Patiño, María del Pilar. (2010) *ITIL VE3: El manual de las buenas prácticas de TI* Universidad Nacional de Colombia Sede Manizales

Universidad de Costa Rica. (2016). *Plan Estratégico Institucional en Tecnologías de Información (PEITI).* San Pedro de Montes de Oca.