TEC | Tecnológico de Costa Rica

Área Académica de Administración de Tecnologías de Información

Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho

Trabajo final de graduación para optar al grado de Licenciatura en Administración de Tecnología de Información

Elaborado por: Carlos Alberto Ramírez Cerdas

Profesor Tutor: Mario Acuña Sánchez

Cartago, Costa Rica

Noviembre, 2018

TEC | Tecnológico de Costa Rica

ÁREA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN
GRADO ACADÉMICO: LICENCIATURA

Los miembros del Tribunal Examinador del Área de Administración de Tecnologías de Información, recomendamos que el presente Informe Final del Proyecto de Graduación del estudiante Carlos Alberto Ramírez Cerdas, sea aceptado como requisito parcial para obtener el grado académico de Licenciatura en Administración de Tecnología de Información.

Lic. Mario Acuña Sánchez
Profesor tutor

Ing. Luis Chavarría Sánchez, M.Ed.
Miembro del Tribunal Examinador

José Agustín Francesa Alfaro, MSc
Miembro del Tribunal Examinador

Ing. Sonia Mora González, MBA
Coordinadora Trabajo Final de Graduación

Noviembre de 2018

Dedicatoria

Dedico este trabajo a mis padres, ya que ellos han sido mi motivo de superación durante mi vida universitaria, siempre me han apoyado y dado todo su esfuerzo para ser un mejor estudiante y una mejor persona.

Resumen

El Despacho Carvajal, mediante su departamento de Auditoría de TI (Tecnologías de Información), brinda servicios a las organizaciones relacionadas con auditorías de TI internas y externas basados en la normativa nacional vigente y en marcos de referencia como *COBIT* 5 o la ISO 27001.

Su ciclo de auditoría está alineado a estándares y normas como la ISO 19011 o el Programa de Evaluación de *COBIT 5,* no obstante, se identificó que el despacho no posee un documento formal dónde se expliquen las actividades del ciclo de auditoría además de la explicación de los procedimientos para realizar las pruebas de auditoría.

Por lo cual este trabajo final de graduación consiste en el desarrollo del manual de auditoría de TI. Está basado en las mejores prácticas y alineado con el proceso de auditoría de la ISO 19011, contiene una parte introductoria dónde se ofrece la historia y servicios brindados por el despacho, los puestos organizacionales del departamento de TI, seguidamente se explica el proceso de auditoría de TI dónde se detallan los procedimientos se definen los atributos mínimos por evaluar para cada tema abarcado, se agrega una explicación de cada tema para facilitar su comprensión.

Al finalizar el proceso de investigación realizado en el despacho, se concluye la falta de estandarización dentro de sus procedimientos abarcados en el ciclo de auditoría de TI, afectando la efectividad de los auditores de TI.

Se recomienda al departamento de TI aplicar el manual propuesto en sus auditorías de TI, además de utilizarlo como material de capacitación para sus colaboradores para así obtener los beneficios establecidos en este documento.

Palabras claves: Auditoría de TI, COBIT 5, ISO 19011, Tecnologías de información, procedimientos, ciclo de auditoría de TI.

Abstract

The Carvajal Bureau, through its Information Technology Audit department, provides services to organizations related to internal and external IT audits based on current national regulations and frameworks such as COBIT 5 or ISO 27001.

Its audit cycle is aligned with standards such as ISO 19011 or the COBIT 5 Evaluation Program, however, it was identified that the firm does not have a formal document explaining the activities of the IT audit cycle neither the explanation of the procedures to perform the audit tests.

Therefore this final graduation work consists of the development of the IT audit manual, it is based on the best practices and is aligned with the ISO 19011 audit process, it contains an introductory part that explains the story of the firm and the services it provides, the organizational structure of the IT department, then the IT audit process is explained, where the procedures are defined, the minimum attributes to be evaluated for each topic covered, and an explanation of each topic is added to facilitate your understanding.

At the end of the research process carried out in the firm, the lack of standardization within its procedures covered in the IT audit cycle is concluded, affecting the effectiveness of IT auditors.

It is recommended that the IT department applies the proposed manual in their IT audits, in addition using it as a training material for their collaborators with the purpose to obtain the benefits established in this document.

Keywords: IT audit, COBIT 5, ISO 19011, Information technologies, procedures, IT audit cycle.

Tabla de contenido

Índice de figuras

Índice de tablas

Nota Aclaratoria

Género[1]:

La actual tendencia al desdoblamiento indiscriminado del sustantivo en su forma masculina y femenina va contra el principio de economía del lenguaje y se funda en razones extralingüísticas. Por tanto, deben evitarse estas repeticiones, que generan dificultades sintácticas y de concordancia, que complican innecesariamente la redacción y lectura de los textos.

Este documento se redacta de acuerdo con las disposiciones actuales de la Real Academia Española con relación al uso del "género inclusivo". Al mismo tiempo se aclara que estamos a favor de la igualdad de derechos entre los géneros.

[1] Recuperado de: http://www.rae.es/consultas/los-ciudadanos-y-las-ciudadanas-los-ninos-y-las-ninas

Abreviaturas

Primeramente, en la Tabla 1 se procede a identificar las abreviaturas que serán utilizadas en el transcurso de este documento. Estos conceptos forman parte del entendimiento del documento por lo cual es fundamental conocerlos antes de empezar la lectura de este documento, además en caso de necesitar consultarlos, tiene la facilidad de hacerlo cuantas veces sea necesario.

Estas abreviaturas no son necesariamente acrónimos, sino que además incluyen otros términos para facilitar su lectura. En el caso de conceptos técnicos o propios del documento que necesiten una explicación de su significado se ubican en el glosario del documento, ubicado en la página 157.

Tabla 1 Abreviaturas

Término	Significado
TI	Tecnologías de información
El Despacho	Despacho Carvajal y Colegiados
COBIT	Objetivos de control para la información y tecnologías relacionadas
ISACA	Asociación de Auditoría y Control de Sistemas de Información
ITIL	Biblioteca de Infraestructura de Tecnologías de Información
TFG	Trabajo final de graduación
CGR	Contraloría General de la Republica
SUGEF	Superintendencia General de Entidades Financieras

Nota: Elaboración propia.

Capítulo I

Introducción

1. Introducción

En este capítulo se describe la información inicial al trabajo final de graduación, dónde se desarrollan los antecedentes del proyecto y se brinda una contextualización de la organización dónde se realiza el proyecto, también se menciona la problemática que originó el proyecto, así como los beneficios que se esperan al finalizar el proyecto.

Se abarca el objetivo general, así como los objetivos específicos del proyecto, además se detalla el alcance de este. Por último, se indican los supuestos, restricciones y entregables del trabajo final de graduación.

1.1 Descripción general

El presente documento tiene como objetivo exponer el desarrollo y la metodología que conforman el trabajo final de graduación “Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho”, el cual se realizó en el Despacho Carvajal y Colegiados, de ahora en adelante Despacho, específicamente en el Departamento de Auditoría y Consultoría de Tecnologías de Información. En este documento se definen los capítulos que describirán aspectos importantes para la elaboración del trabajo final de graduación.

En el primer capítulo se presenta la contextualización general de la entidad dónde se desarrolló el proyecto. Este capítulo posee los antecedentes, la situación actual, la condición que generó la necesidad de elaborar este proyecto. Igualmente, se mencionan los objetivos generales y específicos, el alcance del trabajo, entregables, los supuestos y restricciones que aplican para este trabajo final de graduación.

El capítulo dos consiste en mostrar el fundamento conceptual de los temas vinculantes para el trabajo final de graduación, dónde se detallan los conceptos necesarios para el análisis de resultados y para el desenvolvimiento de la solución planteada.

En el capítulo tres se abarca el marco metodológico, el cual se siguió para obtener los resultados del proyecto. Se desglosan las etapas del desarrollo del proyecto. Además, se incluye los elementos que componen el modelo de ejecución desde el punto de vista metodológico, enfoques, métodos, técnicas, fuentes de recopilación de datos y los instrumentos adicionales que fueron requeridos.

Seguidamente, en el capítulo cuatro, se describe el análisis de los resultados obtenidos. La formulación y confirmación de base teórica, problemática presente y el plan de implementación para impulsar la solución del problema.

En el capítulo cinco se encuentra el abordaje de la solución propuesta, posteriormente, se finaliza con los capítulos seis y siete, los cuales contienen las conclusiones y recomendaciones respectivamente.

El proyecto tiene como base principal COBIT 5, la cual es una metodología creada por el Instituto de control de Tecnologías de Información y la Asociación de Auditoría y Control de Sistemas de Información, esta metodología es usada para evaluar el departamento de tecnologías de información en las organizaciones (ISACA, 2012).

1.2 Antecedentes

En este apartado se describe la organización dónde se realizó el trabajo final de graduación. El equipo de trabajo involucrado, sus responsabilidades y los proyectos similares realizados dentro o fuera de la organización los cuales sirvieron de insumo para consultar como fuentes de información (Despacho Carvajal, 2018).

1.2.1 Descripción de la organización

El Despacho Carvajal y Colegiados Contadores Públicos Autorizados, S.A. es una firma de auditoría y consultoría del área financiera y de tecnologías de información, inició actividades a partir de enero de 1975.

La Firma fue fundada por el Lic. José Antonio Carvajal Arias, quien trabajó para consolidarla como una de las principales Firmas de auditoría y consultoría del país, que atendiera a todos los sectores económicos. Con el paso de los años, la Firma creció a un ritmo acelerado, por lo que se incorporan, en el año 1999, el Lic. Gerardo Montero Martínez y en el año 2005 el Lic. Ricardo Montenegro Guillén, como socios de la Firma, con el propósito de especializar y diversificar los servicios y consolidar el sistema de control de calidad sobre los servicios realizados. Ambos profesionales ya mantenían una trayectoria importante dentro de la Firma (Despacho Carvajal, 2018).

1.2.1.1 Misión

A continuación, se presenta la misión del despacho:

“Somos una firma con presencia local e internacional, dedicada a la prestación de servicios de auditoría y consultoría, orientados a brindar soluciones integrales mediante nuestro conocimiento y capital humano, a clientes del sector privado y público”.

1.2.1.2 Visión

Seguidamente, se presenta la visión:

"Ser una firma reconocida en servicios de auditoría y consultoría, con estándares de control de calidad, actualización profesional y herramientas tecnológicas flexibles a los cambios dinámicos del entorno económico, que nos distingan y proporcionen valor agregado a nuestros clientes".

1.2.1.3 Sobre la organización

El Despacho cuenta con membresías las cuales les permite brindar los servicios indicados más adelante (Despacho Carvajal, 2018).

1.2.1.3.1 Membresías

La empresa se encuentra al día de hoy inscrita y activa en el Registro de Auditores Elegibles que forma parte del Registro Nacional de Valores e Intermediarios, dispuesto en la Ley Reguladora del Mercado de Valores, cumpliendo con lo establecido en el Reglamento de Auditores Externos y Medidas de Gobierno Corporativo aplicable a los sujetos fiscalizados por la Superintendencia General de Entidades Financieras (SUGEF), la Superintendencia General de Valores (SUGEVAL), la Superintendencia de Pensiones (SUPEN) y la Superintendencia General de Seguros (SUGESE), en el Colegio Profesionales de Ciencias Económicas y el Colegio de Contadores Públicos de Costa Rica.

1.2.1.3.2 Dirección del negocio

El Despacho se describe como una firma que ofrece servicios al sector económico y al de TI, tanto para empresas públicas y privadas, se detallará más adelante, no obstante, el equipo de trabajo se adapta a la situación presentada por el cliente, con el fin satisfacer sus necesidades. Dentro de los servicios que ofrecen, se encuentran:

- **Auditoría:**
    - Auditoría presupuestaria: A través de esta auditoría, se emite una opinión objetiva sobre el nivel de observancia de las políticas y metodologías internas establecidas principalmente en el sector público, así como con

el cumplimiento de la normativa técnica y jurídica aplicable promulgado en las Normas Técnicas sobre Presupuesto Público (N-1-2012-DC-DFOE).

- Auditoría forense: Se enfoca en investigar, determinar y cuantificar, por medio de técnicas de auditoría, si han existido fraudes y delitos perpetrados en el desarrollo de las funciones públicas y privadas de funcionarios u otros, en contra del patrimonio de una entidad. El trabajo permite investigar, analizar, interpretar y recopilar información financiera contable y, con base en ello, presentar evidencia ante las autoridades judiciales o determinar la viabilidad de establecer demandas en contra de los perpetradores del fraude.
- Auditoría operativa: Se analiza y se presenta un resultado acerca de aspectos administrativos, estratégicos y operativos de los entes auditados, con lo que se mide la efectividad, eficiencia y economía con los cuales se realizan las actividades en la empresa. Se cuenta con servicios de auditoría operativa integral para toda la organización, departamentos o bien procedimientos específicos, que se llevan a cabo; se evalúan sus controles y desempeño.
- Auditoría Interna u Outsourcing: Se ha diseñado una Unidad de Auditoría Interna, especializada en la prestación de un servicio acorde a las necesidades del cliente. La auditoría interna es una actividad independiente, objetiva y asesora, por medio de la cual se le da seguridad a la empresa para validar y mejorar sus operaciones. El enfoque de auditoría se basa en el cumplimiento de los siguientes objetivos:
    - Evaluar la eficiencia eficacia con que se realizan las operaciones en la empresa.
    - Verificar la confiabilidad de la información que se genera.
    - Verificar el cumplimiento de las operaciones.
    - Velar por la protección del patrimonio de los accionistas.
    - Dar seguimiento del cumplimiento de las operaciones.

- Auditoría externa financiera: Para la realización de la auditoría y maximización del tiempo, se cuenta con sistemas informáticos diseñados para la ejecución de nuestro servicio como el SPT Audit y el ACL.
- Auditoría de TI: comprende la evaluación de las Tecnologías de Información, así como de la Seguridad de la Información, dentro de una organización.

  Está basada en buenas prácticas y normas nacionales e internacionales, que son utilizadas para revisar y calificar el diseño, desempeño y cumplimiento de los controles implementados en el ambiente de TI.

  Permite contar con una evaluación objetiva e independiente respecto a los procesos, servicios, aplicaciones, infraestructura e información, identificando los principales riesgos de negocio relacionados con TI, resultado de posibles debilidades de control.

Además de emitir un dictamen de la información financiera auditada, se suministra una carta de gerencia, con información del trabajo realizado y las oportunidades de mejora detectadas a nivel de control interno y riesgos de control, las cuales representan un valor agregado del servicio.

- **Consultoría:**
  - Consultoría de TI: Brinda servicios de consultoría según las necesidades del cliente, poniendo a disposición de la organización un equipo de trabajo capacitado para atender la situación presentada.

1.2.1.3.3 Clientes y sectores

La firma brinda servicios a diversos perfiles de clientes en todos los sectores productivos a nivel local e internacional entre los cuales se destacan los siguientes:

- Sector gobierno y entidades autónomas del Estado.
- Sector financiero: Bancario y Cooperativo, Pensiones, Seguros, Valores.
- Sector comercial, industrial y servicios.
- Sector solidarista.

1.2.1.3.4 Propuesta de valor

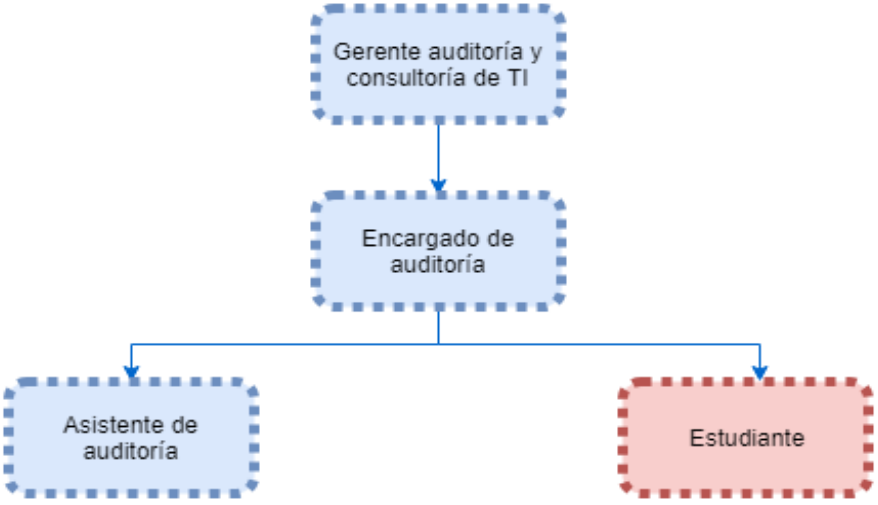
La organización se basa en el conocimiento y la experiencia para desarrollar trabajos de calidad, para lo cual dan cinco razones de peso para convertirse en una excelente opción de servicios (Despacho Carvajal, 2018).

- Experiencia y trayectoria.
- Actualización profesional.
- Atención personal y oportuna.
- Respaldo de la firma internacional.
- Recursos tecnológicos.

1.2.1.4 Equipo de trabajo

En esta sección se menciona el equipo de trabajo involucrado en el proyecto que se pretende desarrollar, primero se verá el organigrama del equipo de trabajo en la Figura 1.1 y seguidamente se mencionará su rol dentro del proyecto y como aportaría al mismo en la Tabla 1.1.

Figura 1.1 Equipo de trabajo



Fuente: Elaboración propia.

1.2.1.4.1 Roles y responsabilidades

A continuación, se procede a identificar en la Tabla 1.1 las responsabilidades del equipo dentro del trabajo final de graduación.

Tabla 1.1 Roles y responsabilidades del equipo de trabajo

Rol	Responsabilidades
Desarrollador del proyecto.	Responsable de procesar la información obtenida de los procesos actuales y analizarla con los procesos de las mejores prácticas para proponer y documentar procesos optimizados y estandarizados.
Asistente de auditoría.	Será la fuente principal para conocer los problemas y dificultades a la hora de realizar las pruebas de auditoría.
Encargado de auditoría.	En primera instancia, será el encargado de verificar y proponer cambios a los procesos establecidos por el estudiante, además apoyará al estudiante con su experiencia profesional.
Gerente de auditoría y consultoría de TI.	Es el responsable de aprobar los procedimientos establecidos por el estudiante, tendrá asimismo la responsabilidad de asesorar y hacer seguimiento del trabajo realizado por el estudiante.

Nota: Elaboración propia con base en Despacho Carvajal (2018).

1.2.2 Trabajos similares realizados fuera de la organización

Anterior a este proyecto, se han identificado tres trabajos similares que sirven de insumos y apoyo para el desarrollo de este proyecto. Se detallan en las siguientes tablas: Tabla 1.2, Tabla 1.3, Tabla 1.4 para su mejor entendimiento.

Tabla 1.2 Proyecto similar #1

Propuesta de definición de controles de auditoría y pruebas sustantivas para la evaluación del proceso de Gestión del Cambio en las organizaciones auditadas, Caso JM Auditores.	
Realizado por:	Descripción del documento:
Adán Josué Masis Álvarez	Establecer controles de auditoría específicos para llevar a cabo evaluaciones sobre la Gestión de Tecnología de Información en las organizaciones auditadas, implica la definición de pruebas sustantivas que respaldan y evalúen cada uno de los escenarios que se pueden presentar en las diferentes empresas. El proyecto se basa en la definición de controles de auditoría y pruebas sustantivas para la evaluación del proceso de Gestión del Cambio en las empresas del mercado industrial, dónde por medio de una rúbrica de evaluación se analizaron las metodologías: *ITIL* v2011, *COBIT 5* y la norma ISO/IEC 20000, con el fin de determinar cuál de estas se adapta mejor a las auditorías realizadas por JM Auditores. Como resultado del proyecto, se definieron los controles de auditoría para el proceso de Gestión del Cambio y las pruebas sustantivas de cada uno de los controles establecidos por medio de *COBIT* 5, las cuales fueron seleccionadas como parte del análisis realizado.

Nota: Adaptado de Álvarez (2017).

Tabla 1.3 Proyecto similar #2

Guía de la auditoría de Tecnologías de Información	
Realizado por:	Descripción del documento:
Auditoría Superior del Estado de Chihuahua	La presente guía está dirigida a los auditores de la Auditoría Superior que realicen funciones de auditoría de tecnologías de información a los diferentes entes públicos de la administración central, descentralizada ya sea estatal y municipal, autónomos, fideicomisos y personas físicas o morales que manejen, recauden o administren recursos públicos. Además, el desarrollo de los procesos generales establecidos en la presente guía es de aplicación general y flexible de acuerdo con la naturaleza del ente.

Nota: Adaptado de Auditoría Superior del Estado de Chihuahua (2013).

Tabla 1.4 Proyecto similar #3

Manual de Auditoría de Gestión a las Tecnologías de Información y Comunicaciones	
Realizado por:	Descripción del documento:
Corte de cuentas de la república. El salvador, c.a.	El presente manual de auditoría de gestión a las tecnologías de información y comunicaciones describe procedimientos que los auditores deben utilizar para verificar el uso de los recursos tecnológicos, confidencialidad, confiabilidad, integridad, disponibilidad de la información procesada por los sistemas de información automatizados y apoyo en la automatización de los procesos operativos y administrativos de la entidad para llegar a medir los indicadores de gestión de eficiencia, efectividad y economía de las tecnologías de información y comunicaciones implementadas por la institución y presentar conclusiones y recomendaciones oportunas y acertadas que sirvan de guía para corregir las deficiencias que pueden llegar a existir y lograr mejorarlas.

Nota: Adaptado de Corte de Cuentas de la República (2011).

1.3 Planeamiento del problema

En esta sección se describe la situación problemática encontrada dentro del entorno de la organización, la cual motiva el desarrollo del proyecto, así como la mención de los beneficios esperados del producto por desarrollar.

1.3.1 Situación problemática

La problemática que se desea resolver con la realización de este manual está enfocada en el proceso de capacitación de los colaboradores en el Despacho, específicamente los auditores de tecnologías de información. Se observó por medio de una reunión que el proceso actual de capacitación no está definido como tal, no se tiene un material propio del Despacho por lo cual se tiende a apoyarse en libros, presentaciones y documentos creados por otros autores. (M. Gutiérrez, comunicación personal, 27 de abril, 2018).

El primer día laboral al colaborador se le imparte una capacitación general de la organización, dónde se le brinda un documento con las políticas del Despacho, por ejemplo, vestimenta, viáticos, entre otros. Este proceso dura aproximadamente cuatro horas.

Seguidamente, empieza el proceso de capacitación para el área de auditoría de tecnologías de información, lo más común es que al colaborador todavía no se le ha entregado su computadora personal, por lo tanto, el material que se le brinda es impreso, entre los cuales se incluye:

- *COBIT* 5.
- Normas técnicas para la gestión y el control de las Tecnologías de Información de la CGR.
- SUGEF 14-17 Reglamento general de gestión de la tecnología de información.
- Presentaciones de apoyo de otros autores.

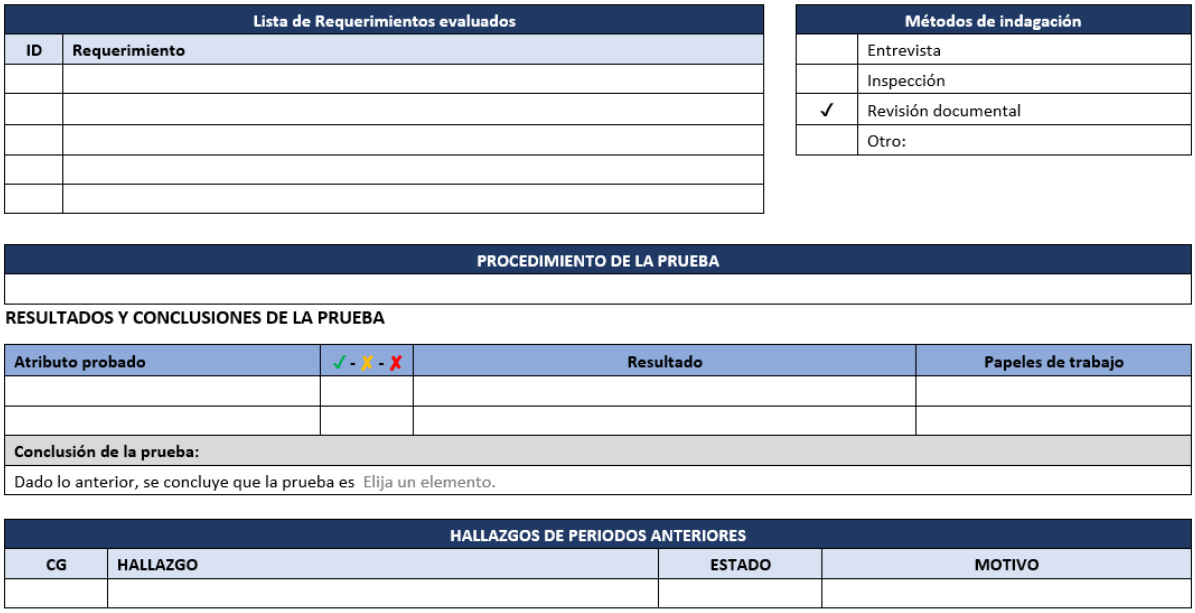
Cuando se le entregan estos documentos, la instrucción girada a los colaboradores, es que lean el material y procedan a realizar un resumen, esquema de ideas, o subrayar lo que consideren más importante, por lo cual se puede decir que se enfrenta a una situación de autoaprendizaje, pero sin una guía a seguir, solo las instrucciones del gerente o la asistente administrativa.

Para el segundo día de ser posible se le asignará un encargado, en caso contrario deberá seguir en las oficinas centrales estudiando el material brindado, por lo cual procede a seguir en la misma situación de autoaprendizaje, una vez que se le asigna un encargado procederá a desplazarse al lugar del cliente de la auditoría. Una vez asignado un encargado, de él dependerá la manera de enseñarle a realizar las pruebas, esto significa que, si hay tres encargados, podría conocer tres formas distintas de aprender y realizar las pruebas, esto no quiere decir que este malo, pero si puede causar confusión en una persona que está dando sus primeros pasos en el ambiente laboral.

El proceso inicial se puede tornar lento, esto porque dependerá de la carga laboral del encargado en el momento, un escenario posible y el más probable es tener muchas actividades por realizar, entonces el tiempo que le dedicará al asistente será mínimo, empezará asignándole una prueba de auditoría, para esto le indicará que se debe llenar una plantilla para realizar la prueba, esta será la primera vez que observe la plantilla, ya que, como se mencionó anteriormente, la primera fase de la capacitación consiste en lecturas de las fuentes externas de información.

El encargado procederá a explicarle la plantilla, se puede observar un extracto en la Figura 1.2 y se puede ver la plantilla completa en el Anexo 1: Plantilla actual de pruebas, la cual es utilizada para la realización de la prueba en clientes dónde se toma como referencia las Normas técnicas o COBIT 5, esta explicación se puede extender aproximadamente por dos horas, dependiendo de la prueba que el encargado haya seleccionado para la explicación.

Figura 1.2 Fragmento de la plantilla de prueba



Lista de Requerimientos evaluados	
ID	Requerimiento

Métodos de indagación	
	Entrevista
	Inspección
✓	Revisión documental
	Otro:

PROCEDIMIENTO DE LA PRUEBA

RESULTADOS Y CONCLUSIONES DE LA PRUEBA

Atributo probado	✓ - X - ✗	Resultado	Papeles de trabajo
Conclusión de la prueba:			
Dado lo anterior, se concluye que la prueba es Elija un elemento.			

HALLAZGOS DE PERIODOS ANTERIORES			
CG	HALLAZGO	ESTADO	MOTIVO

Fuente: Despacho Carvajal y Colegiados.

El encargado volverá a sus labores ordinarias y el asistente procederá a realizar la prueba, para esto deberá repasar las fuentes que leyó anteriormente; es importante mencionar que cada prueba tiene su dificultad y eso repercutirá directamente en el tiempo de investigación y desarrollo, pues uno de los mayores retos a la hora de realizar una auditoría es analizar la información de las buenas prácticas y adaptarla a la realidad del cliente, de tal manera que cuando se realicen las recomendaciones en los hallazgos, estas sean alcanzables en un corto tiempo por el cliente.

El asistente deberá definir los atributos a evaluar, contemplando los atributos generales, los cuales fueron incluidos en la explicación de la plantilla por parte del encargado.

- Existencia.
- Aprobación.
- Estructura.
- Cumplimiento.

Estos atributos aplican para la mayoría las pruebas, no obstante, se deben revisar otros atributos, como por ejemplo en la prueba del Plan estratégico de TI (PETI), se analiza los siguientes atributos.

- Existencia de un Plan Estratégico Institucional. (PEI)
- Existencia de un Plan Estratégico de Tecnologías de Información. (PETI)
- Estructura adecuada del Plan Estratégico de Tecnologías de Información.
- Cumplimiento Plan Estratégico de Tecnologías de Información.
- Seguimiento del Plan Estratégico de Tecnologías de Información.
- Estructura adecuada del Plan Anual Operativo. (POI)
- Seguimiento del Plan Anual Operativo.
- Alineación POI-PETI-PEI.

De los atributos esenciales, el más difícil de asimilar es la estructura del documento a revisar, ya que puede ser tan detallada como la fuente consultada o por el contrario incluir los atributos que el asistente considere necesarios, pero cómo definirlo, si no tiene experiencia en el campo.

Como se puede observar en la lista anterior se abarcan los atributos esenciales, además de varios atributos propios de la prueba como el seguimiento y la alineación de los debidos documentos involucrados, el proceso de análisis para obtener los resultados de la prueba también dependerá de la explicación del encargado, en este caso la explicación se puede extender hasta cuatro horas, dependiendo del detalle y aun así se pueden dejar elementos valiosos por fuera.

Ya el asistente comprendió la explicación y procederá a realizar la prueba, resulta que tiene varias dudas sobre como completar la plantilla, aquí hay varios escenarios, empezará a investigar sus dudas en fuentes externas, por temor a preguntar o porque el encargado no se encuentra, en caso de ser los atributos, podría pasar más de un día laboral y aun así no comprender como realizar el estudio, ya que cuando se decide a realizar la prueba y enviarla para su revisión, el encargado deberá dedicar parte de su tiempo a hacer las correcciones pertinentes.

Esta situación se repetirá cada vez que el asistente realice una prueba por primera vez, o dónde el enfoque por el cliente de la auditoría sea diferente. Al final lograr que una prueba de un asistente recién ingresado reciba la aprobación puede extenderse por más de una semana.

Aproximadamente, las auditorías más comunes en el Despacho están compuestas por 20 pruebas, por lo cual para lograr que el asistente domine estas pruebas podría extenderse por tres meses, debido a que él deberá realizar una extensa investigación sin tener en claro cuál es el procedimiento por seguir.

Aparte de realizar la plantilla anterior, también debe redactar hallazgos, para lo cual debe aplicar su análisis realizado en la prueba, de tal manera, que esté relacionado con el cliente de la auditoría. Las partes del hallazgo son las siguientes.

- Nombre del hallazgo.
- Condición: Situación actual.
    - Causa: Razón del hallazgo.
    - Efecto: Riesgos que se podrían materializar por la causa.
- Criterio: Normativa externa o interna, *COBIT 5* u otro criterio que deba o desea cumplir el cliente.
- Recomendaciones: Se brindan acciones que lograrán subsanar la condición actual, de acuerdo con las necesidades del cliente.

Además, debe aprender a realizar otro tipo de pruebas y plantillas.

Seguridad Física.

- Matriz de riesgo.
- Prueba sistemas de información.
- Matriz de seguimiento.

El procedimiento de aprendizaje tanto para los hallazgos como las otras pruebas es igual al explicado al inicio de este apartado, el encargado debe destinar tiempo para enseñarle al asistente cada una de las pruebas y plantillas mencionadas.

Otro punto importante de mencionar es el siguiente, los estudiantes reciben una educación integral en las universidades, pero con el pasar del tiempo hay conceptos que se van dejando en el olvido, o se conoce su definición, pero no como aplicarlo en el ambiente laboral y, por ende, menos como evaluarlo en las organizaciones, además no se maneja un mismo nivel de educación en todas las universidades por lo que el conocimiento entre un asistente y otro puede variar.

Por lo que, si hay un asistente que tiene debilidades de conocimiento en alguno de los 23 procesos operacionales de *ITIL* o los 37 procesos de *COBIT*, que son la base teórica de los temas abarcados en las auditorías, él deberá estudiar y comprender el proceso en estudio, aparte de entender el procedimiento de la prueba. Aquí se presentan dos situaciones, *COBIT* menciona las actividades que debería tener el proceso, pero no como entender sus actividades, y por otro punto *ITIL* se compone de cinco fases o libros, además de estar en inglés, por lo que un asistente que desconoce estas dos fuentes le será muy difícil aprender en un corto tiempo sin una guía a seguir.

Al final se dura aproximadamente tres meses conociendo la mayoría de las pruebas y herramientas que se utilizan en el Despacho, por parte del asistente, y de aquí en adelante él deberá preguntar todas sus dudas referentes al ciclo de auditoría del Despacho a un encargado o gerente, pues hasta el momento no se cuenta con un documento que incluya estos aspectos.

1.3.2 Beneficios esperados o aportes del proyecto

Con la elaboración del manual en este proyecto se pretende agilizar el proceso de aprendizaje de los colabores en el área de auditoría y consultoría de tecnologías de información. En la siguiente página se mencionan los beneficios esperados producto de su aplicación.

1.3.2.1 Estandarización del conocimiento

Al desarrollar el manual y aplicarlo, se garantiza una estandarización de conocimientos, tanto en el área técnica, como en entender el ciclo de auditoría del Despacho, comprendiendo cada una de las fases.

Se logra el aprendizaje autodidáctico pero guiado y enfocado, ya que el manual guiará al lector sobre los procesos que se realizan en las pruebas según el requerimiento a evaluar y la herramienta utilizada, permitiendo que se enfoque en lo esencial y una vez comprendido esto, puede complementar sus conocimientos con las fuentes bibliográficas establecidas en el mismo manual.

Se reducirá el tiempo de aprendizaje para alcanzar el nivel mínimo de conocimiento necesario en su puesto laboral.

1.3.2.2 Aplicación de las pruebas de auditoría eficaz y eficientemente

Con el estudio del manual por parte del colaborador, se va a reducir el tiempo de realización de las pruebas. Aumentando la eficiencia y productividad en las tareas asignadas. En este caso se espera que el asistente realice consultas sobre cómo aplicar los conocimientos aprendidos a la situación del cliente y eliminar las dudas referentes al entendimiento técnico de la prueba.

1.3.2.3 Recomendaciones enfocadas a la situación del cliente y alcanzables

El manual dentro del proceso de las pruebas va a sugerir una serie de atributos por prueba con su debida explicación, entonces al realizar un estudio más preciso, se podrán realizar recomendaciones más enfocadas a la situación del cliente, y muy importante que sean alcanzables, de lo contrario la auditoría no brindaría valor al cliente.

1.3.2.4 Tiempo efectivo del equipo de trabajo.

Aquí se hace mención en que se enfocará el asistente para comprender la situación del cliente, y no a entender la teoría de las pruebas a realizar, por otro lado, el encargado se dedicará a resolver consultas precisas y no a dar explicaciones extensas de un tema en particular. Permitiéndole concentrase más en sus actividades diarias.

1.4 Objetivos del proyecto

Se procede a definir los objetivos que se desean alcanzar con la realización de este proyecto.

1.4.1 Objetivo general

El objetivo general del proyecto consiste en:

Elaborar un manual de auditoría de tecnologías de información, en un período de 16 semanas, enfocado en el ciclo de auditoría de TI del Despacho, para utilizarlo como material de capacitación en los colaboradores del departamento de TI, logrando un nivel estandarizado de conocimientos técnicos que les permita desarrollarse exitosamente en sus actividades laborales, reduciendo el tiempo de aprendizaje de temas desconocidos o con bases técnicas insuficientes, tomando como referencia las mejores prácticas de la industria para TI.

1.4.2 Objetivos específicos

Los objetivos específicos del proyecto son los siguientes:

- Analizar el proceso actual de capacitación en el departamento de auditoría y consultoría de TI del Despacho, para tomarlo como la base del proyecto.
- Comparar el ciclo de auditoría de TI, especialmente los procedimientos actuales de las pruebas de auditoría con las mejores prácticas de la industria como lo es *COBIT* 5 o *ITIL*, para contrastarlos entre ambos, proponiendo recomendaciones a los procesos actuales producto del análisis efectuado.
- Confeccionar los procedimientos de aplicación de las pruebas de auditoría de TI, para aplicarlos en los clientes del Despacho, además de servir de apoyo en el proceso de conocimiento y aprendizaje de los colaboradores.
- Integrar los procedimientos creados con la explicación de cada una de las fases del ciclo de auditoría de TI en un manual de auditoría de TI, para el estudio y aplicación en su labor diaria.

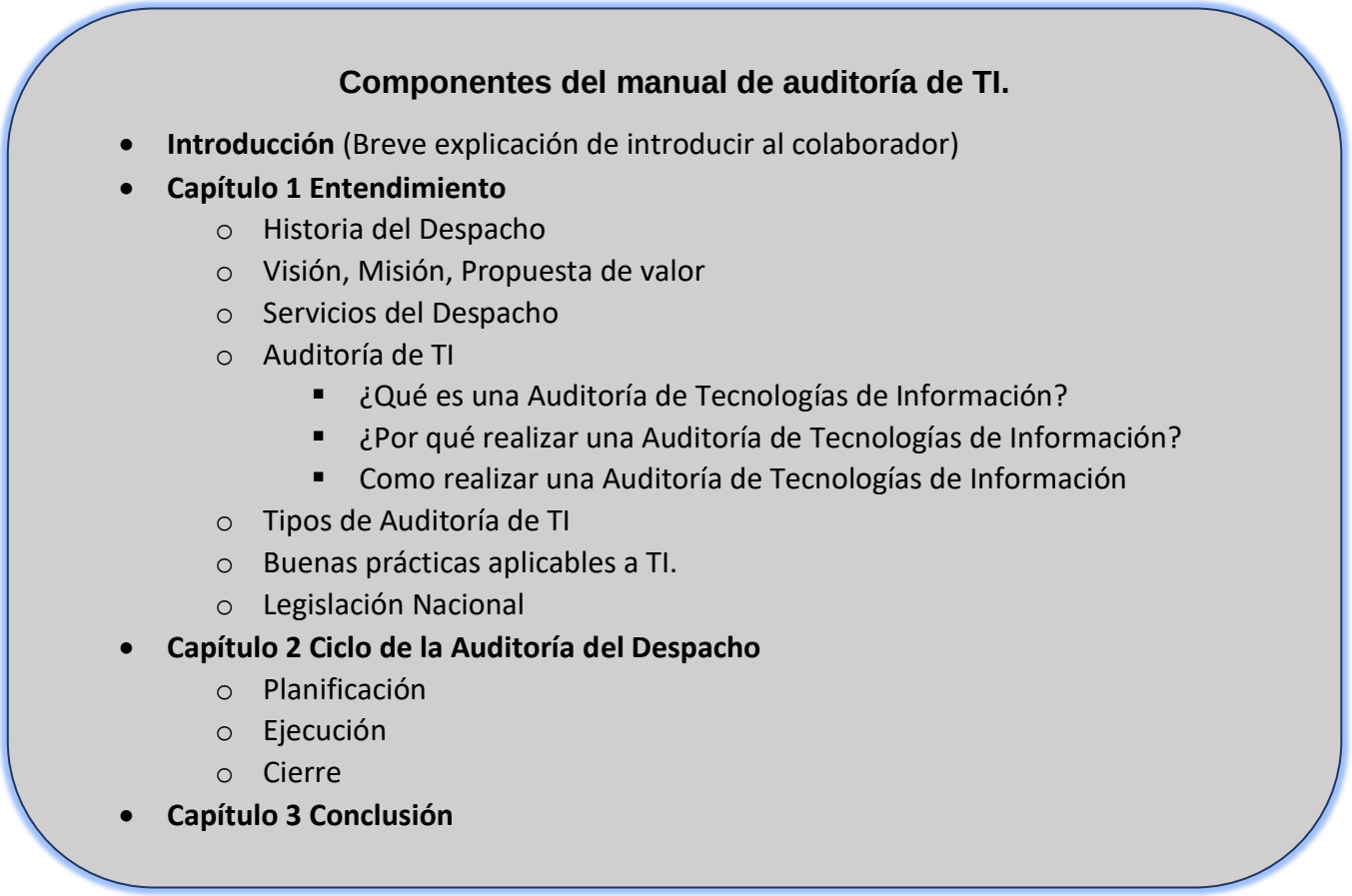
1.5 Alcance

Para facilitar el entendimiento del proyecto, se procede a detallar el alcance según las áreas de la metodología a seguir, no obstante, primero se procede a explicar el ciclo de vida de la auditoría en la firma.

Como se mencionó anteriormente el manual tiene el objetivo de satisfacer las necesidades de capacitación durante el desarrollo de la vida profesional de un auditor de tecnología de información, para esto el proyecto abarcará el ciclo de la auditoría dentro del Despacho de la siguiente manera. La explicación detalla del ciclo de la auditoría y se puede observar en el Apéndice D: Ciclo actual de auditoría.

Los componentes que contempla el manual a desarrollar se observan en la Figura 1.3.

Figura 1.3 Componentes del manual de auditoría de TI



Fuente: Elaboración propia.

1.5.1 Entendimiento

Consiste en conocer el Despacho, dónde se busca que el colaborador conozca la compañía dónde se desenvolverá como profesional. Abarca el origen de la organización, la misión, visión y propuesta de valor, los servicios que brinda. Una explicación de lo que será su nueva área de trabajo, dónde se contempla la respuesta a las siguientes interrogantes:

- ¿Qué es una Auditoría de Tecnologías de Información?
- ¿Por qué realizar una Auditoría de Tecnologías de Información?
- ¿Como realizar una Auditoría de Tecnologías de Información?

Los tipos de auditoría, externa e interna, dónde se indicará en que consiste cada una y las diferencias entre las mismas.

Las buenas prácticas aplicables a TI, más adelante cuando se explique los procedimientos de las pruebas se incluirá un apartado dónde se haga referencia a estas prácticas para facilitar su relación.

Y, por último, se mencionará reglamentos, leyes y normativas que apliquen en Costa Rica, y también a que sectores, entre ellas destacan.

- Normas técnicas para la gestión y el control de las Tecnologías de Información de la CGR.
- SUGEF 14-17 Reglamento general de gestión de la tecnología de información.
- Ley de protección de la persona frente al tratamiento de sus datos personales. (Ley n.º 8968).

En el capítulo de conclusión serán agregados los documentos pertinentes a cada actividad, que hayan sido identificados a lo largo de la ejecución del proyecto.

1.5.2 Ciclo de auditoría

El manual abarcará el entendimiento del ciclo de auditoría, compuesto por las tres fases tradicionales:

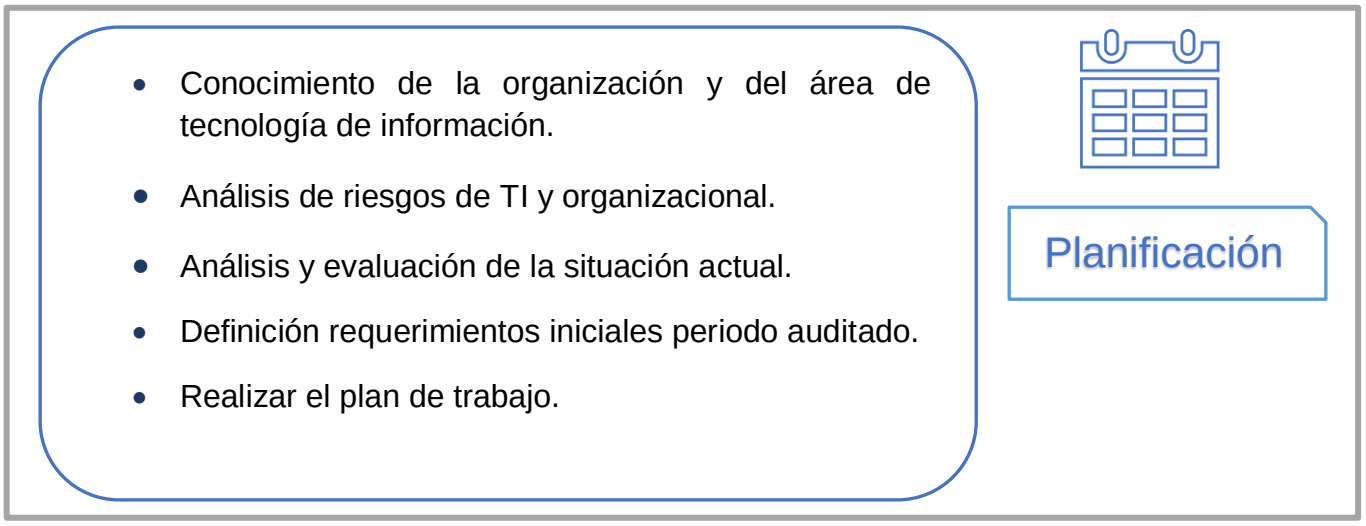
- Planificación.
- Ejecución.
- Cierre.

En el próximo apartado se procede a detallar el contenido de las etapas.

1.5.2.1 Etapa de planificación

En la Figura 1.4 se observa las actividades que la componen.

Figura 1.4 Etapa de planificación



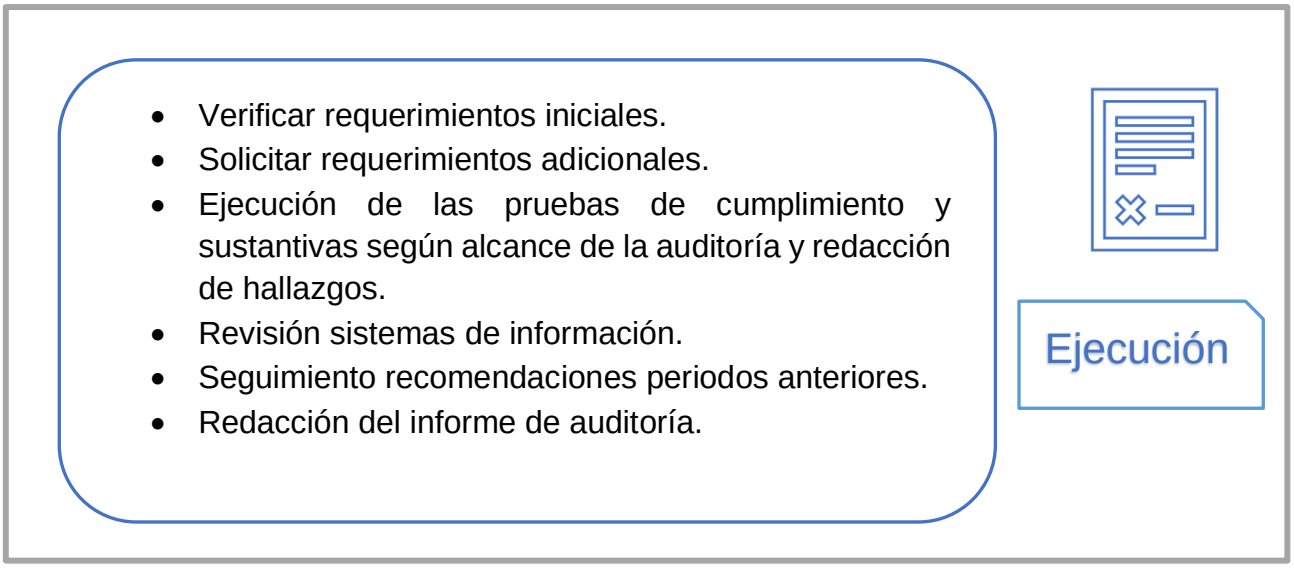
Fuente: Elaboración propia.

Este proyecto abarcará la explicación y el entendimiento de las actividades que compone esta etapa y su aplicación, aunque estas actividades son realizadas por el encargado de la auditoría, se espera que un asistente en un periodo corto este en capacidad de realizarlas satisfactoriamente.

1.5.2.2 Etapa de ejecución

En la etapa de ejecución, la cual se puede observar en la Figura 1.5, es dónde se centrará la aplicación del conocimiento adquirido, por medio de procesos, plantillas y herramientas, ya que será la fase dónde se desenvolverá el colaborador.

Figura 1.5 Etapa de ejecución



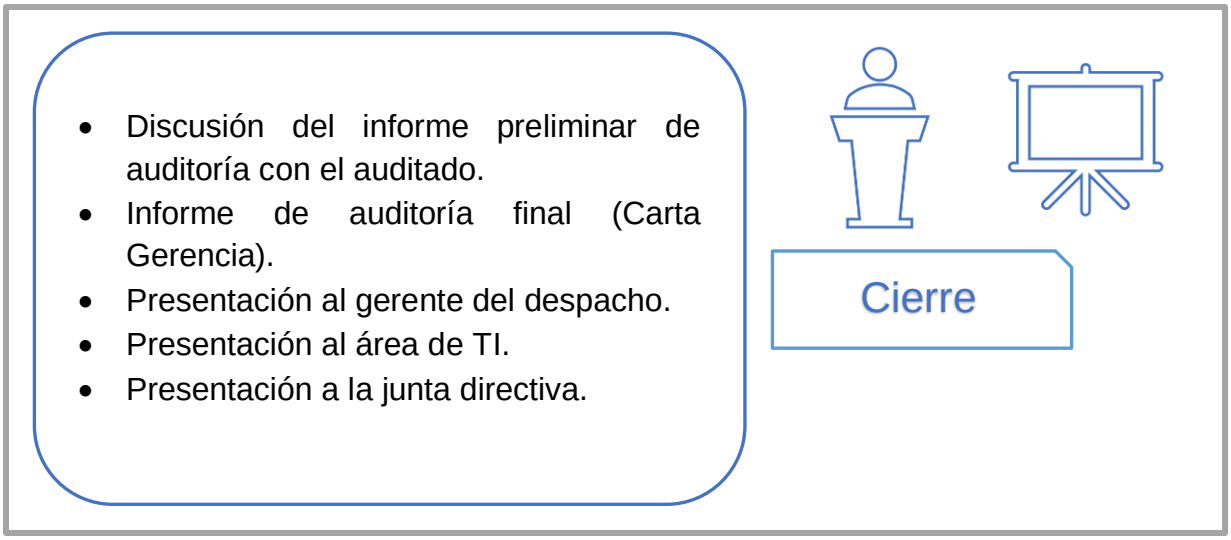
Fuente: Elaboración propia.

En esta etapa es dónde se enfocará el proyecto, más adelante se explicará cómo se abarcará cada actividad con la metodología de trabajo propuesta en el marco metodológico. Las actividades se abarcarán de manera que el colaborador no solo comprenda, si no que sea capaz de aplicar el procedimiento establecido por cada prueba, dónde se abarcará el proceso optimizado, que herramientas o plantillas se utilizan y su debida explicación de cómo usarlas. También se contempla la redacción del informe, la cual es responsabilidad del encargado de la auditoría.

1.5.2.3 Etapa de cierre

En la Figura 1.6 se observa las actividades que componen esta etapa.

Figura 1.6 Etapa de cierre



Fuente: Elaboración propia.

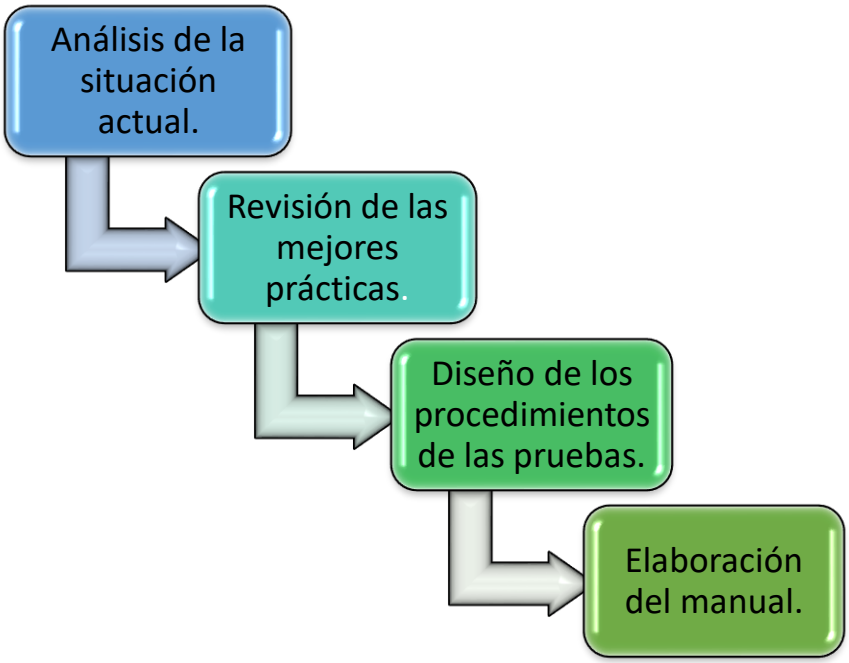
Este proyecto abarcará el entendimiento y ejecución de las actividades descritas en la figura anterior, aunque son responsabilidad del encargado y del gerente del departamento, es importante tomarlas en cuenta, para una visión integral por parte del colaborador.

Auditorías internas, consultorías de TI y otros servicios brindados por el departamento que no tomen como referencia a la CGR o *COBIT* 5, no se incluirá su explicación ni documentación, solo se hará mención de ellos. Como por ejemplo una auditoría basada en la *ISO* 27001.

1.5.3 Metodología de trabajo

Para lograr comprender la elaboración del manual dentro del ciclo de la auditoría de TI en el Despacho, se procedió a proponer y aplicar una metodología de trabajo, la cual se observa en la Figura 1.7, compuesta por cuatro fases, las cuales se identifican a continuación, además de explicar cómo serán consideradas en este proyecto.

Figura 1.7 Metodología de trabajo



Fuente: Elaboración propia.

1.5.3.1 Análisis de la situación actual

En esta fase se busca documentar el proceso actual del ciclo de la auditoría de TI, dónde se analizarán los procedimientos relacionados con cada etapa del ciclo, la cual incluye las pruebas de auditoría, producto de este análisis se definirá una lista de pruebas que serán incluidas posteriormente en el manual.

Es importante mencionar que las pruebas que se incluirán en este manual se basan en un análisis de años anteriores y no contempla estudios a futuro. Para su mejor comprensión en el Apéndice E: Temas por explicar, se indican los temas que serán considerados en este manual, esto quiere decir que cualquier otra prueba que no esté asociada a uno de estos temas, no será considerada en este proyecto.

1.5.3.2 Revisión de las mejores prácticas

Para proponer mejoras a los procedimientos actuales se debe realizar una comparación con las mejores prácticas del mercado. En la Tabla 1.5, se indica las fuentes principales que se abarcarán en este proyecto. Estas fuentes son seleccionadas según el aprendizaje adquirido a lo largo de la carrera y que son aplicables para este proyecto.

Tabla 1.5 Identificación de mejores prácticas

Fuente	Área
Objetivos de Control para Información y Tecnologías Relacionadas (*COBIT* 5).	Controles de auditoría
Information Technology Infrastructure Library (ITIL).	Gestión de procesos de TI
ISO/IEC 20000.	Gestión de servicios de TI.
ISO/IEC 27000.	Estándares de seguridad.
The Open Group Architecture Framework (TOGAF).	Arquitectura.
A Practical Guide to Information Systems Strategic Planning by Anita Cassidy.	Plan estratégico de TI.
Guía de los fundamentos para la dirección de proyectos. (Guía del PMBOK).	Administración de proyectos.

Nota: Elaboración propia.

Se realizará un análisis por cada prueba definida en la primera etapa y se procederá a identificar las mejoras del proceso, esto incluye atributos, plantillas y herramientas. Aquí se contará con la supervisión del encargado para un mejor seguimiento, pero la aprobación por parte del gerente será hasta la fase siguiente.

1.5.3.3 Diseño de los procedimientos de las pruebas

Una vez identificadas las oportunidades de mejora por cada prueba definida en la primera fase, se procede a realizar y documentar el procedimiento, se busca que el colaborador sea capaz de realizar la prueba de auditoría con este procedimiento, y que sea capaz de comprenderlo y aplicarlo de manera autodidacta, por lo cual abarca todos los detalles para completar las plantillas actuales. Para asegurarse la correcta creación de los procesos, estos deberán ser aprobados individualmente por el gerente del departamento.

1.5.3.4 Elaboración del manual

Ya con los procesos aprobados y la documentación de las etapas de planificación y cierre, se procede a elaborar el manual. Además de los apartados de introducción y conclusión mencionados anteriormente en la Figura 1.3.

En la siguiente página se presentan los supuestos del proyecto.

1.6 Supuestos

Para el desarrollo del trabajo final de graduación, se estima que los siguientes elementos serán de apoyo por parte de la organización:

1. Equipo de trabajo: El Despacho facilitará al estudiante una computadora personal para el desarrollo del proyecto, además del espacio físico y demás artículos necesarios.
2. Reuniones con el personal del departamento: Se contará como mínimo una reunión semanal por nivel, gerente, encargado y asistente.
3. Alineación de las pruebas de auditoría con COBIT 5. Aunque COBIT 5 no explica a detalle las pruebas consideras en el manual de auditoría, se considera que las pruebas tienen relación con al menos uno de los 37 procesos.
4. Debido a que la mayor parte de los clientes del Despacho son del sector público, se espera que las normativas a las que están sujetas estas organizaciones por ejemplo Normas técnicas de la CGR o la norma SUGEF 14-17 no varíen de forma drástica en el corto tiempo.
5. Se consideran las buenas prácticas mencionadas en la introducción como las más actas para la gestión de las tecnologías de información.

1.7 Entregables

El proyecto “Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho” cuenta con dos entregables finales:

- **Informe final académico:**

  El informe final cuenta con fines académicos que pretende desarrollar y detallar todo el proceso de investigación, análisis y obtención de los resultados a través de la realización del Proyecto Final de Graduación.

- **Manual de auditoría de tecnologías de información:**

  Este manual es para uso del Despacho cuyo propósito es ser el material principal para la capacitación de los colaboradores, les permitirá a los asistentes tener el conocimiento estandarizado para entender y realizar las pruebas de auditoría de manera eficiente.

Se procede a detallar la gestión de ambos entregables.

1.7.1 Gestión del proyecto

Para realizar una correcta gestión del proyecto, el cual incluye el informe final académico, se utilizarán los siguientes documentos.

1.7.1.1 Minutas

Se completará una o más minutas por reunión realizada con los involucrados del proyecto, pues permitirá tener un respaldo y brindar trazabilidad de lo conversado. En el Anexo 3: Minuta de reuniones, se muestra la minuta a utilizar.

1.7.1.3 Gestión de cambios

Para llevar el adecuado control sobre los cambios que se realizarán durante el proyecto, se procede a detallar la plantilla, dónde se indicará el solicitante, la descripción del cambio, el responsable de la aprobación y los ítems modificados. En el Apéndice F: Plantilla gestión de cambios, se observa la plantilla a utilizar.

1.7.2 Entregables del producto

En esta sección se deberán describir los entregables en cuanto al manual de auditoría de TI. A continuación, se detallan:

1.7.2.1 Entregables: Fase Análisis de la situación actual

En esta fase se entregará un informe de resultados el cual incluye:

- Procedimiento actual de capacitación, cuales materiales recibe el colaborador, como los almacena, porcentaje de estudio por parte de los asistentes actuales, observaciones al procediendo actual por parte de asistentes y encargados.
- Documentación del ciclo de auditoría de TI dentro del Despacho.
- Lista y documentación de las pruebas que se van a contemplar en el manual relacionadas a los temas indicados en el Apéndice E: Temas por explicar. A partir de la investigación realizada en auditorías anteriores, y con las reuniones del personal del departamento de auditoría y consultoría de TI, se presentará la lista definitiva de las pruebas que se incluirán en la creación del manual. Esta lista debe ser aprobada por el gerente del departamento.
- Documentación Capítulo de Introducción del manual de auditoría, mencionado en la Figura 1.3.

1.7.2.2 Entregables: Fase Revisión de las mejores prácticas

En la segunda fase se entregará un informe dónde se contemple una comparación de los procedimientos actuales con el procedimiento establecido por las fuentes externas, consideradas como las mejores prácticas del mercado. En la comparación se recalcarán aspectos claves que actualmente no son considerados.

1.7.2.3 Entregables: Diseño de los procedimientos de las pruebas

Para esta fase se entregarán los procedimientos de las pruebas definidas en la primera fase ya optimizados, considerando el estudio anterior con la mejor práctica, para esto, se le enviará al gerente del departamento los procedimientos uno a uno, para su debida verificación y aprobación. Cada prueba contará con un apartado dónde se indiquen las fuentes consultadas, en caso de que el colaborador ocupe o desee expandir su conocimiento.

1.7.2.4 Entregables: Elaboración del manual

En esta fase se entregará la primera versión del manual como tal, dónde se incluirá además del procedimiento de las pruebas y los ítems definidos en la Figura 1.3.

1.8 Limitaciones

Durante el desarrollo del proyecto, existen posibles factores que puede afectar el proceso, a continuación, se mencionan.

- Las pruebas de auditorías incluidas serán producto de un estudio de años anteriores, no se contempla pruebas a futuro.
- Ausencia del personal involucrado en el proyecto. Por ejemplo, los encargados actuales, quienes son una fuente principal de cómo se realizan los procesos actualmente.
- Los procedimientos actuales se basan en el conocimiento tácito, esto quiere decir que no existe una documentación actual, si no que forma parte del modelo mental, producto de la experiencia que han adquirido en su labor diaria.
- El manual de auditoría solo abarcará dos posibles clientes, organizaciones gubernamentales supervisados por la Contraloría General de la Republica y clientes privados que utilicen COBIT como marco de referencia para la gestión de TI.

Capítulo II

Marco Teórico

2. Marco teórico

El marco teórico, también conocido como marco referencia, tiene como propósito proporcionar un sistema coordinado y coherente de conceptos y definiciones con los cuales se abordó el problema planteado (Ulate Soto & Vargas Morúa, 2016).

Además, se describen los conceptos teóricos y prácticos que sustentan el desarrollo del estudio, dónde se realizó una búsqueda de publicaciones, soluciones anteriores similares, libros y otras fuentes, de tal manera que se pueda conocer como otras personas han resuelto el problema, y así poder construir un método propio de solución (Ulate Soto & Vargas Morúa, 2016).

Se incluyen las metodologías, buenas prácticas y normas asociadas con tecnologías de información, que se consideraron a partir de la investigación como las más usadas en las organizaciones, las cuales son tomadas como referencia para las pruebas de control y la elaboración del manual.

2.1 Administración

El trabajo final de graduación propuesto consiste en un manual de auditoría de TI, por lo cual tomando como base el manual se procede a explicar los conceptos asociados, empezando por administración, ya que de aquí es dónde se originan los procedimientos y, por ende, la documentación en los manuales.

A continuación, se procede a explicar el concepto de administración, y otros conceptos con el fin de dar a entender cómo se asocia con el trabajo por realizar. Se iniciará desde los conceptos considerados como base del proyecto, hasta llegar a conceptos específicos del manual.

Según George R. Terry, “Administrar implica el logro de objetivos por parte de personas que aportan sus mayores esfuerzos de acuerdo con acciones preestablecidas” (Terry, Principios de administración, 1984, pág. 1).

Esto implica saber que deben hacer, determinar cómo lo deben hacer, comprender cómo lograr que lo hagan y verificar la efectividad de sus esfuerzos. Para alcanzar lo anterior se debe establecer y mantener un ambiente dónde los colaboradores, trabajando juntos, puedan desempeñarse de la mejor manera (Terry, Principios de administración, 1984).

Por su parte, Zacarias Torres Hernández menciona que la administración "Es el resultado histórico acumulado de la contribución de científicos en múltiples disciplinas" (Torres Hernández, 2014, pág. 6).

El manual realizado en este proyecto servirá para comprender los procesos actuales de auditoría de TI, y a su vez ayudará a mejorar el tiempo de ejecución de las pruebas de auditoría, más adelante se mencionarán los resultados obtenidos de los tiempos de ejecución actuales.

2.1.1 Planeamiento

Según George R. Terry, "Planear es seleccionar y relacionar los hechos y formular y emplear supuestos respecto al futuro, en lo que se hace a la visualización y formulación de actividades propuestas para alcanzar los resultados esperados." (Terry, Principios de administración, 1984, pág. 35).

Se debe planear tanto la elaboración del manual, como el uso que se le va a dar después al material recopilado. También es importante mencionar que dentro del ciclo de auditoría se encuentra una etapa de planeación.

2.1.2 Organizar

Como se comentó en el apartado 1.3.1 Situación problemática del proyecto, actualmente las pruebas se realizan según el criterio del auditor, y puede variar entre una persona y otra, al crear un manual se ayudaría a organizar tanto los recursos como los procedimientos aplicados en las pruebas de auditoría.

Organizar consiste en reunir y disponer de todos los recursos necesarios, incluyendo las personas, de modo que el trabajo a realizar se cumpla satisfactoriamente (Terry, Principios de administración, 1984).

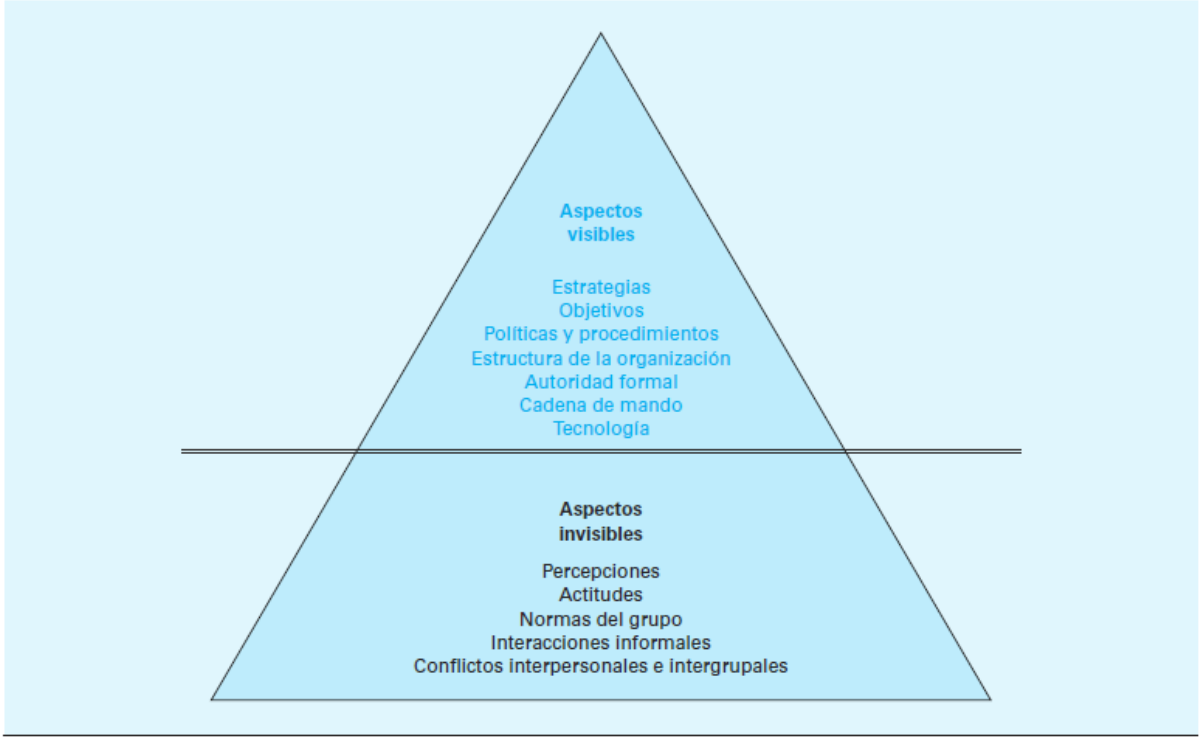
2.1.3 Comportamiento organizacional

El comportamiento organizacional estudia la dinámica y el funcionamiento de las organizaciones. Como cada una es diferente, el comportamiento organizacional define las bases y las características generales de su funcionamiento (Chiavenato, 2009).

También se refiere: “al estudio de las personas y los grupos que actúan en las organizaciones. Se ocupa de la influencia que todos ellos ejercen en las organizaciones y de la influencia que las organizaciones ejercen en ellos.” (Chiavenato, 2009, pág. 6).

En la Figura 2.1, tomada del libro Comportamiento Organizacional de Idalberto Chiavenato, se muestra el comportamiento organizacional como un iceberg, el manual propuesto se enfocará en los aspectos visibles.

Figura 2.1 El comportamiento organizacional como un iceberg



Fuente: Comportamiento organizacional (2009, pág. 7).

El manual propuesto viene a ser un recurso vital para la organización del departamento de tecnologías de información, ya que ejemplifica los procedimientos de tal manera que los colaboradores puedan realizar su trabajo satisfactoriamente. Para esto primero se debe conocer el comportamiento organizacional dentro del despacho y más específicamente el departamento de TI.

2.2 Manual

Los manuales son registros de información documentada que puede ser utilizada para orientar a las personas en temas específicos, hay una gran variedad de manuales, desde los generales, hasta específicos, ya sea para una función o área, brindan ventajas en el proceso de capacitación.

2.2.1 Definición de manual

Se denomina manual a toda guía de instrucciones que sirve para el uso de un dispositivo, la corrección de problemas o el establecimiento de procedimientos de trabajo (Editorial Definición MX, 2014).

2.2.2 Definición de procedimiento

El Diccionario de la Real Academia Española (DRAE) define procedimiento como: “Método de ejecutar algunas cosas” (Dle.rae.es, 2017).

Una definición más detallada es: “Un procedimiento es un plan que contiene la exacta secuencia cronológica para las tareas específicas necesarias para ejecutar el trabajo asignado” (Terry, Principios de administración, 1984, pág. 49).

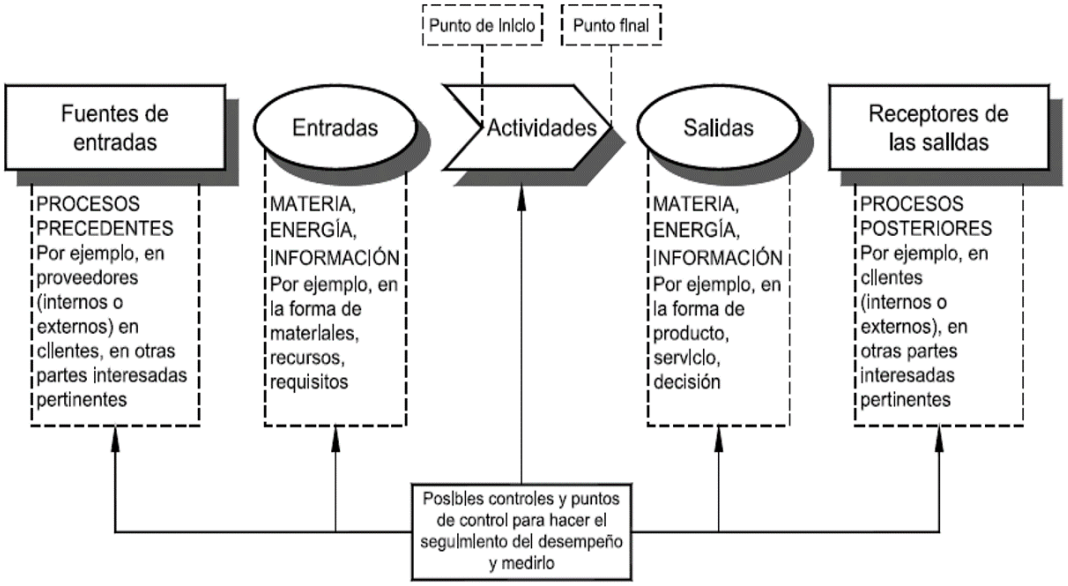
Parte del trabajo por realiza consiste en la elaboración de los procedimientos utilizados en la aplicación de una auditoría de TI.

2.2.3 Definición de proceso

Es común confundir el concepto de proceso y procedimiento, por lo cual se procede a indicar la diferencia entre ambos términos.

Un proceso es: “un conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados, en la Figura 2.2 se muestra la representación de los elementos de un proceso. En cambio, un procedimiento es una forma específica para llevar a cabo una actividad o un proceso” (Toro, 2016).

Figura 2.2 Representación esquemática de los elementos de un proceso



Fuente: Nuevas Normas ISO (2016).

Los procedimientos de las pruebas de auditoría son un elemento esencial en la elaboración de este manual, dónde inicialmente se documentarán los procedimientos actuales y, posteriormente, con ayuda de la metodología seleccionada, se procederá a sugerir opciones de mejora.

2.2.3 Manual administrativo

Según los autores del libro Principios de administración, "[…] son registros escritos de información e instrucciones que conciernen al empleado y pueden ser utilizados para orientar los esfuerzos de un empleado en una empresa" (Terry & Franklin, Principios de administación, 1999).

El uso de los manuales administrativos (basados en los registros antiguos), data de los años de la segunda guerra mundial, en virtud de que en el frente se contaba con personal no capacitado en estrategias de guerra y fue mediante estos que se instruía a los soldados en las actividades que deberían desarrollar en combate (Terry & Franklin, Principios de administación, 1999).

Si bien es cierto hay gran diversidad de manuales administrativos, el proyecto se enfocará en un manual específico de la organización, el cual comprende las funciones y responsabilidades de un área en concreto.

2.2.4 Partes de un manual administrativo

Siguiendo con la fuente del libro principios de administración, se considera los siguientes apartados en la elaboración de un manual administrativo para un área específica (Aguayo, 2013).

1. Portada.
2. Índice.
3. Presentación.
4. Antecedentes.
5. Marco Jurídico.
6. Atribuciones.
7. Estructura Orgánica.
8. Descripción de Puestos.
9. Directorio.
10. Firmas de autorización.

Adicionalmente, como se va a realizar un manual que incluya los procedimientos de pruebas de auditoría, el autor recomienda los siguientes aspectos (Aguayo, 2013):

1. Carátula del manual.
2. Contenido del manual.
3. Documentación de aprobación técnica y registro del manual.
4. Documento de actualización.
5. Introducción del manual.
6. Objetivo del manual.
7. Portada.
8. Índice del procedimiento.
9. Objetivo del procedimiento.
10. Normas de operación.
11. Descripción narrativa del procedimiento.
12. Diagramas de flujo.
13. Anexos y apéndices.
14. Glosario.
15. Participantes en la elaboración del manual.
16. Directorio.

Se tomará en cuenta estas secciones para determinar las partes que debe contener el manual propuesto.

2.3 Auditoría

En el ambiente financiero, la auditoría, en general es un examen sistemático de los estados financieros, registros y operaciones con la finalidad de determinar si están de acuerdo con los principios de contabilidad generalmente aceptados, con las políticas establecidas por la dirección y con cualquier otro tipo de exigencias legales o voluntariamente aceptadas (Madariaga, 2004, pág. 13).

El fin de la auditoría es averiguar la exactitud, integridad y autenticidad de los estados financieros, expedientes y demás documentos administrativos-contables presentados por la dirección (Madariaga, 2004, pág. 13).

Para ampliar el concepto, se puede observar la definición de la RAE, la cual define la auditoría como "Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse" (Dle.rae.es, 2017).

Para finalizar la explicación del concepto es importante mencionar la diferencia de la auditoría en sus inicios y la auditoría actual, según el libro manual práctico de auditoría, "esta reside en la mente del auditor. Antes, el auditor concentraba sus esfuerzos en la verificación y protección; ahora, su examen está enfocado de modo que tenga en cuenta todas las actividades del negocio. Sus recomendaciones están orientadas a que las operaciones de la empresa sean más beneficiosas" (Madariaga, 2004).

En la actualidad, la auditoría ha tenido una explosión de áreas, no obstante, siempre siguen los mismos criterios, resaltándose la independencia (entre el auditor y el auditado), los procedimientos (pruebas selectivas y/o evaluación de riesgos), la documentación (papeles de trabajo), los informes (opinión, dictamen, recomendaciones) y por último los estándares para regular esa actividad (Mantilla, 2003).

2.3.1 Conceptos claves

Se procede a mencionar los conceptos más relevantes en el tema de auditoría, los cuales serán considerados para la creación de los procedimientos en el manual.

2.3.1.1 Control

Henri Fayol, quién es considerado uno de los principales contribuyentes al enfoque clásico de la administración, definía control como “la verificación de si todo ocurre en una empresa conforme el programa adoptado, a las órdenes dadas y a los principios admitidos” (Madariaga, 2004, pág. 14).

Otra definición de control en el área de auditoría es: el análisis permanente de las desviaciones entre objetivos y realizaciones y la adopción de las medidas correctoras que permitan el cumplimiento de los objetivos o bien su adaptación necesaria (Madariaga, 2004).

Por otra parte, Samuel Mantilla indica “Control es un conjunto de normas, procedimientos y técnicas a través de las cuales se mide y corrige el desempeño para asegurar la consecución de objetivos y técnicas” (Mantilla, 2003, pág. 59).

Existen diversos tipos de control, no obstante, se van a mencionar los relevantes para este proyecto, se procederá a ampliar cada concepto más adelante.

- Control interno.
- Auditoría interna.
- Auditoría externa.

2.3.1.1.1 Control interno

Para Robbins Coulter, el control como función consiste en: “Vigilar el desempeño actual, compararlo con una norma y emprender las acciones que hicieran falta” (Contraloría General de la República de Perú, 2010, pág. 17).

El Control Interno es un:

Proceso integral efectuado por el titular, funcionarios y servidores de una entidad, diseñado para enfrentar los riesgos y para asegurar que se alcancen los siguientes objetivos gerenciales:

- Promover la eficiencia, eficacia, transparencia y economía en las operaciones de la entidad, así como en la calidad de los servicios que presta.
- Cuidar y resguardar los recursos y bienes de la organización contra cualquier forma de pérdida, deterioro, uso indebido de los mismos y actos ilegales, así como contra todo hecho irregular o situación que pudiera afectarlos.
- Cumplir con la normatividad aplicable a la entidad y a sus operaciones.
- Garantizar la confiabilidad y oportunidad de la información.
- Fomentar e impulsar la práctica de valores institucionales.
- Promover que los funcionarios o servidores cumplan con rendir cuentas sobre la misión u objetivo que les haya sido encargado, así como sobre los fondos y bienes que les hayan sido asignados (Contraloría General de la República de Perú, 2010).

2.3.1.1.1.1 Sistema de control interno

El sistema de control interno es el conjunto de acciones, actividades, planes, políticas, normas, registros, procedimientos y métodos, incluido el entorno y actitudes que desarrollan autoridades y su personal a cargo, con el objetivo de prevenir posibles riesgos que afectan a una organización. La estructura que menciona la Contraloría General de la Republica de Perú es la siguiente (Contraloría General de la República de Perú, 2010):

- Ambiente de control.
- Evaluación de riesgos.
- Actividades de control gerencial.
- Información y comunicación.
- Supervisión.

2.3.1.1.2 Auditoría externa

La auditoría externa se define como los métodos empleados por una firma externa de profesionales para averiguar la exactitud del contenido de la información presentando por una empresa. Nace como instrumento de control. Sin embargo, actualmente se ha ampliado la responsabilidad social del auditor, ya que existen otras partes interesadas (Madariaga, 2004).

El enfoque principal del manual se basa en la auditoría externa, no obstante, se pretende abarcar puntos esenciales de auditoría interna para que los colaboradores distingan las diferencias entre ambas.

2.3.1.1.3 Auditoría interna

"El Instituto de Auditores Internos de los Estados Unidos define la auditoría interna como una actividad independiente que tiene lugar dentro de la empresa y que está encaminada a la revisión de operaciones contables y de otra naturaleza, con la finalidad de prestar un servicio a la dirección" (Madariaga, 2004, pág. 25).

El objetivo principal es ayudar a la dirección con el cumplimiento de sus funciones y responsabilidades, proporcionándole análisis objetivos, evaluaciones, responsabilidades y comentarios pertinentes sobre las operaciones examinadas. Se mencionan los objetivos específicos que permiten cumplir el objetivo principal (Madariaga, 2004).

En ocasiones no se tienen claras las diferencias entre auditoría interna y auditoría externa, estas diferencias se pueden observar en la Tabla 2.1.

Tabla 2.1 Algunas diferencias entre la auditoría externa y la auditoría interna

Auditoría externa	Auditoría interna
Por la posición	
Los códigos de ética profesional de los institutos de censores de cuentas prohíben que sus miembros puedan realizar una auditoría externa, en una empresa que no sean independientes.	El auditor interno es un empleado de la empresa, dependiente de la misma.
Por los objetivos perseguidos	
Los objetivos por alcanzar son: 1. Expresar una opinión sobre los estados financieros examinados. 2. Sugerir al cliente procedimientos para la mejora y perfeccionamiento de su sistema de control interno.	Los objetivos básicos de la auditoría interna son: 1. Función de asesoramiento. 2. Función de control.
Por la utilidad	
Informe de auditoría y carta de recomendaciones.	Va dirigida a la propia empresa.
Por el periodo de su actuación	
Normalmente, la auditoría externa se realiza una vez al año, es un trabajo discontinuo.	El auditor interno, al ser empleado de la compañía, realiza un trabajo de tipo continuo o permanente, durante todo el año.
Por el enfoque de su trabajo	
El auditor externo revisa y evalúa el sistema de control interno, y de acuerdo con su adecuación, determina el alcance de las pruebas que se tendrá que realizar.	El auditor interno examina tanto los controles operativos como administrativos, siendo su revisión de carácter más amplio que el auditor externo.

Nota: Fuente Madariaga (2004).

2.3.1.2 Evidencia

"La evidencia es cualquier tipo de datos que utiliza el auditor para determinar si la información que está auditando ha sido declarada de acuerdo con el criterio establecido." La evidencia asume varias formas diferentes, entre ellas: (Arens, Elder, & Beasley, 2007, pág. 5).

- Testimonio oral del auditado (cliente).
- Comunicación por escrito con las partes externas.
- Observaciones por parte del auditor.
- Datos electrónicos sobre las transacciones.

Por otra parte, Sergio Espinoza autor del libro Auditoría de aplicaciones informáticas dice la evidencia "[…] es el conjunto de hechos comprobados que sustentan las conclusiones del auditor" (Espinoza, 2009, pág. 7).

Para satisfacer el propósito de la auditoría, quienes la llevan a cabo deben obtener calidad y volumen suficientes de evidencia. Los auditores deben determinar los tipos y cantidad de evidencia necesaria y evaluar si la información corresponde al criterio establecido (Arens, Elder, & Beasley, 2007).

La auditoría de TI, también se basa en la evidencia para brindar sus conclusiones, en cada prueba se explicará a detalle la evidencia utilizada para cada prueba.

2.3.1.3 Criterios de auditoría

La ISO 19001:2001 define los criterios de auditoría como el grupo de políticas, procedimientos o requisitos usados como referencia y contra los cuales se compara la evidencia de auditoría (Umc.edu.ve, 2011). En el caso del despacho, las fuentes más comunes para establecer los criterios de auditoría son *COBIT* 5 y las Normas Técnicas de la CGR.

2.3.1.4 Prueba de control

Las pruebas de control son los procedimientos utilizados para comprobar la eficacia de los controles en apoyo a un riesgo de control evaluado. Debido a esto la auditoría no está diseñada para detectar todas las deficiencias en los procesos y objetivos de control evaluados, ya que no se lleva a cabo de forma continua durante el período de revisión; las evaluaciones realizadas consisten en un estudio sustentado en muestras y pruebas selectivas de la evidencia que respalda el cumplimiento de los procesos y objetivos de control evaluados, los cuales producto de las limitaciones inherentes, pueden presentar resultados fallidos debido a errores o debilidades propias del control interno que ocurran y no sean detectadas (Arens, Elder, & Beasley, 2007).

Se procede a mencionar los cuatro tipos de procedimiento para las pruebas de control (Arens, Elder, & Beasley, 2007):

- Hacer consulta con el personal adecuado del cliente.
- Examinar documento, registros e informes.
- Observar las actividades relacionadas con el control.
- Repetición de procedimientos del cliente.

2.3.1.5 Hallazgo

Un hallazgo es el resultado de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría, este se incluirá dentro del procedimiento de las pruebas. Por su parte, la Contraloría General del Estado de Ecuador menciona: “Los hallazgos en la auditoría se definen como asuntos que llaman la atención del auditor y que, en su opinión, deben comunicarse a la entidad, ya que representan deficiencias importantes que podrían afectar en forma negativa, su capacidad para registrar, procesar, resumir y reportar información confiable y consistente, en relación con las aseveraciones efectuadas por la administración” (Contraloria.gob.ec, s.f.).

2.3.2 Tipos de auditoría

Tomando como referencia el libro Auditoría un Enfoque Integral, se tienen tres tipos principales de auditoría (Arens, Elder, & Beasley, 2007):

- Auditoría operacional: evalúa la eficiencia y eficacia de cualquier parte de los procedimientos y métodos de operación de una organización. Cuando se completa una auditoría operacional, por lo general, la administración espera recomendaciones para mejorar sus operaciones.
- Auditoría de cumplimiento: se realiza para determinar si la entidad auditada aplica correctamente los procedimientos, reglas o reglamentos específicos que una autoridad superior ha establecido.
- Auditoría de estados financieros: se lleva a cabo para determinar si los estados financieros en general (la información que se está verificando) han sido elaborados de acuerdo con el criterio establecido.

En el caso de la auditoría de TI, actualmente es una combinación de una auditoría operacional y una de cumplimiento, operacional porque se busca mejorar los procedimientos actuales, y de cumplimiento ya sea para cumplir lo expuesto por una entidad como la CGR de Costa Rica o CONASIF por medio de la normativa SUGEF 14-17, también se pueden tomar marcos y normas como referencia del cumplimiento por ejemplo *COBIT* 5 o la *ISO* 20000, entre otros.

2.3.3 Etapas de la auditoría

Dependiendo de la fuente de información consultada, este concepto se puede encontrar como etapas, fases o ciclo de auditoría. Igualmente sucede con el nombre de las etapas que pueden variar según la fuente consulta, no obstante, se sigue el flujo de planificación, ejecución y cierre, tal como lo explica la norma *ISO* 19011, la cual se puede observar en el apartado 2.5.3 *ISO* de este capítulo. A continuación, se procede a mencionar una metodología investigada.

2.3.4 Metodología de la auditoría administrativa

En el capítulo tres del libro Auditoría Administrativa del autor Enrique Benjamín Franklin se explica la siguiente metodología, la cual tiene como propósito: “servir como marco de actuación para que las acciones en sus diferentes fases de ejecución se conduzcan en forma programada y sistemática, se unifiquen criterios y se delimite la profundidad con que se revisarán y aplicarán los enfoques de análisis administrativo para garantizar el manejo oportuno y objetivo de los resultados” (Franklin, 2007, pág. 75).

También cumple la función de facilitar al auditor la identificación y ordenamiento de la información correspondiente al registro de hechos, hallazgos, evidencias, transacciones, situaciones, argumentos y observaciones para su posterior examen, informe y seguimiento (Franklin, 2007).

2.3.4.1 Planeación

La planeación se refiere los lineamientos de carácter general que regulan la aplicación de la auditoría para garantizar que la cobertura de los factores prioritarios, fuentes de información, investigación preliminar, proyecto de auditoría y diagnóstico preliminar, sea suficiente, pertinente y relevante (Franklin, 2007).

Uno de los aspectos importantes de esta etapa es el programa de trabajo, el cual abarca a los responsables de las pruebas, las áreas de estudio, actividades por realizar, el calendario de entregas y reportes de avances (Franklin, 2007).

2.3.4.2 Instrumentación

En esta etapa se seleccionan y aplican las técnicas de recolección que se estimen más viables de acuerdo con las circunstancias propias de la auditoría, la selección de instrumentos de medición que se emplearán, el manejo de los papeles de trabajo y evidencia, así como la supervisión necesaria para mantener una coordinación eficaz. Las técnicas de recolección de información más comunes son las siguientes (Franklin, 2007):

- Investigación documental.
- Observación directa.
- Acceso a redes de información.
- Entrevistas y cuestionarios.

2.3.4.3 Examen

Consiste en dividir o separar los elementos componentes de los factores bajo revisión para conocer la naturaleza, características y origen de su comportamiento, sin perder de vista la relación, interdependencia e interacción de las partes entre sí y con el todo, y de éstas con su contexto (Franklin, 2007).

El propósito de esta etapa es aplicar las técnicas de análisis procedentes para lograr los fines propuestos con la oportunidad, extensión y profundidad que requiere el alcance sujeto a examen y las circunstancias específicas del trabajo a fin de reunir los elementos de decisión óptimos (Franklin, 2007).

2.3.4.4 Informe

Una vez realizado el examen, es necesario preparar un informe, en el cual se consignen los resultados de la auditoría e identifique claramente el área, sistema, programa o proyecto auditado, el objeto de la revisión, la duración, alcance, recursos y métodos empleados (Franklin, 2007).

En virtud de que en este documento se señalan los hallazgos, así como las conclusiones y recomendaciones de la auditoría, es indispensable que brinde suficiente información respecto de la magnitud de los hallazgos y la frecuencia con que se presentan, en relación con el número de casos o transacciones revisadas en función de las operaciones que realiza la organización (Franklin, 2007).

Asimismo, es importante que tanto los hallazgos como las recomendaciones estén sustentados por evidencia suficiente y relevante, debidamente documentada en los papeles de trabajo del auditor.

2.3.4.5 Seguimiento

En esta etapa las observaciones que se producen como resultado de la auditoría deben sujetarse a un estricto seguimiento, ya que no solo se orientan a corregir las fallas detectadas, sino también a evitar su recurrencia (Franklin, 2007).

En el capítulo Marco metodológico se indicará como se utilizará esta metodología en el manual.

2.4 Auditoría de Tecnologías de Información

En este apartado se abarcan los conceptos enfocados al área de tecnología de información, con el fin de asociar su definición y aplicación al manual por plantear. En la literatura también se le conoce como auditoría informática.

Se inicia con la explicación de Echenique en su libro Auditoría Informática, el cual menciona: “La auditoría informática es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente […]” (Echenique, 2001, pág. 18).

Por su parte, Ron Weber indica: “es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente” (Echenique, 2001, pág. 17).

El manual por realizar está enfocado en explicar el ciclo de auditoría de TI, además como parte del trabajo final de graduación, se proponen mejoras tanto a las pruebas como a las fases de la auditoría según lo investigado.

2.4.1 Tecnología de información

La tecnología de información se ha convertido en uno de los activos más relevantes en las organizaciones, ya sea con fines de lucro o de bien social, es debida a esa importancia que debe ser revisada periódicamente por medio de exámenes de auditoría que aseguren a la administración que ella está siendo utilizada de manera correcta y adecuada y que está contribuyendo en el logro de las metas y objetivos de la entidad (Espinoza, 2009).

2.5 Fuentes de información aplicables a auditoría de TI

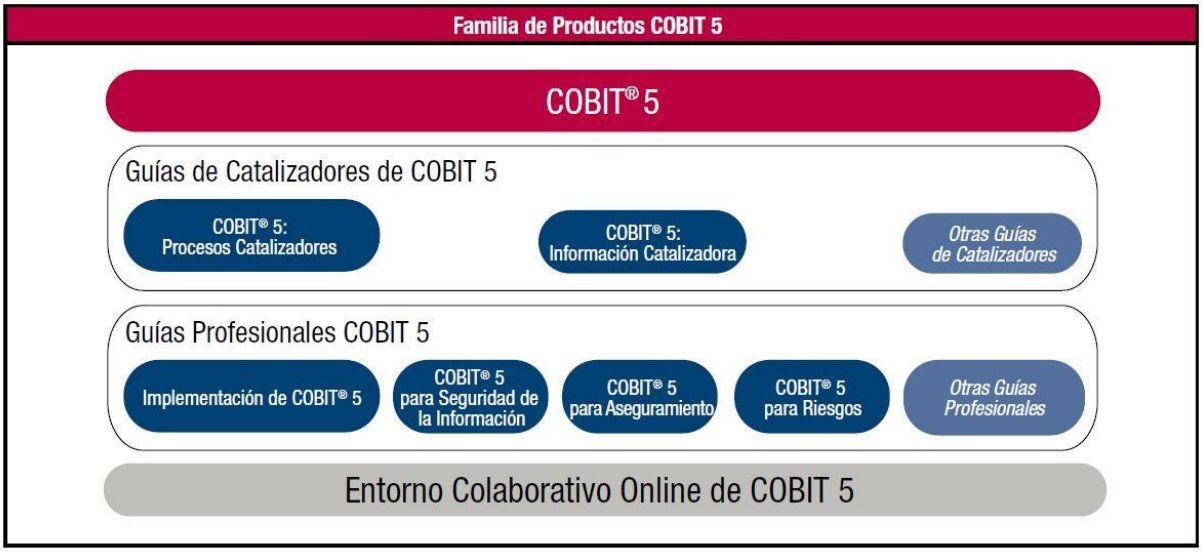
En este apartado se pretende definir las principales fuentes de información que son tomadas como las mejores prácticas a la hora de realizar una auditoría de TI, estas fuentes también serán utilizadas para explicar los temas desarrollados dentro del manual.

- Normas: según define la legislación española (Ley 21/1992), es “una especificación técnica de aplicación repetitiva o continuada, cuya observancia no es obligatoria, establecida con la participación de todas las partes interesadas, que aprueba un organismo reconocido a nivel nacional o internacional” (AENOR, 2009).
- Reglamentos: pueden exigir el cumplimiento de los requisitos definidos en una o varias normas. Es en este caso cuando la norma pasa a ser de obligado cumplimiento para las organizaciones afectadas (AENOR, 2009).
- Buenas prácticas: se entiende un conjunto coherente de acciones que han rendido buen o incluso excelente servicio en un determinado contexto y que se espera que, en contextos similares, rindan similares resultados (AENOR, 2009).

2.5.1 *COBIT*

COBIT 5 proporciona la guía de nueva generación de *ISACA* para el gobierno y la gestión de las TI en la empresa, como se muestra en la Figura 2.3. Se construye sobre más de 15 años de uso práctico y aplicación de *COBIT* por parte de muchas empresas y usuarios de las comunidades de negocio, TI, riesgo, seguridad y aseguramiento (ISACA, 2012, pág. 15).

Figura 2.3 Familia de Productos COBIT 5



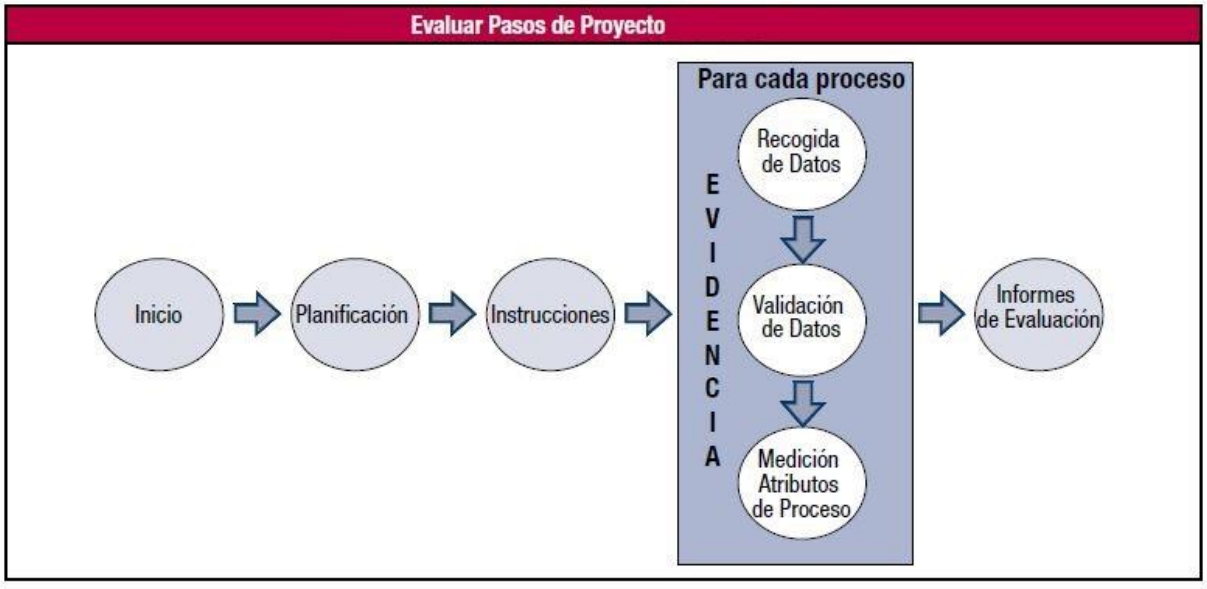
Fuente: *COBIT* 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa (2012, pág. 11).

2.5.1.1 Programa de Evaluación de *COBIT*

El propósito principal de esta guía es ofrecer una orientación a los asesores de cómo llevar a cabo una evaluación, está compuesta por siete pasos claves los cuales se pueden observar en la Figura 2.4 y, seguidamente, se procede a dar una breve explicación de cada paso, ya que serán considerados en el análisis de resultados para poder contrastar estos pasos contra las actividades realizadas actualmente dentro del ciclo de auditoría de TI.

Está diseñada para ofrecer a las empresas una metodología entendible, lógica, repetible, fiable y robusta para la evaluación de la capacidad de sus procesos de TI, basados en el Modelo de Referencia de Procesos de *COBIT* 5 (PRM). Dicha evaluación puede ser utilizada como informe interno para la dirección ejecutiva de la empresa o el comité ejecutivo sobre la capacidad de sus procesos de TI, a fin de establecer un objetivo para la mejora con base a los requerimientos del negocio (ISACA, 2013).

Figura 2.4 Programa de evaluación *COBIT* 5



Fuente: *COBIT* Guía del Evaluador: Usando *COBIT* 5 (2013, pág. 23).

Se procede a indicar los pasos que componen el programa de evaluación de *COBIT* 5.

Iniciación

La etapa de iniciación consiste en confirmar el patrocinador y asegurar que hay acuerdo sobre el objeto y alcance de la evaluación. Este paso también implicará la identificación de cualquier limitación, realizar la planificación inicial de la evaluación (incluyendo cualquier información adicional que precise ser recogida), la elección de los participantes en la evaluación y el equipo completo de evaluación y la definición de los roles de los miembros del equipo (COBIT Guía del Evaluador: Usando COBIT 5, 2013, pág. 24).

Planificación

Planificar la evaluación incorpora el desarrollo de un plan que describe todas las actividades realizadas para recoger evidencia y guiar la evaluación (COBIT Guía del Evaluador: Usando COBIT 5, 2013, pág. 27).

Instrucciones

El líder del equipo de evaluación se tiene que asegurar, antes que tenga lugar la recolección de datos, que el equipo de evaluación entiende tanto el proceso de evaluación como sus motivaciones y resultados. Así mismo, también se tendría que informar a las personas de la empresa que se deberían consultar durante la evaluación, sobre cómo se llevará a cabo dicha evaluación (COBIT Guía del Evaluador: Usando COBIT 5, 2013, pág. 28).

Recolección de datos

La recolección de datos consiste en la obtención de evidencias objetivas para soportar la evaluación de los procesos seleccionados para la evaluación. La estrategia para la recolección se debería desarrollar y aprobar durante la etapa de planificación de la evaluación (COBIT Guía del Evaluador: Usando COBIT 5, 2013, pág. 29).

Validación de datos

La validación de datos significa confirmar que las evidencias reunidas son objetivas y suficientes para cubrir el alcance y propósito de la evaluación, y que los datos en su conjunto son consistentes. (COBIT Guía del Evaluador: Usando COBIT 5, 2013, pág. 30).

Medición atributos de proceso

Para cada proceso evaluado, se asigna una calificación a cada atributo de proceso hasta como máximo el nivel de capacidad más alto definido en el alcance de la evaluación (COBIT Guía del Evaluador: Usando COBIT 5, 2013, pág. 31).

Informes de evaluación

Los informes de evaluación son un paso muy importante. Durante esta fase, los resultados de la evaluación se analizan y presentan al patrocinador (sponsor) y otras partes interesadas, según proceda (COBIT Guía del Evaluador: Usando COBIT 5, 2013, pág. 32).

2.5.1.2 Procesos catalizadores

Este material contiene una guía de referencia detallada de los procesos que están definidos en el modelo de procesos de referencia de *COBIT*, los cuales se pueden observar en Anexo 4: Procesos de *COBIT* 5.

COBIT 5 se toma como fuente principal del proyecto, ya que la normativa actual, SUGEF 14-17, está basada en 34 procesos de los 37 que contempla *COBIT* 5, las normas técnicas también se pueden asociar con *COBIT 5*, en el Apéndice E: Temas por explicarse puede observar su relación.

2.5.1.3 Guías profesionales de *COBIT 5*

COBIT 5 contiene una serie de guías profesionales, las cuales sirven de complemento para el estudio y aplicación de este marco de referencia, a continuación, se procede a mencionar las cuatro guías principales.

2.5.1.3.1 Implementación de *COBIT 5*

El objetivo de esta guía de referencia es proveer un enfoque de buenas prácticas a la hora de implementar el gobierno corporativo de TI, basado en un ciclo de vida de mejora continua que debe adaptarse a las necesidades específicas de la empresa (ISACA, 2012).

2.5.1.3.2 *COBIT* 5 para Seguridad de la Información

Se enfoca en la seguridad de la información y 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 (ISACA, 2012).

2.5.1.3.3 *COBIT* 5 para Aseguramiento

Se enfoca en el aseguramiento y proporciona una guía más detallada y práctica para los profesionales de aseguramiento y otras partes interesadas a todos los niveles de la empresa sobre cómo utilizar COBIT 5 para apoyar varias actividades de aseguramiento de TI (ISACA, 2013).

2.5.1.3.4 *COBIT* 5 para Riesgos

Se centra en el riesgo y proporciona una orientación más detallada y práctica a los profesionales de riesgo y otras partes interesadas en cualquier nivel de la empresa (ISACA, 2013).

2.5.2 *ITIL*

La Biblioteca de Infraestructura de Tecnologías de Información es conocida por sus siglas como ITIL (*Information Technology Infrastructure Library*). Será una de las fuentes principales para la explicación de los temas abarcados en el manual.

ITIL surgió en la década de 1980, la Agencia Central de Telecomunicaciones del gobierno británico, recibió el encargo de desarrollar una metodología estándar para garantizar una entrega eficaz y eficiente de los servicios de TI. El resultado fue el desarrollo de la Biblioteca de Infraestructura de Tecnologías de Información, la cual está formada por una serie de mejores prácticas procedentes de los suministradores de servicios de TI (Van Bon & Redwood, 2010).

2.5.2.1 Buenas prácticas

Una buena práctica es planteamiento o método que ha demostrado su validez en la práctica. Las buenas prácticas se utilizan como un respaldo sólido de las organizaciones que desean mejorar sus servicios de TI (Bon, y otros, 2008).

Al ser *ITIL* aceptado por la industria como conjunto de buenas prácticas para la gestión de TI, es considerado en el proyecto como fuente de información primaria para la elaboración del manual.

2.5.2.2 Gestión del servicio

Es un conjunto de capacidades organizativas especializadas cuyo fin es generar valor para los clientes en forma de servicio (Cannon, Wheeldon, Lacy, & Hanna, 2013).

2.5.2.2.1 Servicio

Es un medio para entregar valor a los clientes, facilitando los resultados que los clientes quieren conseguir sin asumir costos o riesgos específicos (Cannon, Wheeldon, Lacy, & Hanna, 2013).

El ciclo de vida del servicio, según *ITIL*, consta de cinco fases. Cada volumen de los libros de *ITIL* describe una de estas fases. Se puede observar en la Figura 2.5.

Figura 2.5 Ciclo de vida del servicio según ITIL

Fuente: Fundamentos de ITIL® V3 (2010, pág. 19).

2.5.2.3 Ciclo de vida del servicio

A continuación, se procede a indicar en la siguiente página, las fases del ciclo de vida del servicio según *ITIL.*

2.5.2.3.1 Estrategia del servicio

La fase de estrategia desarrolla e implementa la gestión del servicio como un recurso estratégico. La estrategia del servicio proporciona directrices para el diseño, desarrollo e implantación de la gestión del servicio como recurso estratégico (Bon, y otros, 2008).

El objetivo de la estrategia del servicio es identificar la competencia y competir con ella diferenciándose de los demás y ofreciendo un mejor rendimiento (Cannon, Wheeldon, Lacy, & Hanna, 2013).

Procesos de la estrategia del servicio.

Se procede a indicar los procesos contemplados dentro de esta fase y una breve descripción:

- **Gestión financiera:** Es un componente integral de la gestión del servicio. Anticipa la información de gestión, en términos financieros, necesaria para garantizar una prestación eficiente y rentable del servicio.

- **Gestión de la demanda:** Es un aspecto esencial de la gestión del servicio, ya que armoniza la oferta con la demanda. El objetivo de la gestión de la demanda es predecir con la máxima precisión la compra de productos y equilibrar la demanda y los recursos.

- **Gestión de la cartera de servicios:** Es un método que permite gestionar todas las inversiones en gestión de la cartera de servicios en términos de valor para el negocio.

2.5.2.3.2 Diseño del servicio

Diseño del servicio se ocupa del diseño y desarrollo de servicios y sus procesos relacionados, la fase del diseño del servicio inicia con la demanda de requisitos nuevos o modificados por parte de un cliente (Hunnebeck, 2013).

Procesos de diseño del servicio

Se procede a indicar los procesos contemplados dentro de esta fase y una breve descripción:

- **Gestión del catálogo de servicios:** El objetivo general de la gestión del catálogo de servicios es el desarrollo y mantenimiento de un catálogo que incluya todos los datos precisos y estado de los servicios existentes, además de los procesos de negocio a los que apoyan, también los que están en desarrollo.

- **Gestión del nivel de servicio:** El objetivo general de este proceso es garantizar que se cumplen los niveles de provisión de los servicios de TI, incluye los existentes y los servicios futuros, tomando en cuenta los objetivos acordados.

- **Gestión de la capacidad:** El objetivo general de este proceso es garantizar que la capacidad corresponde con las necesidades presentes y futuras de la organización.

- **Gestión de la disponibilidad:** El objetivo de este proceso es garantizar que los niveles de disponibilidad de los servicios corresponden con los niveles acordados.

- **Gestión de la continuidad de los servicios de TI:** El objetivo general es facilitar la continuidad del negocio, garantizando la recuperación de las instalaciones y servicios necesarios en un tiempo acordado.

- **Gestión de la seguridad de la información:** La gestión de la seguridad de la información garantiza que la política de seguridad de la información abarca los requisitos generales de la organización, incluyendo los que tienen su origen desde el gobierno corporativo.

- **Gestión de proveedores: La** gestión de proveedores se centra en los proveedores y contratos para facilitar el acceso de servicios a los clientes.

2.5.2.3.3 Transición del servicio

El propósito de esta fase del ciclo de vida del servicio es garantizar que los servicios nuevos, modificados o retirados cumplan con las expectativas del negocio, tal como se documenta en las etapas de estrategia de servicio y diseño del servicio del ciclo de vida (Rance, Rudd, Lacy, & Hanna, 2013).

Procesos de diseño del servicio.

Se procede a indicar los procesos contemplados dentro de esta fase y una breve descripción:

- **Planificación de la transición y soporte:** El propósito del proceso de planificación y soporte de la transición es proporcionar una planificación general para las transiciones del servicio y coordinar los recursos que requieren.

- **Gestión de la configuración y de activos del servicio:** El propósito de este proceso es garantizar que los activos requeridos para entregar los servicios estén controlados adecuadamente, y que la información precisa y confiable sobre esos activos esté disponible cuándo y dónde sea necesaria. Esta información incluye detalles de cómo se han configurado los activos y las relaciones entre los activos.

- **Gestión de cambios:** Asegura la utilización de procedimientos estandarizados para la gestión eficiente de todos los cambios, para minimizar su impacto en la calidad del servicio y mejorar la operación diaria de la organización.

- **Gestión de liberación e implementación:** Es el proceso responsable de la planificación, programación y control de la construcción, prueba e implementación de liberaciones y de proporcionar nuevas funcionalidades que son requeridas por el negocio al tiempo que protege la integridad de los servicios existentes.

- **Gestión del conocimiento:** Asegurar que la información correcta sea entregada en el lugar apropiado o a la persona adecuada en el tiempo correcto para la toma de decisiones informadas.

2.5.2.3.4 Operación del servicio

El propósito de esta fase es coordinar y llevar a cabo actividades y procesos requeridos para la entrega y gestión de servicios a los niveles acordados para el negocio y los usuarios.

Procesos de operación del servicio

Se procede a indicar los procesos contemplados dentro de esta fase y una breve descripción.

- **Gestión de eventos:** Es responsable de monitorizar todos los eventos que acontezcan en la infraestructura TI con el objetivo de asegurar su correcto funcionamiento y ayudar a prever incidencias futuras.

- **Gestión de incidentes:** Esta gestión es la responsable de registrar todas las incidencias que afecten a la calidad del servicio y restaurarlo a los niveles acordados de calidad en el más breve plazo posible.

- **Petición de Servicios TI o cumplimiento de solicitudes:** Es la gestión responsable de gestionar las peticiones de usuarios y clientes que habitualmente requieren pequeños cambios en la prestación del servicio.

- **Gestión de problemas:** Es responsable de analizar y ofrecer soluciones a aquellos incidentes que por su frecuencia o impacto degradan la calidad del servicio.

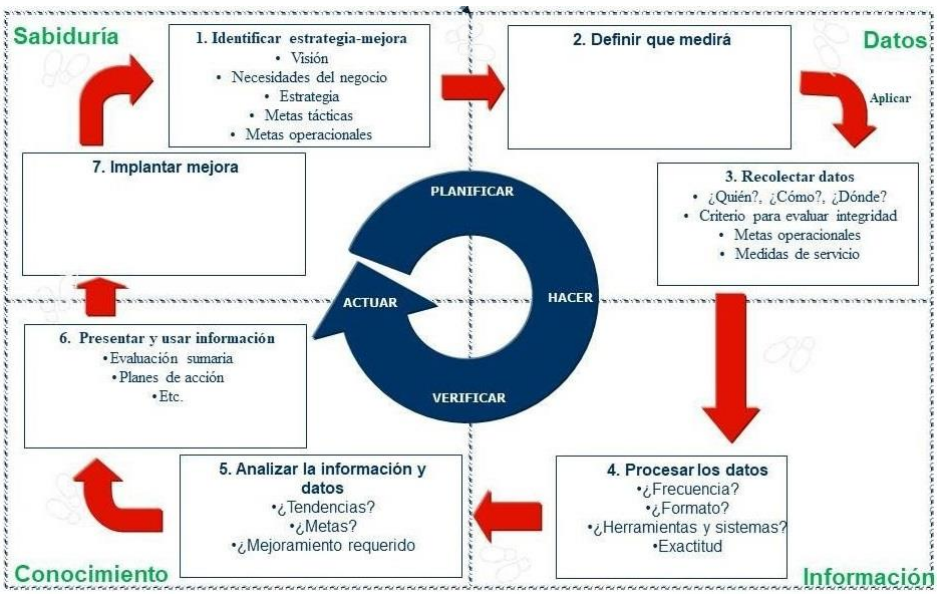
- **Gestión de Acceso a los Servicios TI** La gestión de acceso es el proceso de otorgar a los usuarios autorizados el derecho de utilizar un servicio, al tiempo que impide el acceso a usuarios no autorizados. También se lo conoce como gestión de derechos o gestión de identidades en diferentes organizaciones.

- **Centro de servicio al usuario (*Service Desk*)** Es un único punto de contacto para los usuarios en su comunicación con el proveedor de servicio. Es una función de esta etapa.

2.5.2.3.5 Mejora continua del servicio

Proporciona una guía que sigue los pasos de la Figura 2.6, para el enfoque en la identificación e implementación de mejoras en los servicios de TI (Lloyd, Wheeldon, Lacy, & Hanna, 2013).

Figura 2.6 7 Pasos de mejora continua



Fuente: Fundamentos de ITIL® V3 (2010).

2.5.2.3.5.1 Objetivos

Se procede a indicar los objetivos de la fase de mejora continua del servicio (Lloyd, Wheeldon, Lacy, & Hanna, 2013):

- Gestionar el proceso para la mejora continua.
- Revisar, analizar, evaluar y soportar las actividades de mejora.
- Identificar oportunidades de mejora.
- Mejorar los servicios de TI en calidad, costo y efectividad.

En la Figura 2.7 se puede observar un resumen de las cinco etapas del ciclo de vida de los servicios en ITIL v3 y sus respectivos procesos.

Figura 2.7 Contenido de las etapas del ciclo de vida de los servicios en ITIL v3

Fuente: ISO/IEC 20000. Guía completa de aplicación para la gestión de los servicios de tecnologías de la información (2009, pág. 42).

2.5.3 *ISO*

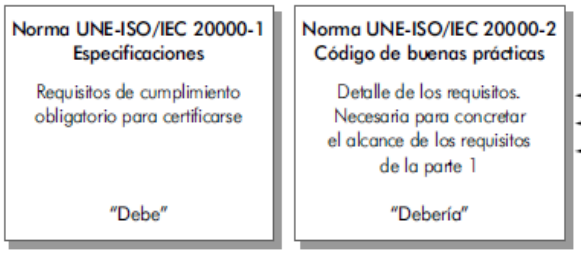
ISO (*International Organization for Standardization,* Organización Internacional de Normalización) es el organismo de normalización oficial reconocido a nivel internacional. Su objetivo es poner a disposición de la industria un catálogo de normas sobre productos y servicios que se puedan utilizar para dar garantía de unos niveles de calidad preestablecidos. Fue creado en febrero de 1947 y tiene su sede en Ginebra. Cuenta en la actualidad con la representación de 153 países. Tiene como objetivo lograr la coordinación internacional y la unificación de las normas de la industria. Coopera estrechamente con la Comisión Electrotécnica Internacional o por sus siglas en ingles IEC (AENOR, 2009).

2.5.3.1 *ISO* 20000

La serie de Normas *ISO*/IEC 20000 es el primer conjunto de normativa internacional específica para la gestión de los servicios basados en las Tecnologías de la Información. Presentan una organización cabal de las principales actividades necesarias para gestionar estos servicios, agrupadas en un conjunto de procesos considerados esenciales para la creación, prestación y evolución de los servicios de las TI (AENOR, 2009).

Las Normas *ISO*/IEC 20000 se componen de dos partes, tal como se muestra en la Figura 2.8, la primera es la especificación para la gestión del servicio y tiene un carácter preceptivo, y la segunda se establece como un código de buenas prácticas o recomendaciones. Ambas partes forman un marco para definir las características de los procesos implicados en la gestión del servicio (AENOR, 2009).

Figura 2.8 Composición norma *ISO* 20000

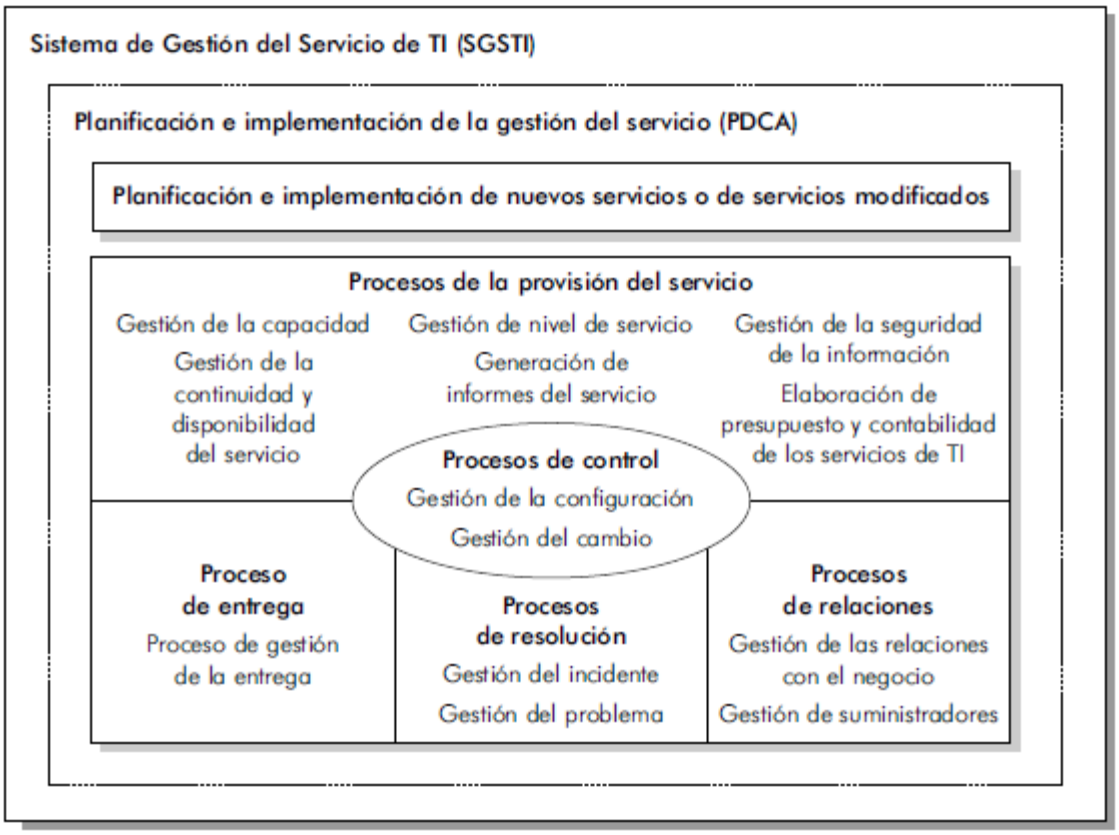


Fuente: ISO/IEC 20000 (2009, pág. 54).

2.5.3.1.1 Estructura de la ISO 20000

En la Figura 2.9 se observan los componentes de la ISO 20000, los cuales serán contemplados como una fuente de información para la explicación de las pruebas de auditoría.

Figura 2.9 Estructura de la ISO 20000



Fuente: ISO/IEC 20000 (2009, pág. 72).

2.5.3.2 ISO 27002 Controles de seguridad

ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios (Iso27000.es, 2005).

2.5.3.3 *ISO* 19011 Directrices para la auditoría de Sistemas de Gestión

La *ISO* 19011 no establece requisitos, sino que provee una guía sobre el manejo de un programa de auditoría, sobre la planeación y realización de una auditoría a un sistema de gestión, así como sobre la competencia y evaluación de un auditor que pertenezca al equipo auditor (ISO, 2011).

Si bien es cierto el manual no se enfoca en la parte de evaluación del auditor, él debería conocer cómo van a medir su trabajo realizado. La *ISO* 19011 y la metodología de auditoría administrativa serán fuentes primarias para respaldar el ciclo de auditoría dentro del despacho.

2.5.3.4 *ISO* 10007 Sistemas de gestión de la calidad. Directrices para la gestión de la configuración

El propósito de esta norma internacional es mejorar la comprensión común sobre el tema de gestión de la configuración, para promover su aplicación y ayudar a las organizaciones que la aplican a mejorar su desempeño (ISO, 2003).

La gestión de la configuración es una actividad de gestión que aplica la dirección técnica y administrativa a todo el ciclo de vida del producto, sus elementos de configuración y la información relacionada con la configuración del producto (ISO, 2003).

2.6 Normativa de TI

Para este apartado, se tomarán en cuenta dos sectores, el sector público, el cual se encuentra regulado por la Contraloría General de la República y el sector financiero, el cual se encuentra regulado por la SUGEF, en este sector también se abarcan las organizaciones cubierta por CONASIFF, el cual supervisa a la SUGEF, SUGEVAL, SUPEN y SUGESE.

La estructura del Consejo Nacional de Supervisión del Sistema Financiero se puede observar en la Figura 2.10.

Figura 2.10 Estructura CONASSIF

Fuente: Consejo Nacional de Supervisión del Sistema Financiero (2010).

2.6.1 Normas técnicas para la gestión y el control de las Tecnologías de Información

Las “Normas técnicas para la gestión y el control de las tecnologías de información”, normativa que establece los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto del Estado (Contraloría General de la República, 2007).

2.6.2 SUGEF 14-17 Reglamento general de gestión de la tecnología de información

Este reglamento establece los requerimientos mínimos para la gestión de la tecnología de información que deben acatar las entidades supervisadas y reguladas del sistema financiero costarricense (SUGEF, 2017).

2.7 Administración de procesos de negocio

En este apartado se procede a explicar cómo se utilizará la administración de procesos de negocio (BPM), en especial la notación y modelaje de procesos de negocio (BPMN), para la representación de los procedimientos explicados en el manual propuesto, pues se puede obtener una notación gráfica estandarizada que permite el modelado de procesos de negocio, en un formato de flujo de trabajo, facilitando la comprensión para los lectores (Hitpass, 2017).

2.7.1 Elementos de BPMN

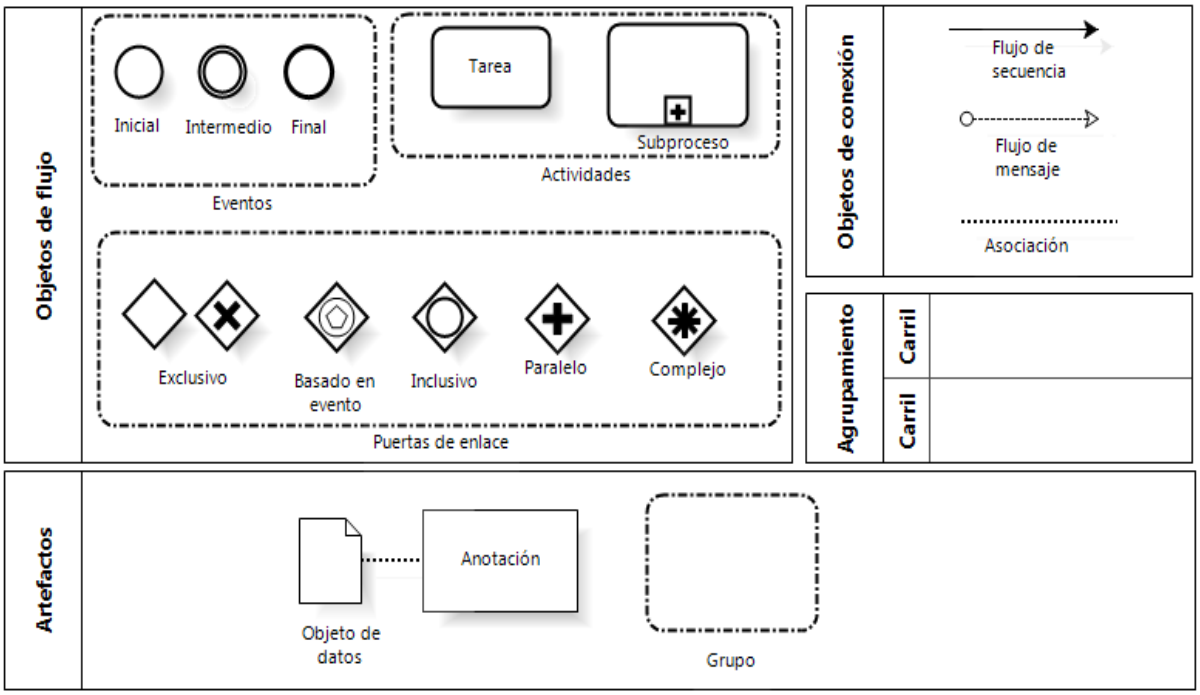
A continuación, se procede a explicar los elementos de BPMN que serán utilizados en este proyecto.

- Actividad: Representa las tareas principales que deberá realizar el equipo de auditoría.
- Evento: Se utilizará para representar los eventos de inicio y fin de los procedimientos, para facilitar su comprensión.
- Puertas de enlace*:* Se utilizará la puerta de enlace XOR o exclusiva, el cual indica que se debe seguir sólo un camino de los caminos posibles.
- Flujo de secuencia: Describe la secuencia temporal y lógica en el cual se combinan los elementos de flujo, actividades, eventos y puertas de enlace, guiara al auditor de TI en el orden que se debe seguir en el momento de realizar los diferentes procedimientos representados en el manual.
- Carril*:* Usado para organizar y categorizar las actividades dentro de un *pool* de acuerdo con su función o rol.
- Agrupamiento *(Pool)*: Representa los participantes principales de un proceso.

Se procede a mencionar los elementos que conformar BPMN en la Figura 2.11, la cual se encuentra disponible en la siguiente página.

A continuación, se indican los elementos de BPMN en la Figura 2.11, no obstante, se utilizarán solo los elementos explicados en la página anterior.

Figura 2.11 Elementos de BPMN



Fuente: Modelado de Negocios: BPMN (Business Process Modeling Notation), (2012).

Capítulo III

Marco Metodológico

3. Marco metodológico

En este capítulo se muestra la manera en que se abordará cada fase de la metodología propuesta, así como el tipo de investigación, diseño, fuentes de información, técnicas de recopilación de información y los instrumentos de investigación utilizados.

Para el desarrollo de la propuesta planteada se requiere una serie de pasos de investigación. En el capítulo actual, se presenta el enfoque metodológico que será utilizado para desarrollar cada una de las cuatro fases que componen la metodología de trabajo, empezando por el análisis de la situación actual, revisión de las mejores prácticas, diseño de los procedimientos de las pruebas con su respectiva explicación, y para finalizar la elaboración del manual, el cual incluye aspectos de mejoras en el ciclo de auditoría.

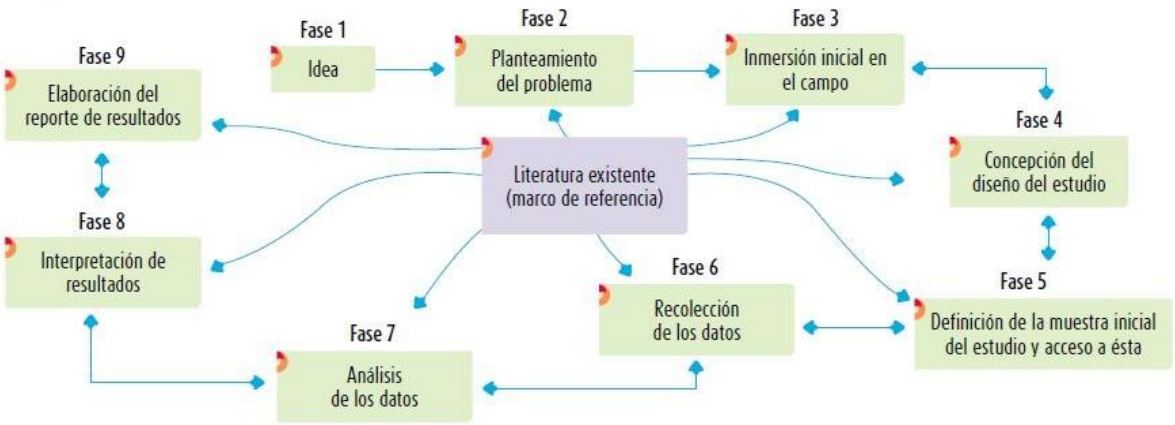
Es importante tener presente los marcos de referencia para el proyecto y cómo se combinarán con el propósito de facilitar el aprendizaje a los lectores del manual propuesto.

Para la explicación de las pruebas, las fuentes principales son ITIL e ISO 20000, en caso de que el tema abarcado tenga una fuente específica se indicara en el material complementario de cada prueba. Para la definición de los atributos de las pruebas la referencia es *COBIT* 5 y la normativa aplicable para TI y, por último, para abarcar el ciclo de auditoría se toma como referencia la ISO 19011 y la metodología mencionada en el apartado 2.3.4 Metodología de la auditoría administrativa, cada una de estas fuentes será explicada en el presente capítulo.

3.1 Tipo de investigación

Para la presente investigación se utilizó un modelo cualitativo, debido a que se enfoca en comprender los fenómenos desde la perspectiva de los participantes, en este caso el equipo de auditoría de TI, en un ambiente natural, el cual sería la aplicación de las auditorías y su relación con el contexto (Hernández et al., 2014).

Figura 3.1 Proceso cualitativo



Fuente: Metodología de la investigación (2014, pág. 7).

Para comprender la Figura 3.1 es necesario tomar en cuenta los siguientes aspectos (Hernández et al., 2014):

- Ciertamente dentro de la metodología hay una fase de revisión inicial de la literatura, la cual se puede complementar en cualquier etapa del estudio y apoyar desde el planteamiento del problema hasta la elaboración de los resultados encontrados.
- En la investigación cualitativa en ocasiones es necesario regresar a etapas previas. Por ello, las flechas de las fases que van de la inmersión inicial en el campo hasta el reporte de resultados se visualizan en dos sentidos.
- La inmersión inicial en el campo significa sensibilizarse con el ambiente o entorno en el cual se llevará a cabo el estudio, identificar informantes que aporten datos y guíen al investigador por el lugar, adentrarse y compenetrarse con la situación de investigación, además de verificar la factibilidad del estudio.

- En el caso del proceso cualitativo, la muestra, la recolección y el análisis son fases que se realizan prácticamente de manera simultánea.

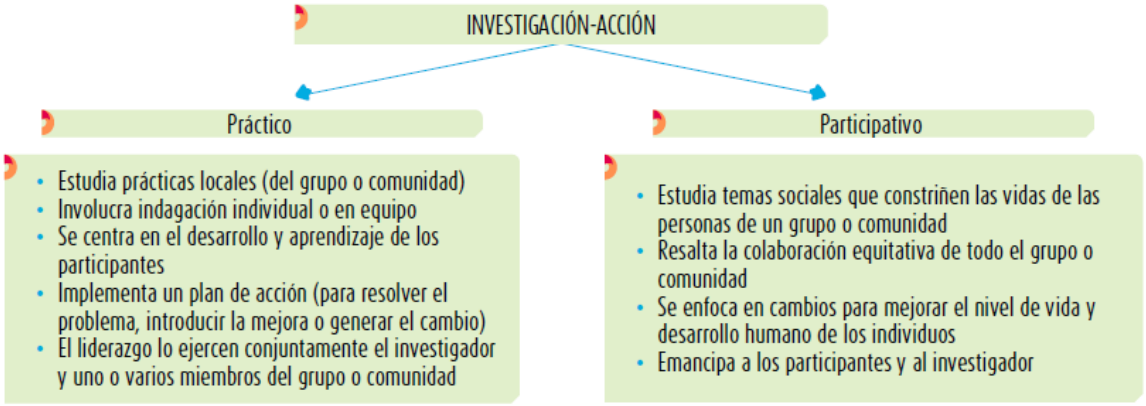
3.2 Diseño de la investigación

Definida la problemática del proyecto, se procede a determinar el diseño de la investigación, el diseño seleccionado es investigación-acción, ya que su finalidad es comprender y resolver problemáticas específicas de una colectividad vinculadas a un ambiente, en este caso vinculadas a una organización (Hernández et al., 2014).

Las tres fases esenciales de los diseños de investigación-acción son: observar (construir un bosquejo del problema y recolectar datos), pensar (analizar e interpretar) y actuar (resolver problemáticas e implementar mejoras), las cuales se dan de manera cíclica, una y otra vez, hasta que todo es resuelto, el cambio se logra o la mejora se introduce satisfactoriamente (Stringer, 1999).

Se consideran dos diseños fundamentales de la investigación-acción, los cuales se observan en la Figura 3.2, para este proyecto se seleccionó el enfoque práctico, ya que se estudian las prácticas del despacho respecto a la auditoría de TI. Y el plan de acción que se desea implementar es el manual de auditoría de TI.

Figura 3.2 Diseños básicos de la investigación-acción



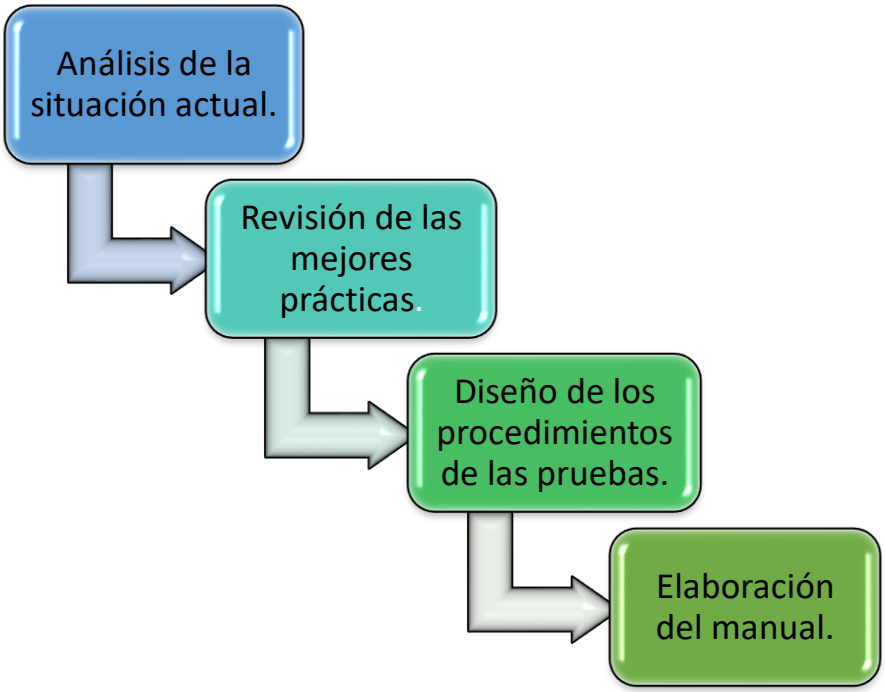
Fuente: Metodología de la investigación (2014, pág. 497).

3.3 Metodología de trabajo

Se ha establecido una metodología de trabajo tomando en cuenta el diseño de la investigación, se pueden observar sus fases en la Figura 1.7, las cuales serán necesarias para cumplir con lo estipulado en el apartado 1.4.2 Objetivos específicos.

Es importante recordar que debido al diseño y tipo de investigación las fases no son secuenciales, si bien es cierto se sigue el orden establecido, en las fases posteriores se puede regresar a las fases anteriores para validar los resultados obtenidos (Hernández et al., 2014).

Figura 1.7 Metodología de trabajo



Fuente: Elaboración propia.

A continuación, se procede a detallar las actividades realizadas en cada fase.

3.3.1 Análisis de la situación actual

Las actividades correspondientes a esta fase son las siguientes:

- Conocer y documentar el ciclo actual de auditoría.
- Investigar la normativa de TI aplicable para Costa Rica.
- Establecer las mejores prácticas según las necesidades del despacho.

3.3.2 Revisión de las mejores prácticas

Las actividades correspondientes a esta fase son las siguientes:

- Identificar los temas abarcados en las pruebas.
- Asociar a cada tema una o más mejores prácticas.
- Identificar los atributos actuales de cada tema seleccionado.

3.3.3 Diseño de los procedimientos de las pruebas

Las actividades correspondientes a esta fase son las siguientes:

- Establecer atributos por cada tema seleccionado tomando en cuenta las mejores prácticas asociadas.
- Contrastar los atributos actuales y los propuestos, solicitar la aprobación por parte del gerente del departamento.
- Explicar cada tema seleccionado para facilitar su comprensión.

3.3.4 Elaboración del manual

Las actividades correspondientes a esta fase son las siguientes:

- Documentar las fases de auditoría ya con sus respectivas mejoras basándose en la ISO 19011 y la metodología de auditoría administrativa.
- Completar los apartados establecidos en la Figura 1.3.
    - Explicar las herramientas actuales.
    - Integrar las fases anteriores.

3.4 Fuentes de información

Es importante incluir las fuentes de información consultadas, las cuales se separan en primarias, secundarias y los sujetos de información.

Las fuentes de información es cualquier escrito o testimonio gráfico o visual que proporciona datos sobre el tema que se está investigando. La información de primera mano es aquella que ha sido obtenida, organizada y formulada por el propio investigador y la información de segunda mano es la que se obtiene de las fuentes documentales que provienen de otras investigaciones (Martínez, 2012, pág. 135).

3.4.1 Fuentes primarias

A continuación, se procede a mencionar las fuentes primarias para realizar la investigación, las cuales serán consideradas a lo largo de la metodología de trabajo, estas fuentes proporcionan datos de primera necesidad, dentro de las cuales destacan libros, tesis, documentos oficiales, entre otros (Hernández et al., 2014).

Si se desea ver detalladamente todas las fuentes utilizadas en este trabajo se pueden observar en el apartado 8. Lista de referencias, no obstante, se procede a indicar las principales fuentes en la Tabla 3.1 y cómo se relacionan con el trabajo realizado.

Tabla 3.1 Fuentes de información primarias

Fuente	Área
Objetivos de Control para Información y Tecnologías Relacionadas (*COBIT* 5).	Controles de auditoría.
Information Technology Infrastructure Library (ITIL).	Gestión de procesos de TI.
ISO/IEC 20000.	Gestión de servicios de TI.
ISO/IEC 27000.	Estándares de Seguridad.

Fuente	Área
The Open Group Architecture Framework (TOGAF).	Arquitectura.
A Practical Guide to Information Systems Strategic Planning by Anita Cassidy.	Plan estratégico de TI.
Guía de los fundamentos para la dirección de proyectos. (Guía del PMBOK).	Administración de proyectos.
Gerente de TI (CISA).	Auditoría de TI.

Nota: Elaboración propia.

3.4.2 Fuentes secundarias

Las fuentes secundarias son compilaciones, resúmenes sobre un área particular, principalmente de documentos de fuentes primarias (Hernández et al., 2014). Estas fuentes se utilizaron principalmente para asociarlas con fuentes primarias, dónde se incluye artículos, páginas web y foros.

Se procede a enlistar las fuentes secundarias utilizadas:

- Foros y páginas de internet.
  - https://www.auditool.org/
  - https://www.segu-info.com.ar/foro/
  - http://www.portalcalidad.com/
- Biblioteca del Instituto Tecnológico de Costa Rica y su catálogo en línea (SIBITEC).
- Libros de auditoría informática.
- Normativa interna de países.
  - Chile.
  - Ecuador.
  - Colombia.
  - México.
  - España.
  - Costa Rica.

3.4.3 Sujetos de información

Parte de las fuentes de información, para recopilar información de la situación actual del proyecto planteado, son las personas que laboran actualmente en el Despacho, las cuales se presentan en la Tabla 3.2, específicamente en el departamento de TI, además brindaran retroalimentación de las propuestas planteadas.

Tabla 3.2 Sujetos de información

Rol	Descripción
Asistente de auditoría de TI	Son fuente de información para conocer la situación actual de las pruebas, cuáles son los atributos que actualmente se revisan por cada prueba, el procedimiento a seguir, las fuentes que consultan en caso de necesitar apoyo externo. Personal que tiene como función principal realizar pruebas de auditoría, licenciado de informática o tecnologías de información.
Encargado de auditoría de TI	Son fuentes de información para conocer el ciclo actual de auditoría, como se gestiona cada fase y cuáles son las actividades que se realizan. Personal con mínimo dos años de experiencia, realiza la planificación de la auditoría.
Gerente de auditoría de TI	Brinda orientación de como abarcar el trabajo final de graduación, además se encarga de aprobar las mejoras propuestas, incluyendo la explicación y el procedimiento de cada tema planteado. Dentro del departamento supervisa las actividades realizadas por los equipos de auditoría.

Nota: Elaboración propia.

3.5 Técnicas de recopilación de información

Seguidamente, se procede a indicar en la Tabla 3.3 las técnicas utilizadas para recopilar la información y la razón por la que se seleccionó, después en el siguiente apartado se muestran los instrumentos usados en la investigación.

Tabla 3.3 Técnicas de recopilación de información

Objetivo específico	Técnica
Analizar el proceso actual de capacitación en el departamento de auditoría y consultoría de TI del Despacho, para tomarlo como la base del proyecto.	• Entrevistas.
Comparar el ciclo de auditoría de TI, especialmente los procedimientos actuales de las pruebas de auditoría con las mejores prácticas de la industria de TI como lo es COBIT o ITIL, para contrastarlos y así proponer recomendaciones a los procesos actuales.	• Revisión documental. • Encuestas. • Fuentes primarias
Confeccionar los procedimientos de aplicación de las pruebas de auditoría de TI, para aplicarlos en los clientes del Despacho, además de apoyar el proceso de conocimiento y aprendizaje de los colaboradores.	• Revisión documental. • Reunión. • Fuentes primarias
Integrar los procedimientos creados con la explicación de cada una de las fases del ciclo de auditoría de TI en un manual de auditoría de TI, para el estudio y aplicación en su labor diaria.	• Entrevistas. • Reunión. • Revisión documental. • Fuentes primarias

Nota: Elaboración propia.

3.6 Instrumentos de investigación

Los instrumentos de investigación son aquellos que son utilizados en conjunto con las técnicas de obtención de información para adquirir los datos necesarios para el desarrollo del proyecto. En la Tabla 3.4 se muestra los instrumentos utilizados por objetivo.

Tabla 3.4 Instrumentos de investigación

Objetivo específico	Instrumento
Analizar el proceso actual de capacitación en el departamento de auditoría y consultoría de TI del Despacho, para tomarlo como la base del proyecto.	• Entrevista semi estructurada a un auditor de TI.
Comparar el ciclo de auditoría de TI, especialmente los procedimientos actuales de las pruebas de auditoría con las mejores prácticas de la industria de TI como lo es COBIT o ITIL, para contrastarlos y así proponer recomendaciones a los procesos actuales.	• Estudio pruebas anteriores. • Formulario *Google Form.* • Entrevista semi estructurada a encargado de TI. • Fuentes primarias.
Confeccionar los procedimientos de aplicación de las pruebas de auditoría de TI, para aplicarlos en los clientes del Despacho, además de apoyar el proceso de conocimiento y aprendizaje de los colaboradores.	• Reunión con el gerente de TI. • Apoyo de las fuentes primarias de información.
Integrar los procedimientos creados con la explicación de cada una de las fases del ciclo de auditoría de TI en un manual de auditoría de TI, para el estudio y aplicación en su labor diaria.	• Reunión con el gerente de TI para validación. • Apoyo de las fuentes primarias de información.

Nota: Elaboración propia.

3.7 Variables de estudio

A continuación, se procede a indicar las variables de estudio de este proyecto en la Tabla 3.5. Estas variables surgen de los objetivos específicos y constituyen las características por estudiar (Ulate Soto & Vargas Morúa, 2016, pág. 81).

Tabla 3.5 Variables de estudio

Objetivo específico	Variable de estudio
Analizar el proceso actual de capacitación en el departamento de auditoría y consultoría de TI del Despacho, para tomarlo como la base del proyecto.	• Proceso de capacitación de los auditores de TI dentro del despacho.
Comparar el ciclo de auditoría de TI, especialmente los procedimientos actuales de las pruebas de auditoría con las mejores prácticas de la industria de TI como lo es COBIT o ITIL, para contrastarlos y así proponer recomendaciones a los procesos actuales.	• Ciclo de auditoría de TI del despacho.
Confeccionar los procedimientos de aplicación de las pruebas de auditoría de TI, para aplicarlos en los clientes del Despacho, además de apoyar el proceso de conocimiento y aprendizaje de los colaboradores.	• Procedimientos estandarizados y alineados con las mejores prácticas.
Integrar los procedimientos creados con la explicación de cada una de las fases del ciclo de auditoría de TI en un manual de auditoría de TI, para el estudio y aplicación en su labor diaria.	• Ciclo de auditoría estandarizado y alineado con las mejores prácticas.

Nota: Elaboración propia.

3.8 Matriz de trazabilidad

Se procede a indicar la matriz de trazabilidad realizada en el marco metodológico, la cual resume los principales componentes utilizados en el trabajo final de graduación, indicada en la Tabla 3.6.

Tabla 3.6 Matriz de trazabilidad

Objetivo específico	Técnica	Instrumento	Variable de estudio
Analizar el proceso actual de capacitación en el departamento de auditoría y consultoría de TI del Despacho, para tomarlo como la base del proyecto.	• Entrevistas.	• Entrevista a un auditor de TI.	Proceso de capacitación de los auditores de TI dentro del despacho.
Comparar el ciclo de auditoría de TI, especialmente los procedimientos actuales de las pruebas de auditoría con las mejores prácticas de la industria de TI como lo es COBIT o ITIL, para contrastarlos y así proponer recomendaciones a los procesos actuales.	• Revisión documental. • Encuestas. • Fuentes primarias	• Estudio pruebas anteriores. • Formulario *Google Form.* • Entrevista encargada de TI. Fuentes primarias	Ciclo de auditoría de TI del despacho.
Confeccionar los procedimientos de aplicación de las pruebas de auditoría de TI, para aplicarlos en los clientes del Despacho, además de apoyar el proceso de conocimiento y aprendizaje de los colaboradores.	• Revisión documental. • Reunión. • Fuentes primarias	• Reunión con el gerente de TI. Apoyo de las fuentes primarias de información.	Procedimientos estandarizados y alineados con las mejores prácticas.
Integrar los procedimientos creados con la explicación de cada una de las fases del ciclo de auditoría de TI en un manual de auditoría de TI, para el estudio y aplicación en su labor diaria.	• Entrevistas. • Reunión. • Revisión documental. • Fuentes primarias	• Reunión con el gerente de TI para validación. Apoyo de las fuentes primarias de información.	Ciclo de auditoría estandarizado y alineado con las mejores prácticas.

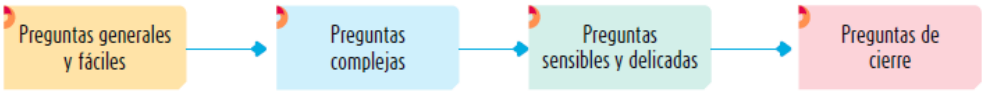
Nota: Elaboración propia.

3.9 Procedimiento y análisis de la información

Se procede a detallar cómo será el procedimiento para analizar la información tomando en cuenta el objetivo específico y la técnica de recopilación de información que se seleccionó en la Tabla 3.3.

- Analizar el proceso actual de capacitación en el departamento de auditoría y consultoría de TI del Despacho, para tomarlo como la base del proyecto.
    - Para conocer el ciclo actual de auditoría se realizará una entrevista semiestructurada, el formato para documentar la entrevista se puede observar en el Apéndice A: Formato de entrevistas, empezando de preguntas generales, después preguntas estructurales y, por último, las preguntas de cierre. De ser necesario se harán preguntas sensibles, sin embargo, no están consideradas en primera instancia, la secuencia de las preguntas se puede observar en la Figura 3.3. El objetivo principal de esta entrevista en lograr obtener las actividades de cada fase.

Figura 3.3 Orden de las preguntas en una entrevista cualitativa



Fuente: Metodología de la investigación (2014, pág. 405).

    - Para crear la estructura de la entrevista y seleccionar las preguntas guías, se tomará como referencia la ISO 19011 “Directrices para la auditoría de Sistemas de Gestión”, la cual propone un ciclo de auditoría dentro de su contenido, el mismo se puede observar en el Anexo 5: Flujo de proceso para la gestión de un programa de auditoría.
    - Para extraer los temas que se incluirán en el manual se tomará una muestra de cinco auditorías en las cuales se abarca una auditoría por cada sector de los más comunes en el despacho, como: municipalidades, asociaciones, bancos, operadoras de pensiones entre otras entidades del gobierno, el periodo considerado para estas auditorías es del primer

semestre del 2018, y para elegir las auditorías de cada sector se tomará el juicio de experto del encargado de auditoría, el cual tiene más de dos años de laborar para el despacho, las auditorías seleccionadas se pueden observar en el Anexo 6: Auditorías seleccionadas para identificar los temas del manual, seguidamente se crea un archivo de Excel para asociar cada tema con *COBIT* 5, las Normas Técnicas y el acuerdo SUGEF 14-17, el cual se puede apreciar en el Apéndice E: Temas por explicar, y por último para verificar que los temas sean correctos se realiza una reunión con el gerente de TI, con el fin de tener su aprobación de los temas seleccionados.

- Comparar el ciclo de auditoría de TI, especialmente los procedimientos actuales de las pruebas de auditoría con las mejores prácticas de la industria de TI como lo es *COBIT* o *ITIL*, para contrastarlos y así proponer recomendaciones a los procesos actuales.
    - Para hacer el análisis de los procedimientos actuales y poder contrastarlos con los procedimientos recomendados se utilizará una muestra de 10 auditorías, considerando las cinco anteriores para definir los temas y una más por cada sector, de igual forma, se le consultará al encargado de TI para seleccionar las auditorías del primer semestre del 2018, seguidamente, se procede a separar las pruebas de auditorías por cada tema seleccionado en la etapa anterior, después se extraen los atributos seleccionados y se procede a graficarlos, primeramente los gráficos permitirán observar la tendencia de los atributos seleccionados por cada prueba, después servirá de base para definir los atributos por considerar dentro del manual.

- Confeccionar los procedimientos de aplicación de las pruebas de auditoría de TI, para aplicarlos en los clientes del Despacho, además de apoyar el proceso de conocimiento y aprendizaje de los colaboradores.

  - Para confeccionar los procedimientos, primero se deben elegir los temas que abarcara el manual, para esto se utilizó una tabla dónde se asocian los temas sugeridos con las mejores prácticas y la normativa de Costa Rica para TI, después se procede a realizar una reunión con el gerente de TI para validarlos.
  - Seguidamente, se procede a combinar las mejores prácticas, normas y marcos de referencia, con el fin de brindar una explicación completa y de fácil comprensión para el lector del manual.

- Integrar los procedimientos creados con la explicación de cada una de las fases del ciclo de auditoría de TI en un manual de auditoría de TI, para el estudio y aplicación en su labor diaria.
  - Una vez que se tengan los procedimientos listos y las etapas documentadas, se procede a integrar la información en una propuesta del manual la cual se puede observar en el Apéndice L: Propuesta manual de auditoría de TI.

Con base en la metodología de trabajo descrita, las fuentes de información seleccionadas, las técnicas e instrumentos utilizados, se procederá a desarrollar el siguiente capítulo, en dónde se analizarán los resultados obtenidos.

Capítulo IV

Análisis de Resultados

4. Análisis de resultados

Para el capítulo de análisis de resultados se procede a explicar los resultados analizados por cada fase del ciclo de auditoría para facilitar su comprensión, además se puede observar el flujo del ciclo actual en el Apéndice D: Ciclo actual de auditoría.

4.1 Fase de planificación

A continuación, se procede a indicar las actividades realizadas actualmente dentro del despacho.

Como parte del análisis se hicieron las gestiones para obtener el proceso de auditoría actual, no obstante, no se cuenta con el mismo de forma explícita, ya que el gerente y los encargados si saben y comprenden las actividades que conforman el proceso de auditoría de TI.

Producto de la entrevista realizada con uno de los encargados de TI, se procede a extraer y describir las actividades, la entrevista se puede observar en el Apéndice B: Entrevista ciclo actual de auditoría.

Mercadeo

Si bien es cierto esta actividad no forma parte del ciclo de auditoría, si es importante completarla con éxito para poder iniciar una auditoría en los clientes. Por lo que se procederá a explicar en el manual de auditoría de TI.

Conocimiento de la organización y del área de tecnología de información

Una vez ganada la licitación o cerrado un trato con un cliente privado, se realiza una investigación rápida de la organización, a que se dedica, si ha sido cliente en periodos anteriores, dónde se ubican las oficinas, dónde se va a ubicar el equipo de trabajo, quién es el encargado del área tecnológica, ya que las auditorías por lo general son solicitadas por la junta directiva, entonces estos datos se desconocen.

Seguimiento de hallazgos y recomendaciones de informes de auditorías anteriores

Se solicitan los informes de periodos anteriores con el fin de ver su situación anterior. Se procede a verificar los hallazgos del periodo actual y si cada uno cuenta con su requerimiento inicial, en caso contrario, se procede a solicitar la información necesaria para evaluar la condición encontrada y determinar su estado actual.

Análisis y evaluación de la situación actual

Se evalúan los requerimientos actuales y su contexto en la organización, nuevos proyectos o administración.

Definición requerimientos iniciales periodo auditado

A partir de los informes anteriores y la situación actual se definen los requerimientos iniciales, con los cuales la auditoría empezaría a trabajar.

Plan de trabajo

El plan de trabajo es responsabilidad del encargado de la auditoría, para esto cuenta con dos asistentes, el cual definirá la forma de trabajar, definiendo los siguientes puntos:

- Pruebas: Cuáles pruebas se van a realizar, unificando requerimientos iniciales.
- Entrevistas: Tanto de los sistemas en producción como el centro de datos.
- Cronograma: Fechas límites tanto para los asistentes como para la entrega del informe actual.
- Responsables: Asigna quién va a realizar las pruebas y entrevistas.

Esta fase es contrastada con el estándar ISO 19011, ya que es la que más se adapta al proceso actual. El resumen de las fases para el programa de auditoría según la ISO 19011 se puede observar en la Figura 4.1, la cual se ubica en la siguiente página.

Figura 4.1 Resumen fases proceso para la gestión de un programa de auditoría

Fuente: Adaptado de ISO 19011 Directrices para la auditoría de Sistemas de Gestión, (2011).

La fase de planear está compuesta por dos actividades:

- Establecer los objetivos del programa de auditoría.
- Establecer el programa de auditoría.

Para la primera actividad, el gerente de TI determina el marco de gestión aplicable a la organización, los más comunes son las normas técnicas, el acuerdo SUGEF 14-17, COBIT 5 y la ISO 27002, no obstante, podría utilizarse otro según las necesidades de la organización, seguidamente se estudia los informes anteriores de auditoría externa y con base en estos elementos se procede a definir cuáles son los objetivos por abarcar en el proceso evaluado. Estos objetivos se traducen en requerimientos iniciales.

La segunda actividad de establecer el programa de auditoría se contrasta con la actividad documentada “Plan de trabajo”, en dónde se establecen las pruebas, entrevistas, cronograma y los responsables.

Por lo cual en el manual se procederá a establecer los procedimientos documentados, para estandarizar las tareas que se realizan en estas actividades.

Tomando en cuenta el programa de evaluación de la Figura 2.4, se asocia la fase de planificación con los primeros tres pasos del programa, que serían, inicio, planificación en instrucciones, ya que en el paso de inicio o iniciación se confirma el patrocinador en este caso las organizaciones, y se procede a establecer el alcance de la auditoría de TI y a elegir el equipo de la auditoría de TI.

En el caso del paso de planificación *COBIT* 5 menciona que se deben describir todas las actividades realizadas para obtener la evidencia y guiar la evaluación, en el despacho viene a hacer el plan de trabajo, dentro del cual se cuenta con pruebas para guiar la evaluación, no obstante, no se tiene documentado el procedimiento de estas.

Respecto al paso de instrucciones *COBIT* 5 hace énfasis a que el equipo de auditoría de TI debe entender el proceso de evaluación, y los resultados que se desean, para esto en el despacho el gerente de TI el primer día de la auditoría comenta con el equipo auditor cada uno de los requerimientos iniciales, que se evalúa y que se espera, además en caso de situaciones particulares de la organización también se comentan, para ser consideradas cuando se realicen las pruebas.

4.2 Fase de ejecución

Respecto a la fase de la ISO 19011, se encuentra la diferencia que en la ISO se establece el equipo de auditoría después de realizar el plan de trabajo, por otra parte, en el despacho primero se establece el equipo de auditoría y después el encargado establece el plan de trabajo.

El orden se mantendrá igual, ya que es un tema de gestión de recursos dentro del despacho, por lo cual la asignación de responsabilidades en el plan de trabajo dependerá del equipo asignado.

Se procede a indicar los resultados obtenidos en la fase de ejecución además en el apartado 4.2.1 Pruebas se profundiza el análisis de resultados por cada tema incluido en el manual.

4.2.1 Pruebas

Para el análisis de las pruebas se utilizaron varios instrumentos, primero se procedió a identificar cuáles son los temas que se van a abarcar en el manual, para lo cual se realizó un estudio por medio de una matriz para poder extraer los temas de los requerimientos, se utilizó una muestra de cinco auditorías efectuadas en el primer semestre del 2018, las cuales se pueden observar en el Anexo 6: Auditorías seleccionadas para identificar los temas del manual, con este análisis se está asegurando abarcar la normativa aplicable para TI dentro del manual. Al final se obtuvo un resultado de 30 temas indicados en el Apéndice E: Temas por explicar.

Seguidamente, se procede a crear un formulario con la herramienta *Google Form*, dónde se abarca los 30 temas del punto anterior, el formulario está compuesto por las siguientes preguntas para cada tema:

- ¿Ha realizado una prueba relacionada con el tema indicado?
- ¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?
- ¿A cuál fuente de información acudiría para realizar la prueba?

Para la última pregunta se debe responder que afirmativamente la segunda pregunta, esta pregunta ya tiene opciones cargadas como lo es *ITIL*, *COBIT*, Google, Encargado, no obstante, el colaborador puede agregar más fuentes en la opción de otros.

Los resultados del formulario se pueden observar en el Apéndice H: Encuestas de procesos, y serán comentados en el siguiente apartado según corresponda.

Por último, se hizo una revisión documental de 10 empresas, las cuales se pueden observar en el Apéndice G: Repositorio de pruebas, dónde se abarca 172 pruebas, en la revisión se hace un análisis de los atributos seleccionados para cada uno de los 30 temas identificados anteriormente.

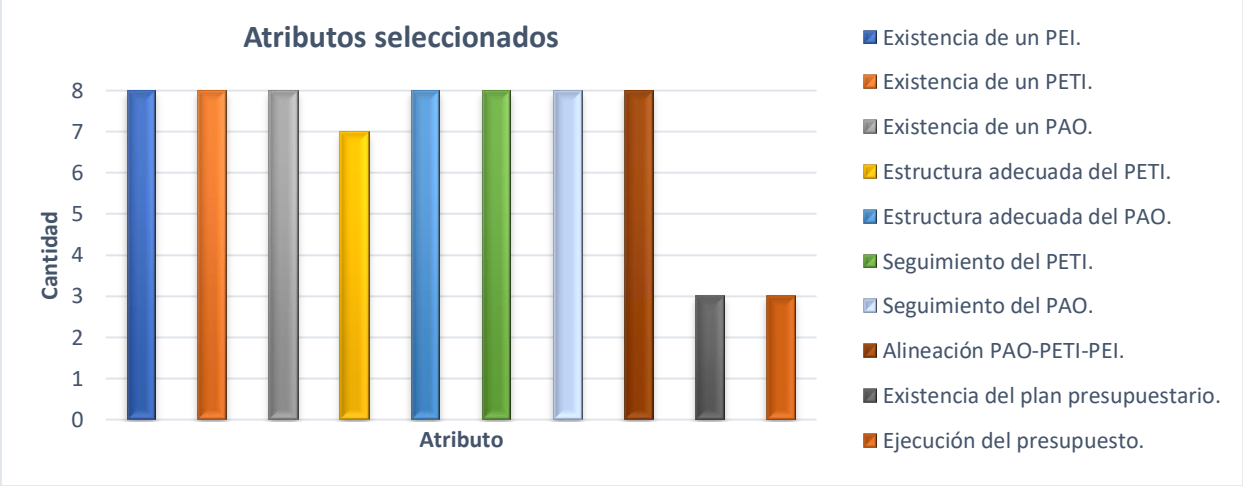
.

4.2.3.1 Gestión de la estrategia de TI

Es importante mencionar que el enfoque principal de este tema es la planificación estratégica de TI, a continuación, se presentan los resultados obtenidos sobre gestión de la estrategia de TI, de un total de cuatro personas que respondieron la encuesta, el 100% ha realizado una prueba relacionada con la estrategia de TI.

De las cuatro personas que han realizado una prueba relacionada con gestión de la estrategia de TI, tres personas acudirían a una fuente externa, que deja como resultado que solo el 25% realizaría la prueba con los conocimientos adquiridos.

Figura 4.2 Atributos seleccionados para la prueba del PETI



Fuente: Elaboración propia.

Para analizar los atributos seleccionados en la prueba del PETI, se recolectaron ocho pruebas, las cuales fueron realizadas por el equipo de auditoría, dando como resultado la escogencia de 10 atributos según se muestra en la Figura 4.2, dónde se observa que en una prueba no se revisó explícitamente la estructura del PETI.

Para las pruebas relacionadas con este tema, resalta *COBIT 5*, no obstante, se observa que dos personas consultarían en Google, estas personas también consultarían al encargado o gerente para realizar la prueba, según se muestra en el Apéndice H: Encuestas de procesos.

Un punto importante por mencionar es el atributo de la estructura del PETI, pues las fuentes anteriores no indican con exactitud cuál es una estructura aceptada, para así poder evaluarla.

Tampoco fue posible identificar en los documentos del despacho una estructura establecida como la esencial para ser contemplada en un PETI, por tal razón, en el manual se indicará cual es la estructura correcta para un PETI, basándose en el libro de (Cassidy, 2006), además de la explicación de los demás atributos. Esto permitirá a los auditores brindar puntos de mejoras para los planes estratégicos de TI actuales en las organizaciones.

Según la información consultada principalmente en el libro de (Cassidy, 2006), la estructura esencial de cualquier PETI es la siguiente:

- Misión, Visión y Valores de ATI.
- Mapa estratégico.
- Objetivos estratégicos.
- Alineamiento con las líneas estratégicas.
- Riesgos.
- Descripción marco arquitectura organizacional empresarial.
- Estructura organizacional.
- Factores críticos de éxito.
- Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) de TI.
- Cuadro de mando integral de TI.
- Catálogo de Proyectos vigente.
- Proyectos propuestos.
- Plan de TI.
- Resumen de costos.
- Impacto para el negocio.
- Plan de Comunicaciones.

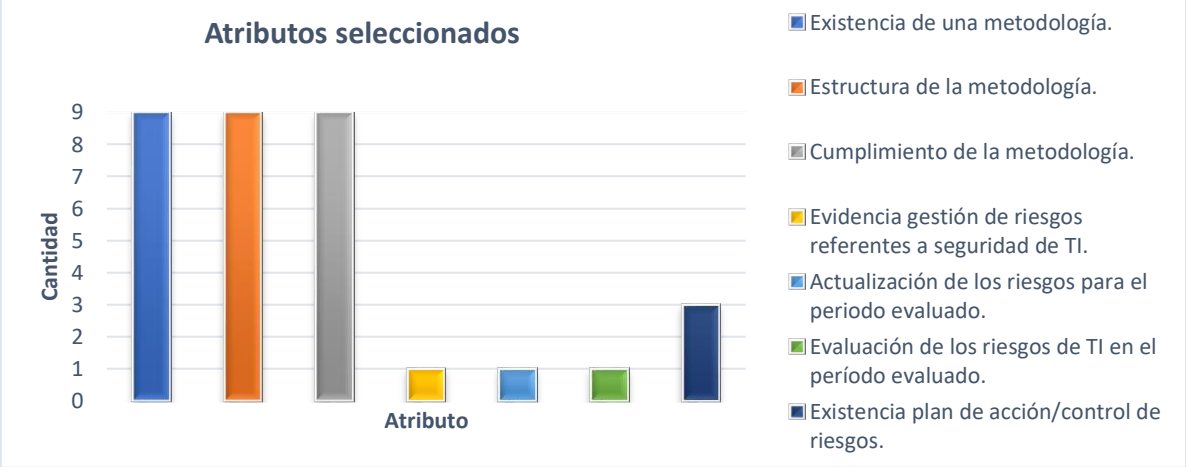
Se observa que en tres pruebas se consideró la existencia del plan presupuestario y la ejecución de dicho presupuesto, por lo cual su explicación se considerará dentro de la propuesta del manual de auditoría de TI.

4.2.3.2 Gestión de riesgos

Seguidamente, se procede a analizar los resultados obtenidos sobre gestión de riesgos, para esta prueba de los cuatro encuestados el 100% ha realizado una prueba de auditoría asociada a este tema, de igual manera todos los integrantes se apoyarían en una fuente externa para realizar esta prueba.

Para el análisis de los atributos seleccionados, se utilizaron nueve pruebas, destaca que el 100% de las pruebas analizadas mantienen la secuencia (existencia – estructura – cumplimiento). Gráficamente se puede observar en la Figura 4.3.

Figura 4.3 Atributos seleccionados: Prueba gestión de riesgos



Fuente: Elaboración propia.

En un una prueba se revisó la evidencia de la gestión de los riesgos referentes a la seguridad de TI, además se comprobó en otra prueba la actualización de los riesgos de TI para el período auditado y su respectiva evaluación, en tres pruebas se verificó la existencia del plan de acción de riesgos, se debe evaluar estos atributos en todas las pruebas, pues tener una metodología en la organización sin evaluar los riesgos es como no tener la metodología, o el otro caso, seguir evaluando los mismos riesgos con el pasar de los años, se debe tener presente que los riesgos van a sufrir modificaciones, por lo cual se deben actualizar según la periodicidad establecida por TI o por la organización.

Para las fuentes consultadas, las cuales se indican en la Figura 4.4 se destaca la consulta al encargado o gerente, el 75% de los integrantes consultarían a su mando superior para realizar esta prueba, cabe mencionar que ya todos los encuestados han realizado esta prueba como mínimo una vez.

Figura 4.4 Fuentes consultadas: Gestión de riesgos

Fuente: Elaboración propia.

Se menciona la ISO 31500, la cual es una norma para gestión de riesgos, el sistema específico de valoración de riesgos institucional y el modelo de gestión en el sector público o por sus siglas SEVRI y, por último, el estándar AS/NZS 4360, este es el estándar australiano para administración de riesgos.

Se considera importante incluir las explicaciones y referencias de estas tres fuentes dentro del manual de auditoría de TI, debido a que son más especializadas en el tema.

4.2.3.3 Gestión del portafolio de servicios

Dentro del análisis de las pruebas relacionadas con la gestión del portafolio de servicios se notó que el 100% de las pruebas ejecutadas se relacionan con la gestión de los SLA's, por tal motivo comparten el mismo gráfico. Este se puede observar en la Figura 4.5.

Además, se observó, que se evalúa la existencia de un catálogo de servicios, dejando por fuera los demás componentes del portafolio de servicios, como los servicios que se desean desarrollar y los servicios que ya han sido retirados.

Se puede observar que solo hay un atributo para la gestión del catálogo de servicios de TI, sin embargo, este atributo no contempla todo lo necesario para validar que la gestión del catálogo de servicios se realiza correctamente, por ejemplo, el catálogo esta accesible a los usuarios o el catálogo es actualizado periódicamente.

Por tal motivo se creará un tema en el manual para estos aspectos y se da la opción al auditor para que fusione esta prueba con la prueba de acuerdos de niveles de servicio, según la situación presentada en la organización por evaluar.

4.2.3.4 Acuerdos de niveles de servicio

Para este tema se analizaron cinco pruebas, gráficamente se observa en la Figura 4.5, una de ellas estuvo asociada a contratos.

Figura 4.5 Atributos seleccionados: Prueba Gestión de los acuerdos de niveles de servicio

Fuente: Elaboración propia.

En esta prueba se observa que además de revisar la existencia, estructura y complimiento de los SLA's, también se revisa que los SLA's sean actualizados y la existencia de un procedimiento para elaborar los acuerdos de niveles de servicio, no obstante, las actualizaciones de los SLA's se revisaron solo en una prueba, lo cual puede permitir acuerdos de niveles de servicio que no se reflejan la situación actual.

Tomando con referencia el proceso de ITIL Gestionar el nivel de servicio, ubicado en la fase de diseño del servicio se obtiene que los SLA's deben contener los siguientes aspectos:

- Descripción del servicio.
- Alcance del acuerdo.
- Horas de servicio.
- Funcionalidad.
- Disponibilidad.
- Confiabilidad.
- Rendimiento.
- Continuidad del servicio.
- Seguridad.
- Servicio al cliente.
- Escalaciones.
- Gestión de cambios.
- Responsabilidades.
- Reportes y revisión de servicios.
- Glosario.
- Versiones.

4.2.3.5 Gestión de proveedores

Se procede a analizar los resultados obtenidos sobre gestión de proveedores, dónde se recolectaron cinco pruebas, el gráfico se observa en la Figura 4.6, se detectó que esta prueba en una ocasión se realizó con la gestión de los SLA's.

Figura 4.6 Atributos seleccionados: Prueba gestión de proveedores

Fuente: Elaboración propia.

En este caso se observa el atributo de existencia de una metodología para la gestión de servicios establecidos con terceros, se revisa la existencia de contratos con terceros, además la estructura de dichos contratos, se analiza el seguimiento que el departamento de TI realiza a los contratos para verificar su cumplimiento, aquí se notó en las cinco pruebas investigadas que se revisa la estructura de los contratos existentes, no obstante, no hay un estándar de lo esencial que debería contener un contrato.

Producto de la revisión de las fuentes primarias de información, se obtiene la siguiente estructura base para los contratos, la cual será considerada en la elaboración del manual de auditoría de TI.

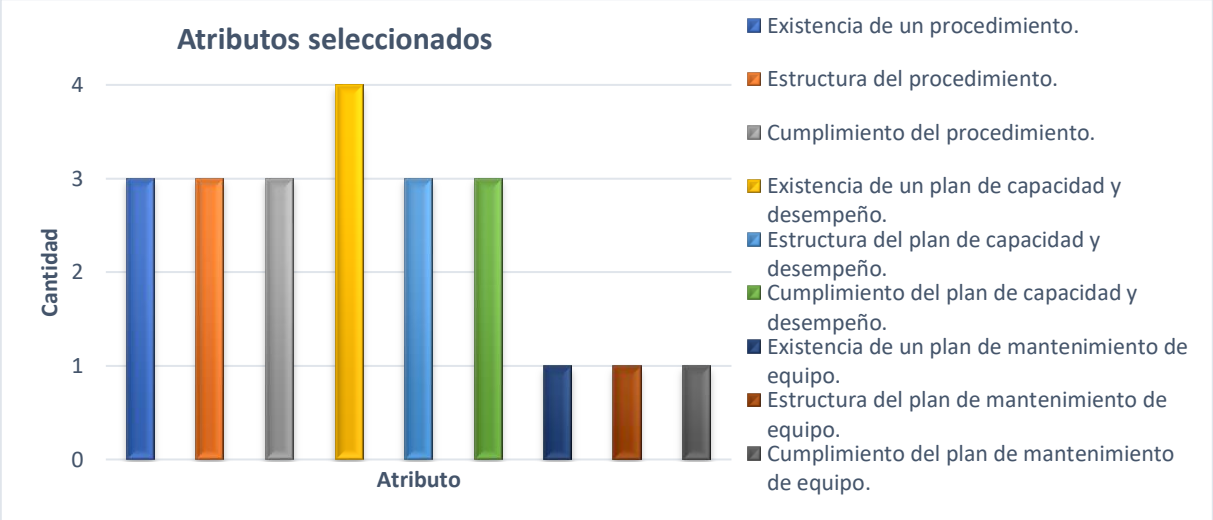
- Objeto del contrato.
- Obligaciones proveedor.
- Obligaciones del consumidor.
- Naturaleza del suministro.
- Duración.
- Cesión.
- Representación.
- Arbitramiento.
- Confidencialidad.

4.2.3.6 Gestión de la capacidad y desempeño

Se procede a presentar los resultados obtenidos para gestionar la capacidad y desempeño de la plataforma de TI, los mismos se muestran en la Figura 4.7, la cual se ubica en la siguiente página, para este análisis de revisaron seis pruebas anteriores, además, como se mencionará más adelante, gestión de la disponibilidad en algunos casos se incluye en esta prueba, esto debido a que *COBIT* 5 en su proceso BAI04 Gestionar la Disponibilidad y la Capacidad abarca los dos temas.

En esta prueba su pueden ver dos ejes principales, el primero consiste en la existencia de un procedimiento y el segundo en la existencia de un plan de capacidad y desempeño, los cuales fueron seleccionados dos veces, también se identifica un plan de mantenimiento de equipo.

Figura 4.7 Atributos seleccionados: Prueba gestión de la capacidad y desempeño



Fuente: Elaboración propia.

Con la referencia de ISO 20000 e ITIL, se procederá a explicar estos atributos, además en la tabla de atributos se indicará los componentes del procedimiento para gestionar la capacidad y el desempeño de la plataforma de TI.

4.2.3.7 Gestión de la disponibilidad

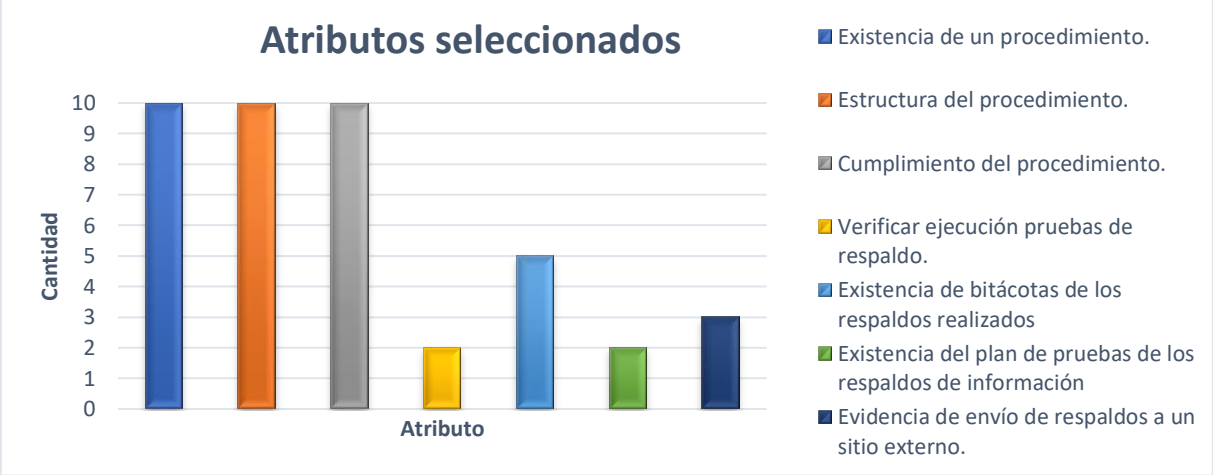
Para gestión de la disponibilidad no se hallaron pruebas relacionadas con este tema, si bien es cierto en la encuesta digital realizada, el 100% de los encuestados indicó haber realizado una prueba relacionada con disponibilidad, esto se debe a dos situaciones, la primera y más común es relacionar disponibilidad con los acuerdos de niveles de servicio, pues cada SLA define su porcentaje de disponibilidad, aquí es importante recalcar que gestión de la disponibilidad va más allá de brindar un porcentaje, sino que conlleva una serie de actividades y prácticas para que el departamento pueda asegurar que pueda brindar un porcentaje de disponibilidad del servicio.

La segunda situación es que se combina disponibilidad con capacidad, no obstante, es importante conocer la diferencia entre estos conceptos ya que comúnmente son confundidos, para lo cual en el apartado de conceptos claves del manual se abarcará la explicación de estos conceptos.

4.2.3.8 Respaldos y recuperaciones

Respaldos y recuperaciones según las buenas prácticas como ITIL, ISO 20000 o el marco de referencia de COBIT 5 pertenece a otros procesos como lo es seguridad, continuidad u operaciones, no obstante, dentro del despacho este tema se maneja como una prueba independiente por su importancia para el negocio, además facilita la realización de hallazgos en caso de ser necesario, de igual manera contempla su relación tanto con COBIT 5 como la normativa aplicable para la organización. Los resultados obtenidos se observan en la Figura 4.8.

Figura 4.8 Atributos seleccionados: Prueba respaldos y recuperaciones



Fuente: Elaboración propia.

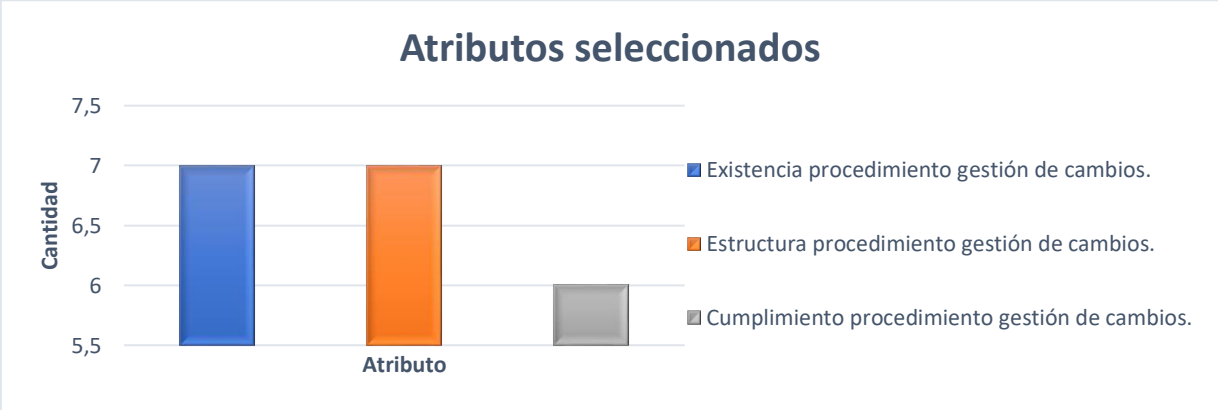
Para este tema se sigue la tendencia de revisar existencia – estructura – cumplimiento del procedimiento, se pudo notar que la mayoría de las organizaciones realizan los respaldos correctamente, no obstante, las recuperaciones no siempre se realizan, las cuales están asociadas con el plan de pruebas de los respaldos de información, esto para asegurarse que los mismos sean funcionales en caso de hacer manejo de ellos.

El procedimiento para respaldos y recuperaciones debe contener las actividades que lo componen, los responsables de ejecutar las operaciones, cada cuanto se deben realizar las actividades y, por último, se debe indicar textualmente el alcance del respaldo, eso quiere decir cual información si se respalda o cual no.

4.2.3.9 Gestión de cambios

Para gestión de cambios se analizaron siete pruebas, dónde no se obtuvieron atributos diferentes a existencia – estructura – cumplimiento, además hubo una prueba que no se revisó el cumplimento, pero esto se debe a que no había un procedimiento, por lo cual el auditor decidió omitirlo. Gráficamente se observa en la Figura 4.9.

Figura 4.9 Atributos seleccionados: Prueba gestión de cambios



Fuente: Elaboración propia.

Producto de la revisión de las fuentes primarias de obtuvo la siguiente estructura para el procedimiento de gestión de cambios, la cual será tomada en cuenta para la elaboración del manual:

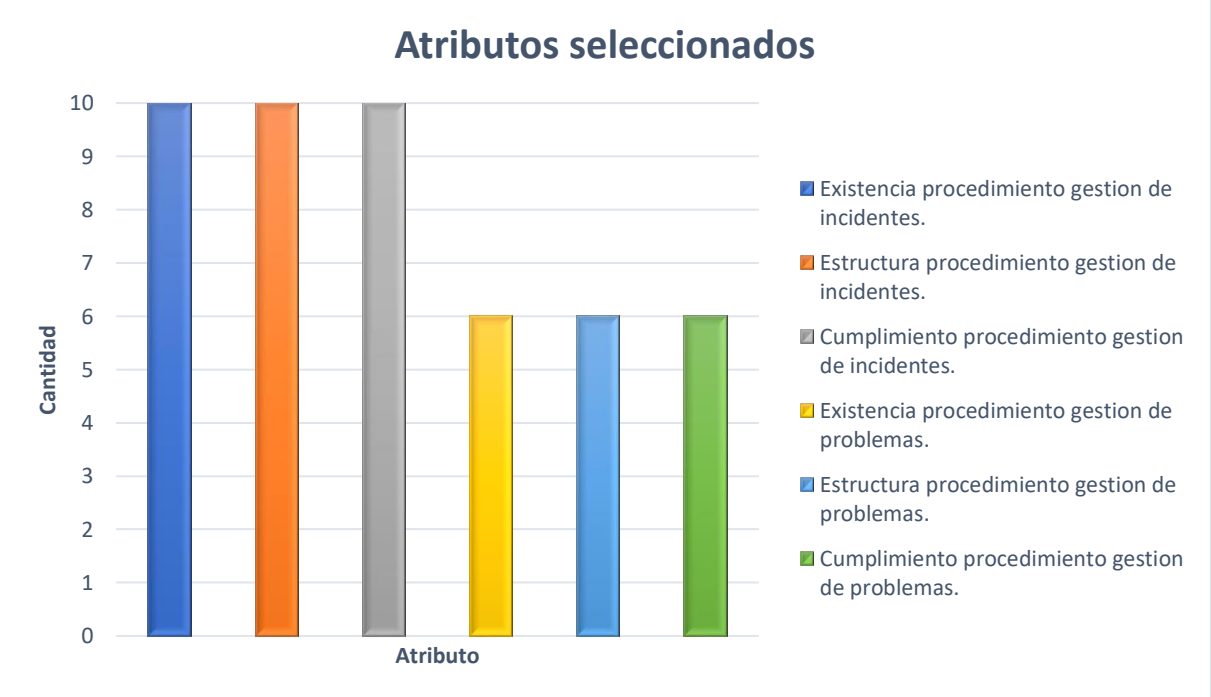
- Creación de la solicitud de cambio.
- Clasificación de la solicitud, dónde se pueden clasificar los cambios en estándares, normales o de emergencia.
- Priorización de las solicitudes de cambio basada en riesgos del negocio.
- Análisis del impacto de los cambios.

- Implementación de roles y responsabilidades que involucren a los dueños de procesos del negocio y a las funciones técnicas de TI apropiadas para la autorización y gestión de los cambios.
- Seguimiento e informe de cambios de estado.
- Cerrar y documentar los cambios.

4.2.3.10 Gestión de incidentes y solicitudes de servicio

Este tema y gestión de problemas se contemplan en la misma prueba, los atributos se observan en la Figura 4.10, no obstante, para fines del manual se van a abarcar los procesos por aparte, para así poder enfatizar las diferencias principalmente entre incidentes y problemas, en el caso de solicitudes de servicio si se contempla en este tema, pero de igual manera la explicación del tema abarcara las diferencias entre estos conceptos.

Figura 4.10 Atributos seleccionados: Prueba gestión de incidentes, solicitudes y problemas



Fuente: Elaboración propia.

De igual manera, se sigue manteniendo la tendencia de los atributos seleccionados, con la diferencia de que para el cumplimiento se toma en cuenta una función de la fase de operación en ITIL, como lo es la mesa de ayuda, indirectamente se evalúa en esta prueba, por lo cual también se abarcará su explicación y puntos por revisar cuando se audita.

La estructura para el procedimiento según las buenas prácticas y COBIT 5 es la siguiente:

- Detección.
- Registro.
- Categorización.
- Priorización.
- Aprobación (Solicitudes).
- Diagnóstico inicial.
- Escalación.
- Investigación y diagnóstico.
- Resolución.
- Cierre.

4.2.3.11 Gestión de problemas

Como se mencionó anteriormente gestión de problemas se abarcó en la Figura 4.10, dónde se observa la misma tendencia de los atributos seleccionados, se pudo observar en las pruebas analizadas que una de las irregularidades detectada es tratar un problema como si fuera un incidente, lo cual significa restaurar el servicio lo más pronto posible, pero no se realiza todo el estudio que conlleva gestión de problemas para evitar nuevamente incidentes asociados a este problema.

La estructura identificada en las buenas prácticas es la siguiente:

- Identificación de problemas mediante incidentes repetitivos o conocidos.
- Clasificación de problemas según categoría, impacto, urgencia y prioridad.
- Determinar la causa raíz del problema.
- Definir un plan de acción para la resolución de problemas.
- Definir el proceso de cierre del problema.

4.2.3.12 Gestión de eventos

No se encontró una prueba como tal para este tema, no obstante, si es considerado en varias pruebas como lo es capacidad y desempeño, dónde se definen umbrales para avisar en caso de que la capacidad de un elemento de TI cumpla el nivel establecido, también en seguridad se definen alarmas automáticas en caso de filtraciones físicas o lógicas, alertas por niveles de temperatura o húmedas, estas acciones generan eventos para que TI pueda atender las situaciones sin mayores contratiempos.

En la propuesta de manual de auditoría de TI ubicado en el Apéndice L: Propuesta manual de auditoría de TI, se indicarán los atributos por considerar para auditar este tema, y su relación con otras pruebas realizadas en el despacho, de tal manera que el auditor revise directamente los atributos propuestos.

La estructura base del procedimiento para el tema de gestión de eventos según la lectura realizada en *ITIL*, *COBIT* 5 y la *ISO* 20000 es la siguiente.

- Mantenimiento de mecanismos y reglas de monitorización de eventos.
- Clasificación y categorización de eventos.
- Correlación de eventos y selección de respuestas.
- Revisión y cierre de eventos.
- Elaboración de reportes de los eventos detectados.

4.2.3.13 Gestión del personal

Aquí se identificaron tres pruebas, la primera relacionada con capacitaciones del personal de TI, la segunda con el desempeño del personal y la última con acuerdos de propiedad intelectual. La selección de atributos de estas pruebas se observa en la Figura 4.11, ubicada en la siguiente página.

Se procede a exponer los atributos de este tema en la Figura 4.11, y posteriormente la explicación de las tres pruebas abarcadas en esta revisión documental de 11 pruebas.

Figura 4.11 Atributos seleccionados: Prueba gestión del personal

Fuente: Elaboración propia.

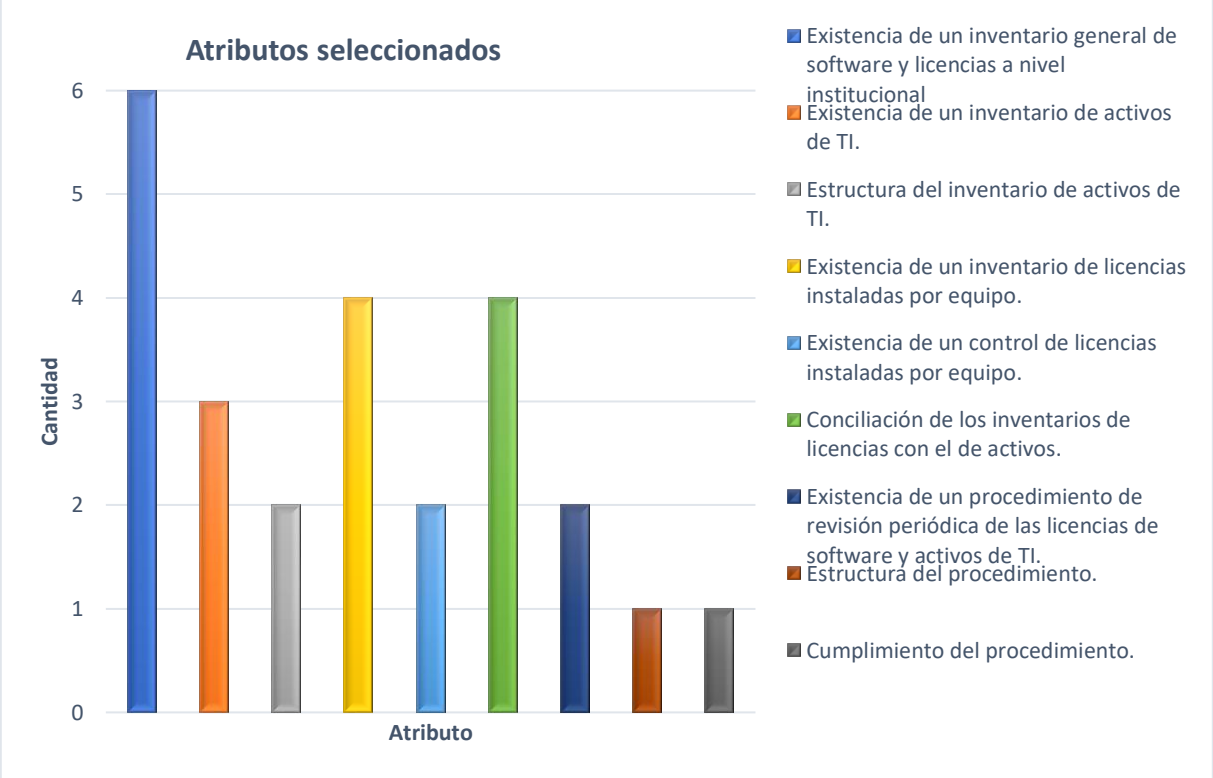
Las dos primeras pruebas se abarcan en la propuesta como tablas apartes, esto debido a que no siempre se realizan las dos, puede ser que se aplique una o ambas, en el caso de propiedad intelectual solo se identificó en una de las 10 empresas analizadas, no obstante, se mencionará en el manual como atributos opcionales.

La tendencia en estas 11 pruebas es la evaluación del plan de capacitaciones, aunque la evaluación del personal está directamente relacionada, ya que le permitirá a la organización definir las debilidades en las áreas de los colaboradores y así definir el plan de capacitaciones, de lo contrario el plan puede basarse en criterios personales para definir las áreas por abarcar en el plan.

4.2.3.14 Gestión de activos

Para gestión de activos se identificaron seis pruebas, las mismas se observan en la Figura 4.12, se identificó la revisión de dos inventarios, el de activos, y el de licencias, no obstante, una licencia forma parte de los activos de la organización, sin embargo, se pide por aparte para ver la conciliación con las licencias instaladas, además asegurarse que las licencias adquiridas estén vigentes y, por ende, no sean falsas, eso debido al decreto ejecutivo N° 37549-JP, el cual establece el Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central.

Figura 4.12 Atributos seleccionados: Prueba gestión de activos



Fuente: Elaboración propia.

En la propuesta del manual de auditoría de TI, se incluirá el decreto ejecutivo N° 37549-JP como anexo, además la aclaración de que abarca solo los Ministerios e Instituciones Adscritas al Gobierno Central, para que el auditor no vaya a evaluar su cumplimiento en una organización privada.

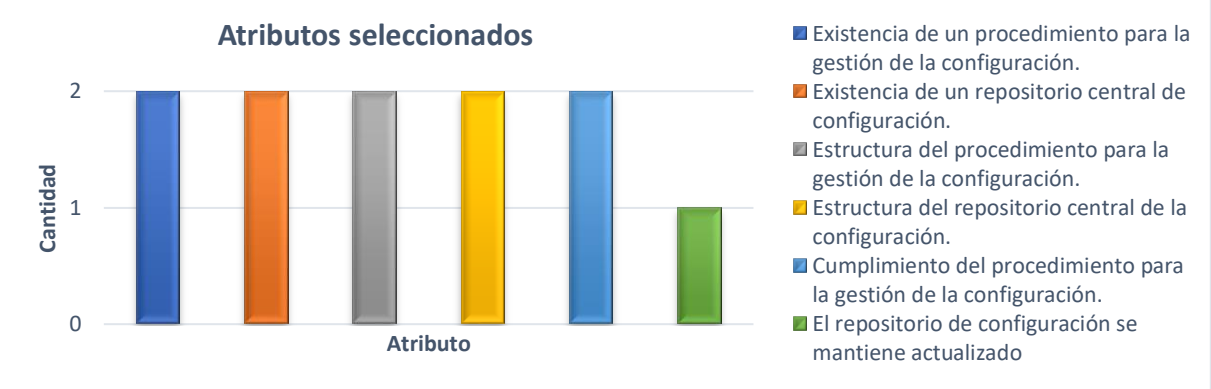
4.2.3.15 Gestión de la configuración

A continuación, en la Figura 4.13 se presenta los resultados obtenidos sobre gestión de la configuración.

Es una prueba poco aplicada según los datos recolectados, pero importante considerar, especialmente tomando en cuenta que se encuentra dentro de la normativa de la SUGEF 14-17, es un proceso que las organizaciones no realizan o lo hacen manualmente, sin embargo, existen herramientas para su gestión.

Con la explicación indicada en el manual propuesto, el auditor podrá recomendar tanto la estructura del procedimiento, como la importancia de que la organización gestione este tema.

Figura 4.13 Atributos seleccionados: Prueba gestión de la configuración



Fuente: Elaboración propia.

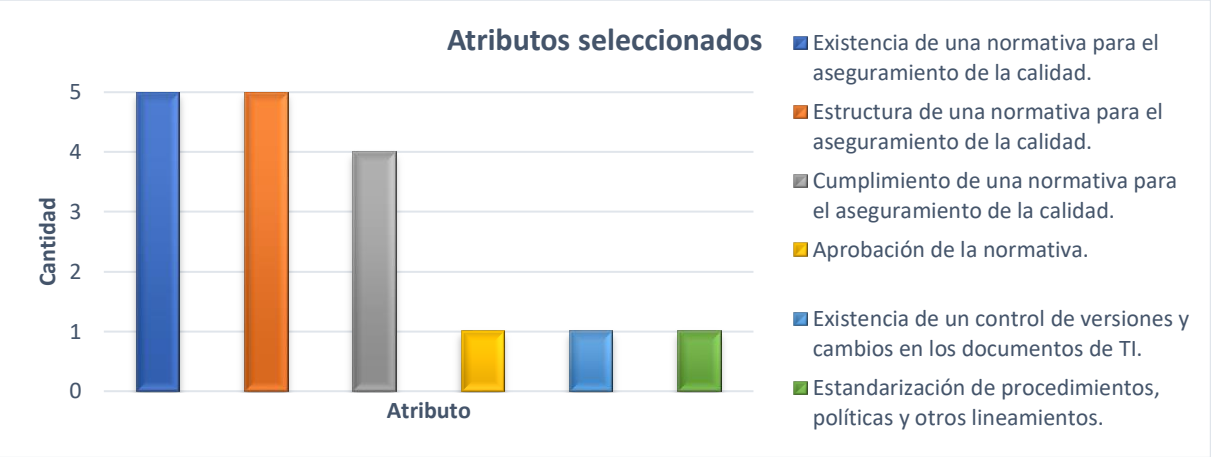
La estructura base para gestión de la configuración según ITIIL y la ISO 10007 es la siguiente:

- Línea base de los *CI's*.
- Registro de los elementos de configuración.
- Mantenimiento de las relaciones entre *CI's* y el repositorio de configuraciones.
- Revisión de la integridad de la con0figuración.
- Reportes o informe para verificar su cumplimiento.
- Periodicidad y responsable del cumplimiento.

4.2.3.16 Gestión de la calidad

Dentro del análisis de gestión de la calidad en cual se observa en la Figura 4.14, se pudo observar la existencia, estructura y cumplimiento de la normativa de calidad, estos atributos fueron revisados en el 100% de las pruebas, además en una prueba se revisó la aprobación de la normativa, la existencia de un control de versiones en los documentos de TI, y la estandarización de los procedimientos, políticas y otros lineamientos realizados por TI.

Figura 4.14 Atributos seleccionados: Prueba gestión de la calidad



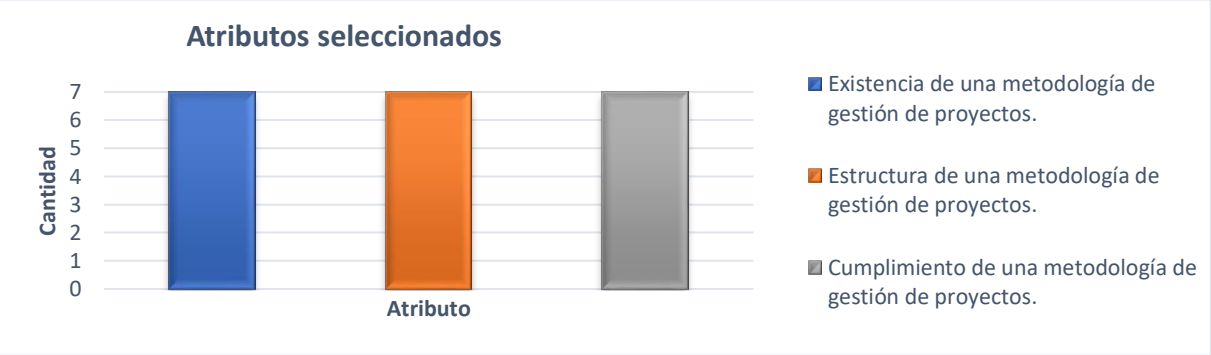
Fuente: Elaboración propia.

En una de las pruebas se observó la evaluación de la norma ISO 9001 referente a calidad, no obstante, no abarca los aspectos necesarios para evaluar la calidad de los servicios y productos de TI. Para gestionar este tema por parte de las organizaciones los auditores recomiendan el ciclo de Demming, el cual se puede comprender estudiando la quinta fase de *ITIL* denominada *Continual Service Improvement.*

4.2.3.17 Gestión de proyectos

En la Figura 4.15 se analiza que el siguiente tema tiene una estructura definida de los atributos por revisar, es importante recalcar que la gestión de proyectos puede variar dependiendo de la metodología que la organización adopte, si es una general o si por el contrario se tiene con una metodología propia adaptada a las necesidades de cada organización.

Figura 4.15 Atributos seleccionados: Prueba gestión de proyectos



Fuente: Elaboración propia.

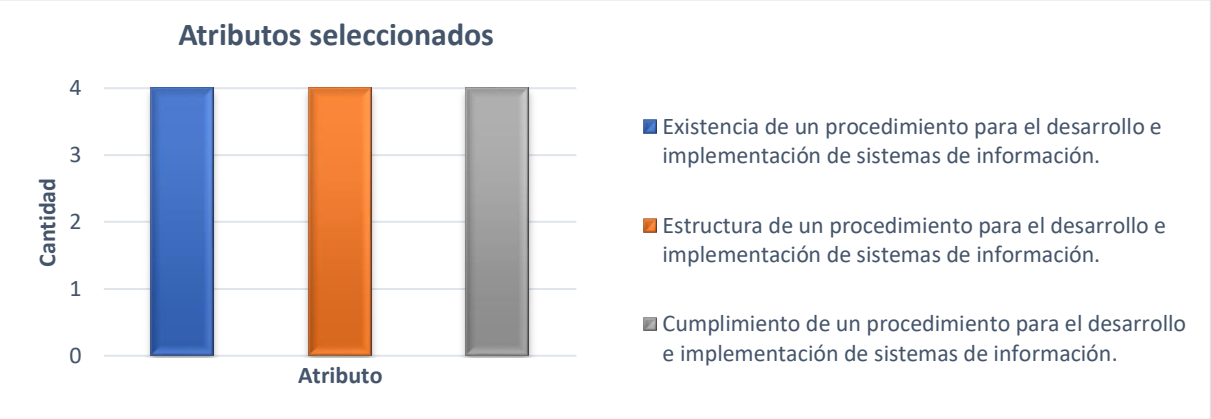
Producto de la investigación realizada sobre este tema se determinó que una metodología de proyectos mínimo debería considerar los siguientes aspectos:

- Dirección de proyectos.
- Requerimientos.
- Objetivos.
- Responsabilidades.
- Planeación del alcance, tiempo y estimación de recursos.
- Acta de constitución del proyecto.
- Gestión de alcance.
- Gestión del tiempo del proyecto.
- Plan de gestión de los recursos Humanos.
- Roles y responsabilidades.
- Estructura detallada de trabajo.
- Capacitaciones.
- Evaluaciones del desempeño.
- Generalidades del plan de gestión de comunicaciones.
- Matriz de comunicaciones.
- Distribución de la información.
- Análisis FODA.
- Gestión de la planificación de los riesgos del proyecto.
    - Riesgos del proyecto.
    - Plan de gestión de Riesgos.
    - Priorización de riesgos.
    - Probabilidad e impacto de los riesgos.
    - Categorización de los riesgos.

4.2.3.18 Implementación de software

Aunque el desarrollo e implementación de software se puede considerar como un proyecto más, la forma de gestionarlo es distinto, por ende, es necesario tener un procedimiento o metodología para proyectos de software, los atributos seleccionados se observan en la Figura 4.16. El desarrollo de los atributos se realiza en la propuesta del manual de auditoría de TI.

Figura 4.16 Atributos seleccionados: Prueba implementación de software



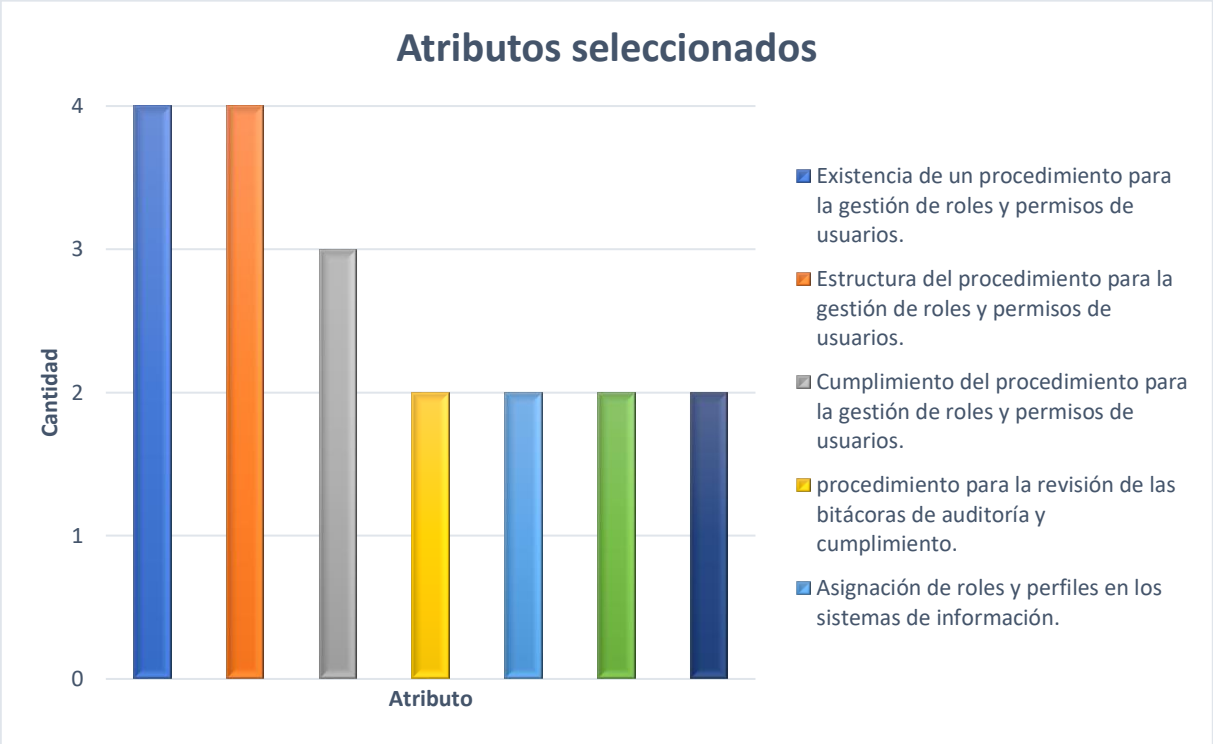
Fuente: Elaboración propia.

4.2.3.19 Gestión de accesos

Para gestión de accesos, se identificaron dos pruebas, los atributos seleccionados se observan en la Figura 4.17 ubicada en la siguiente página, la primera relacionada con accesos como tal, como roles, perfiles y permisos de usuario, la segunda más administrativa, la cual consiste en verificar la inexistencia de exfuncionarios activos dentro de la organización, también se evalúa la existencia de cuentas genéricas y en caso de ser positivo que estas cuentas posean su responsable.

Se procede a mencionar los atributos seleccionados para la gestión de accesos.

Figura 4.17 Atributos seleccionados: Prueba gestión de accesos



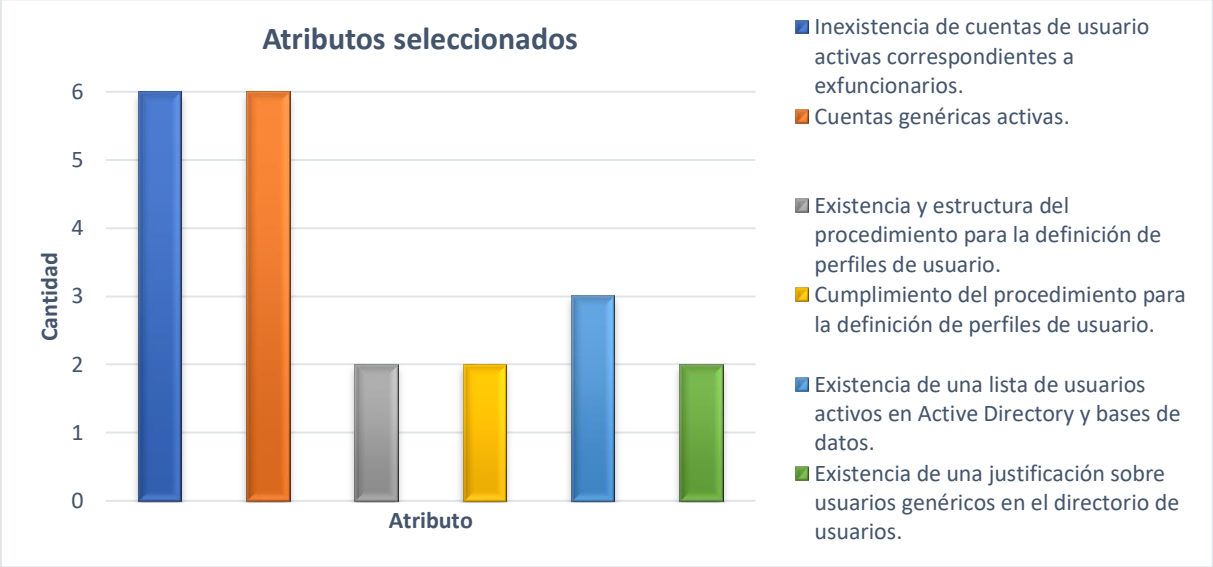
Fuente: Elaboración propia.

Para gestión de accesos se revisa la existencia de un procedimiento para la gestión de roles y perfiles, se evalúa su estructura y procedimiento, además en el 50% de las pruebas analizadas también se evaluó la asignación de roles y perfiles en los sistemas de información, además de informes de seguimiento tanto para pistas de auditoría como para roles y perfiles.

En el caso de esta prueba, se analizaron seis pruebas anteriores, de forma gráfica se observa en la Figura 4.18, de las cuales en el 100% se evaluó la inexistencia de cuentas de usuarios activas correspondiente a exfuncionarios, además de las cuentas genéricas activas, en solo el 33% se evaluó la existencia de un procedimiento para la definición de perfiles de usuario, esto se debe a que este atributo también es evaluado en la prueba anterior.

Se procede a indicar los atributos seleccionados para la prueba dónde se verifica la existencia de usuarios activos dentro de la organización y sus sistemas.

Figura 4.18 Atributos seleccionados: Prueba existencia de usuarios activos



Fuente: Elaboración propia.

4.2.3.20 Arquitectura Empresarial

En el caso de la Figura 4.19 se revisa la existencia de un modelo de arquitectura de información, se verifica su estructura y, por último, se evalúa si se le realizan actualizaciones periódicas al modelo de arquitectura de información.

Figura 4.19 Atributos seleccionados: Prueba modelo arquitectura empresarial

Fuente: Elaboración propia.

En el manual se explicará cómo está compuesto el modelo de arquitectura de información y cuáles son las fuentes que uno puede consultar en caso de querer expandir los conocimientos adquiridos.

Producto de la investigación realizada sobre este tema en fuentes como *COBIT* 5 y *TOGAF* se verificó que el modelo de arquitectura empresarial está compuesto por cuatro capas, las cuales abarcarán su aplicación en la propuesta del manual de auditoría en su respectivo tema, ubicado en el Apéndice L: Propuesta manual de auditoría de TI. Se procede a mencionar las cuatro capas identificadas:

- Modelo de negocio.
- Modelo de datos.
- Modelo de aplicaciones.
- Modelo de tecnología.

4.2.3.21 Gestión de la continuidad

Para gestión de la continuidad se verifica la existencia de un plan de continuidad, además de la estructura de este, también es necesario contar con un plan de pruebas para el periodo evaluado, que se realicen las pruebas planeadas.

Es importante complementar las pruebas con capacitaciones sobre este tema, para que, en caso de una eventual emergencia, las personas puedan reaccionar de la mejor manera.

Por último, en dos pruebas se revisó la existencia de un sitio alterno, dónde se pudo observar que se enfoca en verificar si se tiene o no el sitio alerto, pero no abarca más atributos.

El resumen de los atributos seleccionados se observa en la Figura 4.20.

Figura 4.20 Atributos seleccionados: Prueba plan de continuidad

Fuente: Elaboración propia.

Dentro de la investigación realizada en las fuentes primarias sobre este tema, se identificó la siguiente estructura como la estándar:

- Análisis de impacto sobre el negocio.
- Análisis de riesgos.
- Identificar procesos críticos del negocio.
- Identificar las acciones de contingencia y controles preventivos previo a una incidencia.
- Definir los procesos de activación del plan.
- Documentar los procedimientos de comunicación entre los responsables de ejecutar el plan.
- Definir los procedimientos para recuperar los procesos de negocio incluyendo la infraestructura tecnológica.
- Definir los procedimientos posteriores a recuperación, considerando evaluación de daños y efectividad del plan de continuidad.

4.2.3.22 Gestión de la seguridad de la información

Gestión de la seguridad es un tema complejo de abordar por su gran cantidad de atributos que se pueden evaluar, incluso hay estándares especializados en este tema como la ISO 27000 y su familia de normas.

En la Figura 4.21 se pueden observar los atributos seleccionados según las ocho pruebas analizadas, en el 100% se revisó la existencia, estructura y cumplimiento de la política de seguridad, en una prueba se verificó la realizaciones de capacitaciones referentes al marco de seguridad, se notan aristas como vulnerabilidad de la red, dónde se evalúa la existencia de un procedimiento, además la ejecución de estudios de vulnerabilidad, otro punto que se observó son las políticas de internet, uso de equipo y correo electrónico y, por último, el tema de clasificación de la información.

Figura 4.21 Atributos seleccionados: Prueba seguridad de la información

Fuente: Elaboración propia.

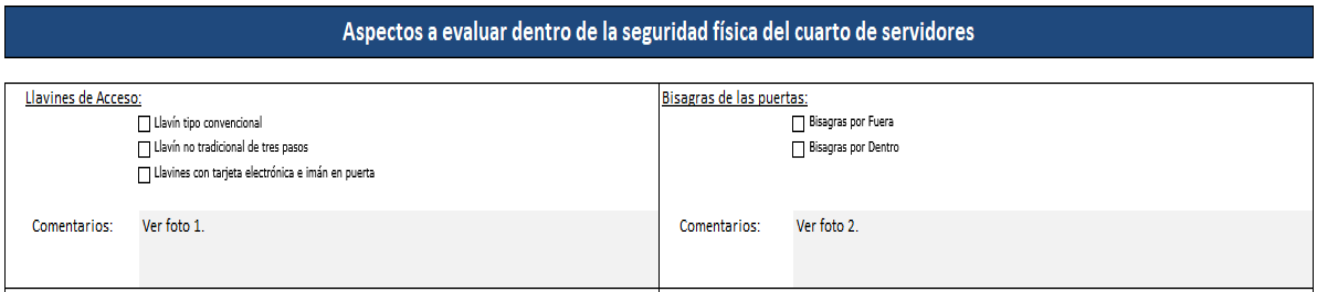
Para facilitar la comprensión de este tema en la propuesta del manual de auditoría se procederá a dividir en los siguientes subtemas:

- Política de seguridad de la información.
- Estudio de vulnerabilidad de la red.
- Políticas referentes al uso de equipo de cómputo, internet y correo electrónico.
- Metodología para clasificación de la información.
- Seguridad Física (Se abarca como un tema independiente).

4.2.3.23 Seguridad Física

Para seguridad física se posee una plantilla, por lo cual los atributos son iguales cuando se procede a realizar la prueba de seguridad física, se procede a mencionar la plantilla utilizada en la Figura 4.22.

Figura 4.22 Sección de la plantilla de Seguridad Física



Fuente: Despacho Carvajal (2018).

Para esta prueba se realiza una visita al cuarto de servidores de la organización para verificar los siguientes aspectos dentro de la seguridad física:

- Llavines de acceso.
- Bisagras de la puerta.
- Ventanas dentro del cuarto de servidores.
- Paredes de concreto.
- Piso falso.
- Aires acondicionados.
- Detectores de humo.
- Temperatura en el momento de la revisión.
- Medidores de humedad.
- Oficinas dentro del cuarto de servidores.
- Equipo en desuso.

- Oficinas dentro del cuarto de servidores.
- Servidores ordenados en racks.
- Cableado ordenado y etiquetado.
- Estado de las UPS.
- Lugar del extintor, fecha de recarga y tipo de carga.
- Bitácoras de acceso.
- Acceso al cuarto de servidores.
- Visitas de mantenimiento al hardware.
- Localización del cuarto de servidores.
- Almacenamiento de los respaldos.
- Bitácoras de revisión de respaldos.
- Cableado estructurado.
- Controles o bitácoras de acceso al cuarto de servidores.
- Entrenamiento del personal en la utilización de materiales peligrosos.
- Reporte de alarmas del centro de datos.
- Bitácoras de envío de los respaldos al sitio alterno.
- Verificar la información de los componentes de los servidores y sus versiones de software.
- Actualizaciones instaladas en los servidores.
- Acceso remoto a los servidores.

Para cada uno de los atributos anteriores se procede a revisar de la siguiente manera, primeramente, se coordina la visita al cuarto de servidores y después se valida punto por punto, para la evidencia se realiza una fotografía de cada punto, en caso de que algún punto posea una debilidad se procede a realizar un hallazgo.

4.2.3.24 Sistemas de información

Para los sistemas de información, se cuenta con una plantilla para la revisión, se procede a mencionar un extracto de la plantilla utilizada, la cual se puede observar en la Figura 4.23.

Figura 4.23 Plantilla seguridad lógica

Bitácoras	Revisión Bitácoras	Una Única Sesión	Validación Directorio de Usuarios (Active Directory / LDAP / Base de datos)	Vencimiento Clave (60 días máx.)	Histórico de claves	Tamaño clave (mín. 8)	Cambio 1er Clave	Complejidad Clave (Letras, Números, Mayúsc., Minúsc.)

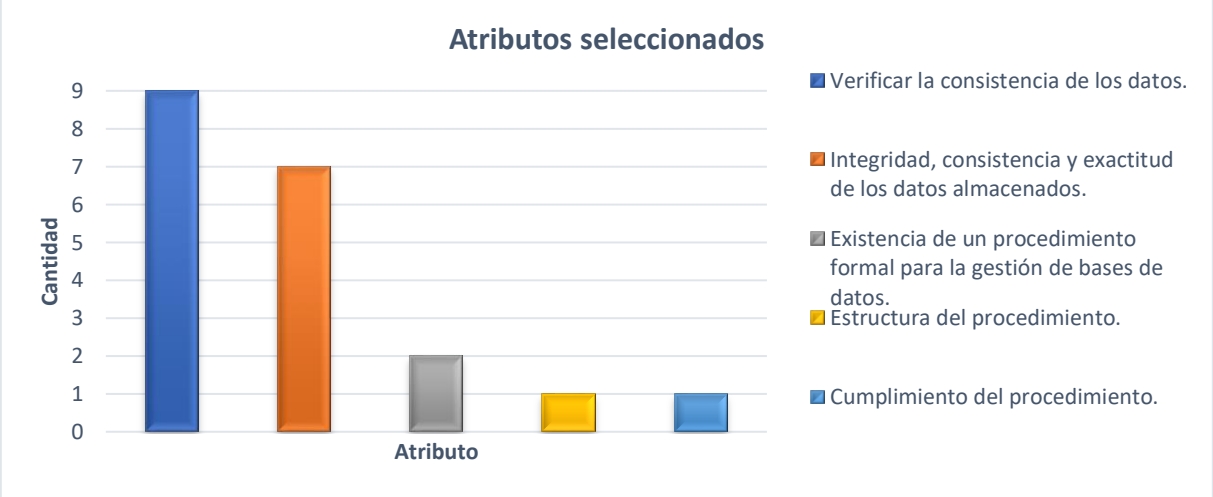
Fuente: Despacho Carvajal (2018).

Los atributos anteriores son consultados a los usuarios de los sistemas de la organización, la muestra la define el gerente y depende del tamaño de la organización y alcance de la auditoría.

4.2.3.25 Administración de bases de datos

Esta prueba consiste básicamente en verificar la integridad, consistencia y exactitud de los datos almacenados, tal y como lo muestra la Figura 4.24, la manera en que se evalúan estos atributos es cambiante según la organización, pero el fin es el mismo, encontrar irregularidades que afecten la información almacenada y su uso dentro de la organización.

Figura 4.24 Atributos seleccionados: Prueba Administración de bases de datos



Fuente: Elaboración propia.

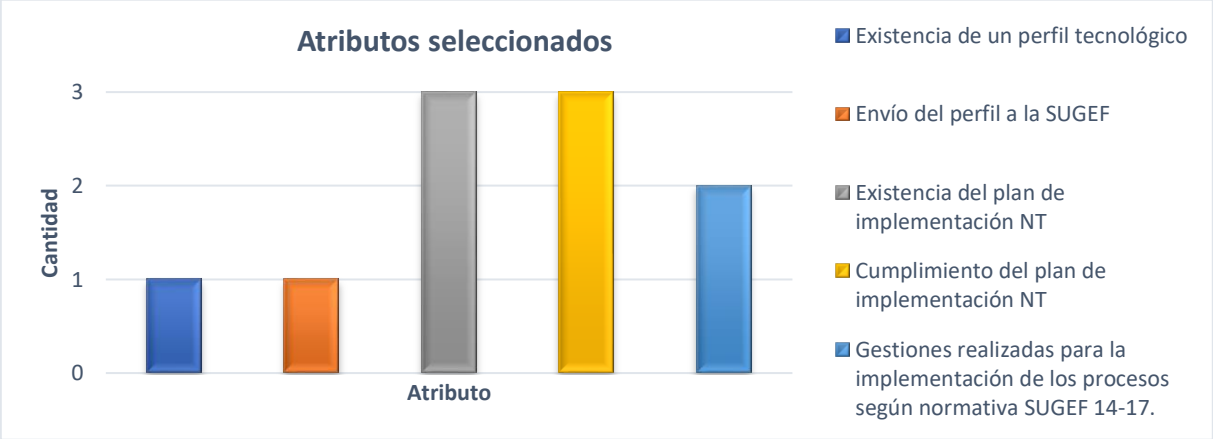
4.2.3.26 Cumplimiento de la normativa aplicable

Para el cumplimiento de la normativa aplicable se logró identificar tres normativas principales, las primeras dos que son de carácter obligatorio por el sector en que se ubican y la tercera es porque se adopta como marco de cumplimiento.

- Normas técnicas.
- SUGEF 14-17.
- *COBIT* 5.

Se observan los atributos de la prueba cumplimiento de la normativa aplicable en la Figura 4.25.

Figura 4.25 Atributos seleccionados: Prueba cumplimiento de la normativa



Fuente: Elaboración propia.

4.2.3.27 Control

Existen diversos tipos de control, sin embargo, en el manual se abarcarán tres tipos, los cuales son explicados en el marco teórico de este documento:

- Control interno.
- Auditoría externa.
- Auditoría interna.

En el caso de control interno si se evalúa la existencia de un procedimiento o metodología, para las auditorías se revisa la realización de auditorías y el seguimiento al cumplimiento de las recomendaciones emitidas en estos informes, por último, en dos pruebas se evaluó la existencia de un auditor interno de TI, el resumen de los atributos seleccionados se observa en la Figura 4.26.

Se procede a mostrar gráficamente los atributos seleccionados para la prueba de control en la Figura 4.26.

Figura 4.26 Atributos seleccionados: Prueba control

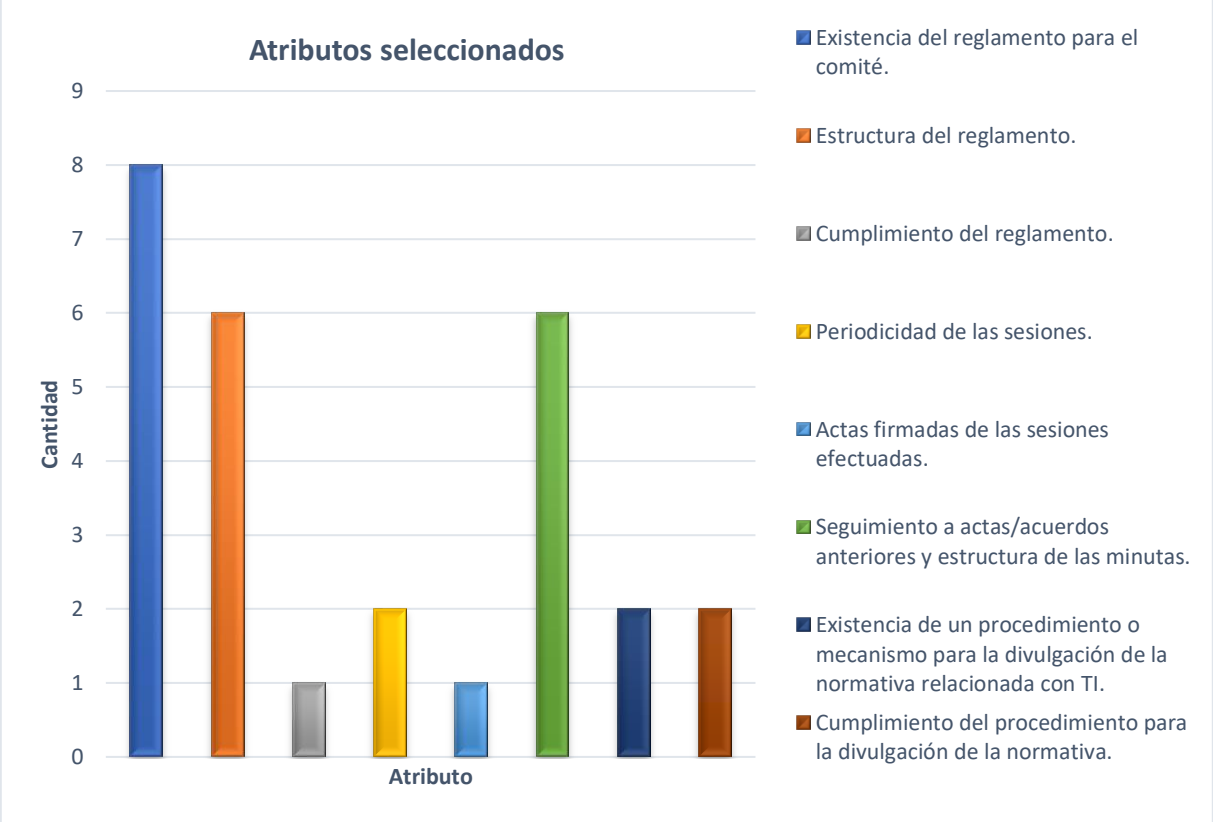
Fuente: Elaboración propia.

4.2.3.28 Marco de gestión de TI

Para este tema se identificaron dos pruebas, tal y como se muestra en la Figura 4.27, la primera relacionada con el comité de TI, la cual puede variar de nombre, por ejemplo, comisión, pero con el mismo fin de abarcar los temas estratégicos de TI, en la cual primeramente se revisa la existencia de un reglamento para el comité, la estructura del reglamento, que se cumpla el reglamento lo cual está relacionado con la periodicidad de las sesiones.

La segunda prueba relacionada con el marco de gestión de TI está relacionada con el o los mecanismos para la divulgación de la normativa relacionada con TI, en la cual se revisa la existencia de un procedimiento y su cumplimiento.

Figura 4.27 Atributos seleccionados: Prueba marco de gestión de TI

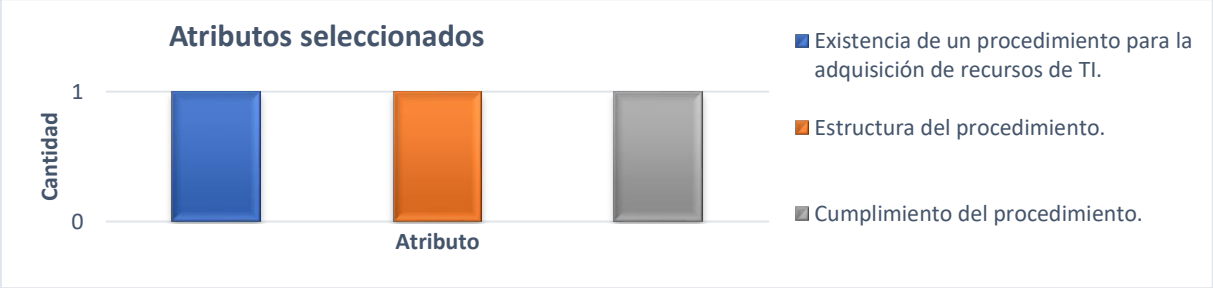


Fuente: Elaboración propia.

4.2.3.29 Plan adquisición de TI

Para el plan de adquisición se logró analizar una prueba, se observa en la Figura 4.28, dónde se incluye el procedimiento para la adquisición de recursos de TI, además de su estructura y cumplimiento.

Figura 4.28 Atributos seleccionados: Prueba adquisición de TI



Fuente: Elaboración propia.

Dentro de la estructura del plan de adquisición de TI, según la investigación realizada, se deben contemplar aspectos como:

- Necesidad real de la adquisición.
- Costo de la tecnología o servicio por adquirir.
- Fecha de entrega.
- Capacitaciones necesarias para gestionar la adquisición.
- Beneficios esperados.
- Razones financieras.

4.2.3.30 Gobierno de TI

No se encontró ninguna prueba relacionada directamente a gobierno de TI, no obstante, este tema es considerado tanto en COBIT 5 en su dominio EDM, como en el acuerdo SUGEF 14-17, por tanto, se abarcará en el manual y los posibles atributos por revisar en caso de tener que auditar una organización dónde aplique la implementación formal del gobierno de TI.

4.3 Fase de cierre

Se procede a mencionar las actividades realizadas actualmente en la fase de cierre.

Revisión de resultados obtenidos

Se hace una revisión a lo interno por parte del encargado sobre equipo de trabajo para asegurarse cumplir con todos los requerimientos iniciales y demás requisitos para finalizar la auditoría.

Estado de pruebas

El encargado revisa que las pruebas estén realizadas y aprobadas, además que cuenten con su respectivo hallazgo.

Informe de auditoría (Carta Gerencia)

El encargado construirá el informe de auditoría con base en la información obtenida de las fases anteriores, aunque esta no es una actividad de los asistentes, se explicará en el manual las partes que contiene un informe de auditoría.

- Introducción.
- Hallazgos.
- Seguimiento.
- Matriz de Riesgos.

Presentación al gerente del Despacho

El encargado de la auditoría le presentará el informe al gerente para su respectiva revisión y aprobación. En caso de realizar cambios se valora si es responsabilidad del encargado o los asistentes.

Presentación al área de TI

Una vez aprobado el informe, se le presentará al área de TI de la organización, ya sea el gerente o el encargado, para corroborar que los hallazgos de verdad correspondan a la situación actual de TI.

Presentación a la junta directiva

El gerente en ocasiones acompañado con el encargado de la auditoría hará la presentación de los resultados obtenidos ante la junta directiva de la organización, de ser aceptado aquí terminará el ciclo del periodo de la auditoría, si no se deben hacer los cambios pertinentes para su aceptación. En el caso de *COBIT* 5, habla de informes de evaluación, los cuales consisten en los resultados de la evaluación y son presentados al patrocinador de la auditoría.

4.4 Fase de evaluación

Esta fase surge a partir de la norma ISO 19011, la cual considera en sus directrices para la auditoría de sistemas de gestión, una actividad de competencia y evaluación de los auditores, dónde se determinan las competencias del auditor para cumplir las necesidades del programa de auditoría, se establecen los criterios de evaluación, se realiza la evaluación y se procede a realizar el mantenimiento y mejora de las competencias de los auditores.

Basándose en las tareas mencionadas se procede a realizar un procedimiento para esta fase, el procedimiento se puede observar en la Figura 5.6 y el apartado completo de esta fase se encuentra en el manual de auditoría de Ti ubicado en el Apéndice L: Propuesta manual de auditoría de TI.

Capítulo V

Propuesta de Solución

5. Propuesta de solución

En este capítulo se procede a explicar la propuesta de solución, la cual viene a cubrir la situación problemática, utilizando como referencia la investigación realizada en el marco teórico además de la información recolectada y analizada por medio de entrevistas, cuestionarios y revisión documental.

El entregable de la propuesta consiste en un manual de auditoría de TI, el cual se puede observar su primera versión en el Apéndice L: Propuesta manual de auditoría de TI, se procede a explicar su creación y puntos esenciales.

5.1 Elaboración del manual

A continuación, se procede a explicar el procedimiento para elaborar el manual.

5.1.1 Estructura del manual

Primeramente, se procedió a definir la estructura del manual, separándolo por capítulos:

Capítulo 1 Entendimiento

El objetivo de este capítulo es lograr que el colaborador tenga una noción de la organización dónde labora, conozca la historia del despacho, cuál es su misión y visión, además de la propuesta de valor, los servicios que brinda incluyendo los de TI.

Seguidamente, se explican los puestos dentro del departamento de TI, así el colaborador podrá identificar cuáles son sus actividades en el ambiente laboral, e identificar las relaciones a las que estará expuesto, se describen los requerimientos, conocimientos, habilidades y actitudes del puesto, así podrá identificar si posee debilidad en alguna de las características anteriores y así trabajar en su desarrollo.

Después se procedió a explicar conceptos esenciales del puesto, dónde se incluye el concepto de auditoría de TI, se da respuesta a tres interrogantes, las cuales son planteadas en el ambiente laboral y se explica las diferencias entre auditoría interna y externa.

Por último, se abarca la explicación de las principales fuentes de información utilizadas en el despacho, dónde se incluye COBIT 5, ITIL y dos énfasis de la Legislación Nacional, el primero sería el sector público, el cual se encuentra regulado por la Contraloría General de la Republica y el sector financiero regulado por la SUGEF, la normativa SUGEF 14-17 también aplica para otras superintendencias reguladas por CONASSIF, la estructura se puede observar en la Figura 2.10.

. Capítulo 2 Ciclo de Auditoría del Despacho Carvajal

En este capítulo se procede a explicar las fases de la auditoría de TI dentro del despacho, para lo cual primeramente se realizó una entrevista con uno de los encargados de TI para identificar como se realiza actualmente una auditoría de TI, el cual se puede observar en el Apéndice D: Ciclo actual de auditoría.

Posteriormente, se procedió a realizar mejoras al ciclo de auditoría siguiendo el estándar la ISO 19011, el cual dicta las directrices para la auditoría de sistemas de gestión. En el Anexo 5: Flujo de proceso para la gestión de un programa de auditoría., se agrega el flujo propuesto por el estándar.

En cuanto a las mejoras realizas del ciclo, consiste en definir y documentar las actividades, para no generar ambigüedades por diversos criterios de la misma actividad, las actividades se observan en el manual de auditoría de TI.

Después se procede a explicar las actividades por fase.

Planificación

Se detalla en que consiste cada actividad realizada en la auditoría de TI, además se indica las plantillas que actualmente se utilizan.

Ejecución

La fase de ejecución es dónde se centra más el proyecto, de igual forma se empieza con la explicación de las actividades realizadas y las plantillas que se utilizan de forma genérica, esto quiere decir que, si hay una plantilla para una prueba en específica, se explicara dentro de la prueba y no al inicio, las pruebas con plantilla específicas son: seguridad física y seguridad lógica.

Para la selección de los temas que se incluyeron en el manual se utilizó cinco auditorías de los diferentes sectores de clientes del despacho, las cuales se pueden observar en el Anexo 6: Auditorías seleccionadas para identificar los temas del manual, se identificaron y analizaron los requerimientos iniciales y se procedió a asociarlos con la normativa vigente y las buenas prácticas, esto para asegurar que se abarque todos los puntos descritos en la normativa nacional. Los temas seleccionados se observan en la Tabla 5.1 y fueron validados con el gerente de TI en la segunda reunión de avance, su minuta se puede observar en el Apéndice I Minuta de reunión N°1 con Gerente de TI.

Tabla 5.1 Temas seleccionados

Tema
1. Gestión de la estrategia de TI.
2. Gestión de riesgos.
3. Gestión del Catálogo de servicios.
4. Acuerdos de niveles de servicio.
5. Gestión de proveedores.
6. Gestión de la capacidad y desempeño.
7. Gestión de la disponibilidad.
8. Respaldos y recuperaciones.
9. Gestión de cambios.

Tema
10. Gestión de incidentes y solicitudes de servicio.
11. Gestión de problemas.
12. Gestión de eventos.
13. Gestión del personal.
14. Gestión de activos.
15. Gestión de la configuración.
16. Gestión de la calidad.
17. Gestión de proyectos.
18. Implementación de software.
19. Gestión de accesos.
20. Arquitectura empresarial.
21. Gestión de la continuidad.
22. Gestión de la seguridad de la información.
23. Seguridad física.
24. Sistemas de información.
25. Administración de bases de datos.
26. Cumplimiento de la normativa aplicable.
27. Control interno.
28. Marco de gestión de TI.
29. Plan adquisición de TI.
30. Gobierno de TI.

Nota: Elaboración propia.

Después se procedió con la explicación de los temas indicados en la Tabla 5.1, para eso se tomó como referencia *ITIL*, *COBIT* 5, las fuentes de información indicadas por el equipo de auditoría en el Apéndice H: Encuestas de procesos y la revisión de

otras fuentes, como ISO y libros específicos, en el caso de tomar en cuenta una de estas fuentes, la cual es indicada dentro del manual en el apartado Material complementario.

Dentro de la explicación se incluye un apartado por cada prueba seleccionada, aquí se debe aclarar que por tema se puede incluir una o más pruebas, tal es el caso de seguridad de información, que se toman cuatro pruebas (Seguridad de la información, vulnerabilidad de la red, clasificación de la información y políticas de uso de recursos) aparte de seguridad lógica y seguridad física.

Un punto importante por considerar de la propuesta es que el manual se distribuirá a los colaboradores del departamento de forma digital, esto para facilitar el estudio de las plantillas utilizadas con los atributos de cada prueba, de esta manera las plantillas serán agregadas como hipervínculos.

Cierre

Dentro de la fase de cierre se explican las actividades que se realizan y los documentos que se deben generar para cada una, se considera en análisis realizado en el capítulo anterior para la explicación de las actividades.

Evaluación

En el caso de evaluación, es una fase que se está en proceso de implementación, sin embargo, no se encuentra un procedimiento establecido de cómo se realiza dicha evaluación.

En esta fase se indicó la evaluación que se realiza, cuáles son los factores sé que se evalúan, además se verificó su estructura con base en la ISO 19011, su explicación también se puede observar en el Apéndice L: Propuesta manual de auditoría de TI.

Capítulo 3 Conclusión

Este es un capítulo de cierre dónde se incluye conclusiones y recomendación importantes para el colaborador, que fueron identificadas durante el proceso de desarrollo del manual, además se agrega un glosario, en el caso de los anexos se procede a indicar los links de la normativa de TI y, por último, se incluye las referencias bibliográficas que fueron soporte para la creación del manual.

5.2 Implementación de la propuesta

Se procede a indicar las actividades pendientes para implementar la propuesta. Para esto el manual se someterá a una revisión final por parte del gerente de TI, es importante mencionar que ya se realizaron tres reuniones de revisión de avance y en la última el gerente da como aceptado el manual, aun así, es recomendable la última revisión y gestionar los cambios convenientes, después proceder a gestionar su aprobación en la organización para que sea considerado como un documento oficial dentro del despacho.

Una vez aprobado el manual, se procede a brindar una copia digital a cada miembro del equipo de auditoría para su lectura, además de brindar una copia cuando haya un nuevo colaborador en el departamento, para este caso la propuesta incluye un cronograma de aprendizaje del manual, siguiendo la metodología de la Figura 5.1.

5.2.1 Roles

Se procede a indicar en la Tabla 5.2 los roles que se relacionan con el manual y cuál es su función.

Tabla 5.2 Roles dentro del manual

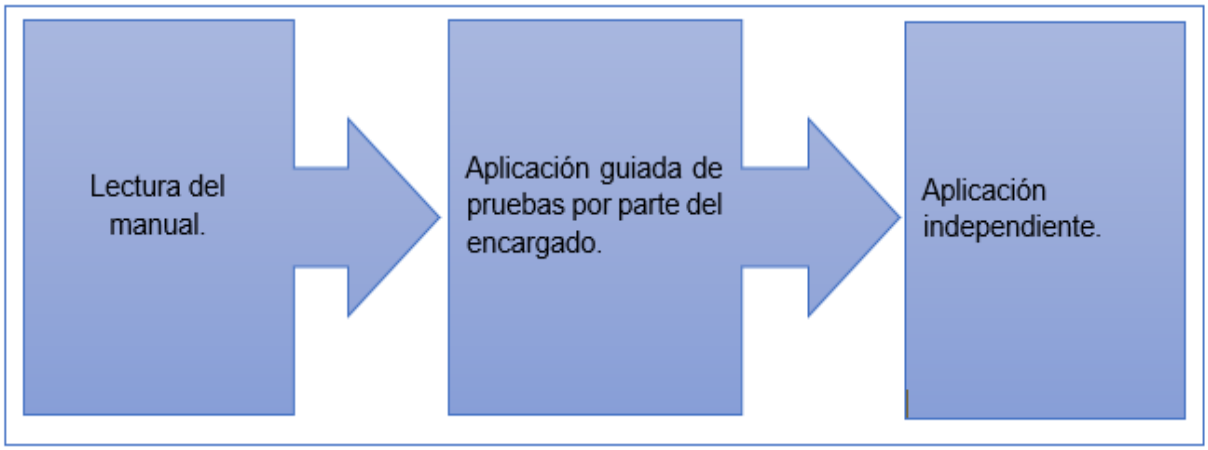
Rol	Función
Gerente de TI	Es el responsable de velar por la actualización constante del manual, además de distribuir la última versión a los colaboradores de TI.
Encargado de auditoría	Apoyar a los asistentes y nuevos colaboradores con el estudio del manual y las dudas que se presenten en el proceso.
Asistente de auditoría	Leer y comprender el manual, en caso de identificar debilidades en temas específicos, ampliar el conocimiento con las fuentes sugeridas.
Nuevo colaborador	Cumplir con el cronograma de estudio en el apartado 5.3 Cronograma de estudio.

Nota: Elaboración propia.

5.3 Cronograma de estudio

Este apartado aplica para asistentes de nuevo ingreso, para el equipo actual de auditoría pueden consultar el manual según las necesidades que se le presenten en las auditorías, los nuevos asistentes deben seguir las fases indicadas en la Figura 5.1.

Figura 5.1 Aplicación del manual de auditoría de TI



Fuente: Elaboración propia.

Lectura del manual de auditoría de TI

Se estima cuatro horas por tema para leerlo y comprenderlo, al ser 30 temas, se ocupan 120 horas, y el día laboral es de ocho horas, dando como resultado 15 días laborales. En este proceso va a estar acompañado de un asistente o encargado por lo cual se puede apoyar en él para las consultas que se le presenten.

Aplicación guiada de pruebas por parte de encargado

El encargado de la auditoría procederá a irle asignando pruebas, empezando por pruebas no tan complejas, para las cuales el colaborador aplicará lo aprendido en el manual, además de tener el documento digital como guía, posteriormente el encargado procederá a revisar las pruebas y brindarle la retroalimentación necesaria. Para este proceso se consideran cuatro semanas o 20 días laborales.

Aplicación independiente

Después de concluir satisfactoriamente las dos fases anteriores, el colaborador está en la capacidad de desenvolverse por sí mismo, siempre contando con el manual como guía en caso de aclarar algún concepto en el momento de la aplicación de las pruebas de auditoría u otra actividad dentro del ciclo de auditoría del despacho.

5.4 Objetivos por alcanzar

En este apartado se explica cómo se alcanza o se pretende alcanzar los objetivos con la propuesta realizada.

5.4.1 Objetivo general

El objetivo general del proyecto consistía en:

Elaborar un manual de auditoría de tecnologías de información enfocado en el ciclo de auditoría de TI del Despacho, para utilizarlo como material de capacitación en los colaboradores del departamento de TI, logrando un nivel estandarizado de conocimientos técnicos que les permita desarrollarse exitosamente en sus actividades laborales, reduciendo el tiempo de aprendizaje de temas desconocidos o con bases técnicas insuficientes, tomando como referencia las mejores prácticas de la industria para TI.

El manual se realizó satisfactoriamente y se puede observar en el Apéndice L: Propuesta manual de auditoría de TI, dónde se abarca las cuatro fases que componen el ciclo de auditoría, además es basado en el estándar ISO 19011, se realizó un estudio para elegir los temas adecuados de tal manera que no se presenten temas desconocidos para el personal a la hora de realizar una auditoría, además se explican cuáles y como se deben evaluar los atributos por prueba y, por último, se sugiere la lectura de las fuentes de información tomadas para el desarrollo del tema para ampliar conocimiento, no obstante, con lo aprendido el en manual puede comprender y realizar las pruebas de auditoría.

5.4.2 Objetivos específicos

- Analizar el proceso actual de capacitación en el departamento de auditoría y consultoría de TI del Despacho, para tomarlo como la base del proyecto.

  Para esto se realizó una entrevista con el encargado de TI y así conocer las actividades que se realizan en cada fase, se seleccionaron 30 temas de TI, los cuales fueron aprobados por el gerente de TI, la minuta de la reunión se ubica en el Apéndice I Minuta de reunión N°1 con Gerente de TI y se le consultó al equipo de auditoría si ya ellos lo habían evaluado en su vida laboral, además de una revisión documental de 172 pruebas para extraer los atributos seleccionados por cada prueba.

- Comparar el ciclo de auditoría de TI, especialmente los procedimientos actuales de las pruebas de auditoría con las mejores prácticas de la industria de TI como lo es *COBIT* o *ITIL*, para contrastarlos y así proponer recomendaciones a los procesos actuales.

  Para los procedimientos se utilizaron los atributos seleccionados de cada prueba por tema de las 172 pruebas analizadas anteriormente y se compararon con fuentes como *ITIL, COBIT* 5 entre otras, las cuales se indican en el material complementario de cada tema, y se procedió a definir y explicar los atributos seleccionados, en caso de los atributos de estructura se indica la estructura esencial para cada tema. Esta información se ubica en el manual de auditoría.

- Confeccionar los procedimientos de aplicación de las pruebas de auditoría de TI, para aplicarlos en los clientes del Despacho, además de apoyar el proceso de conocimiento y aprendizaje de los colaboradores.

El formulario aplicado al equipo de TI también sirvió como base para seleccionar las fuentes de información tomadas en cuenta a la hora de confeccionar los procedimientos de aplicación, con su respectiva explicación para un correcto entendimiento de los conceptos.

- Integrar los procedimientos creados con la explicación de cada una de las fases del ciclo de auditoría de TI en un manual de auditoría de TI, para el estudio y aplicación en su labor diaria.

  Con base en el estándar *ISO* 19011 y *COBIT* 5, se procedió a identificar, explicar y documentar las actividades realizadas en cada fase. Con la información contenida en el manual de auditoría de TI, el colaborador puede desenvolverse independientemente en sus labores diarias.

5.5 Propuesta del manual

Se procede a explicar los aspectos más relevantes del manual de auditoría de TI, la versión completa se puede observar en el Apéndice L: Propuesta manual de auditoría de TI.

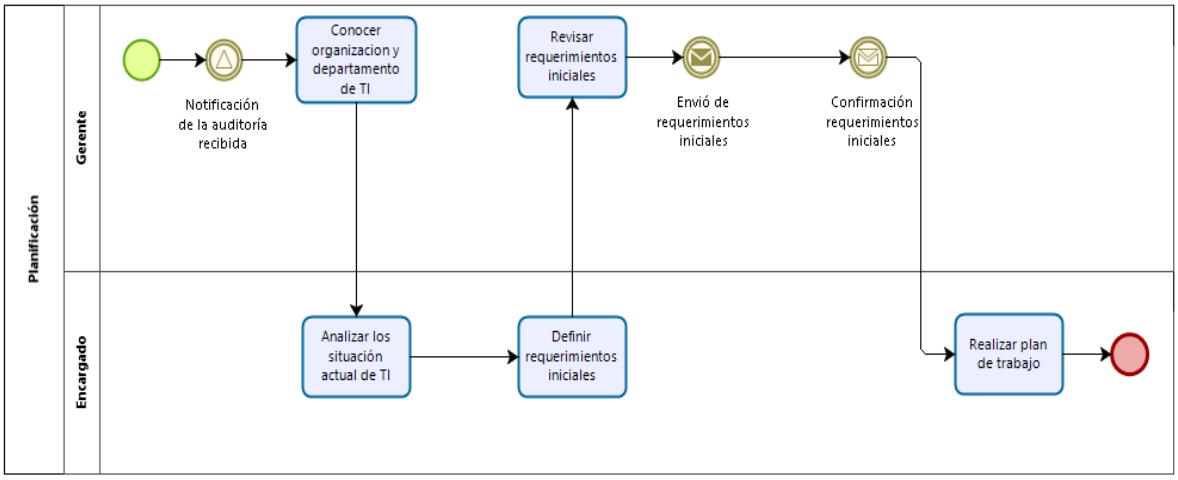
La fase de evaluación se procedió a implementar paralelamente al desarrollo del proyecto, se procedió a documentarla y formalizarla para asegurar el entendimiento del personal de TI.

Para la elaboración de los diagramas de los procedimientos, se utilizó un nivel de abstracción alto, dónde se toman en cuenta las validaciones y actividades principales con el fin de facilitar el entendimiento gráfico, no obstante, en la explicación del procedimiento se explica y detalla las actividades, además en caso de tener asociada una validación se procedió a explicarla.

5.5.1 Fase de planificación

Primeramente, se procede a diagramar la etapa de planificación, tal como se observa en la Figura 5.2.

Figura 5.2 Fase de planificación



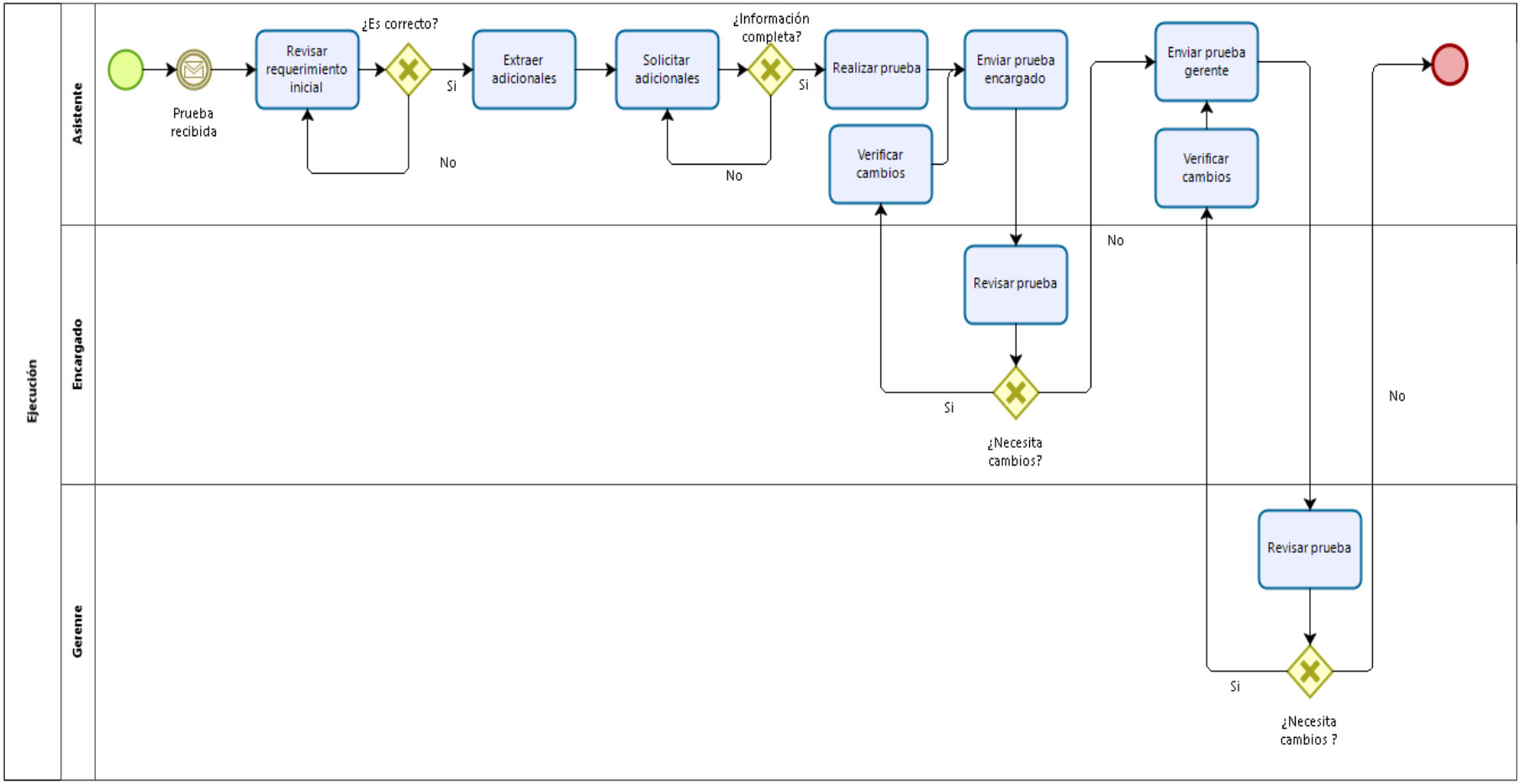
Fuente: Elaboración propia.

5.5.2 Fase de ejecución

Para esta fase primeramente se expone el procedimiento para realizar cualquier prueba dentro del despacho, en el manual se detalla el procedimiento específico de cada tema, el cual se puede observar en el Apéndice L: Propuesta manual de auditoría de TI.

El procedimiento que conlleva realizar una prueba de auditoría de TI se puede observar en la Figura 5.3, ubicada en la siguiente página.

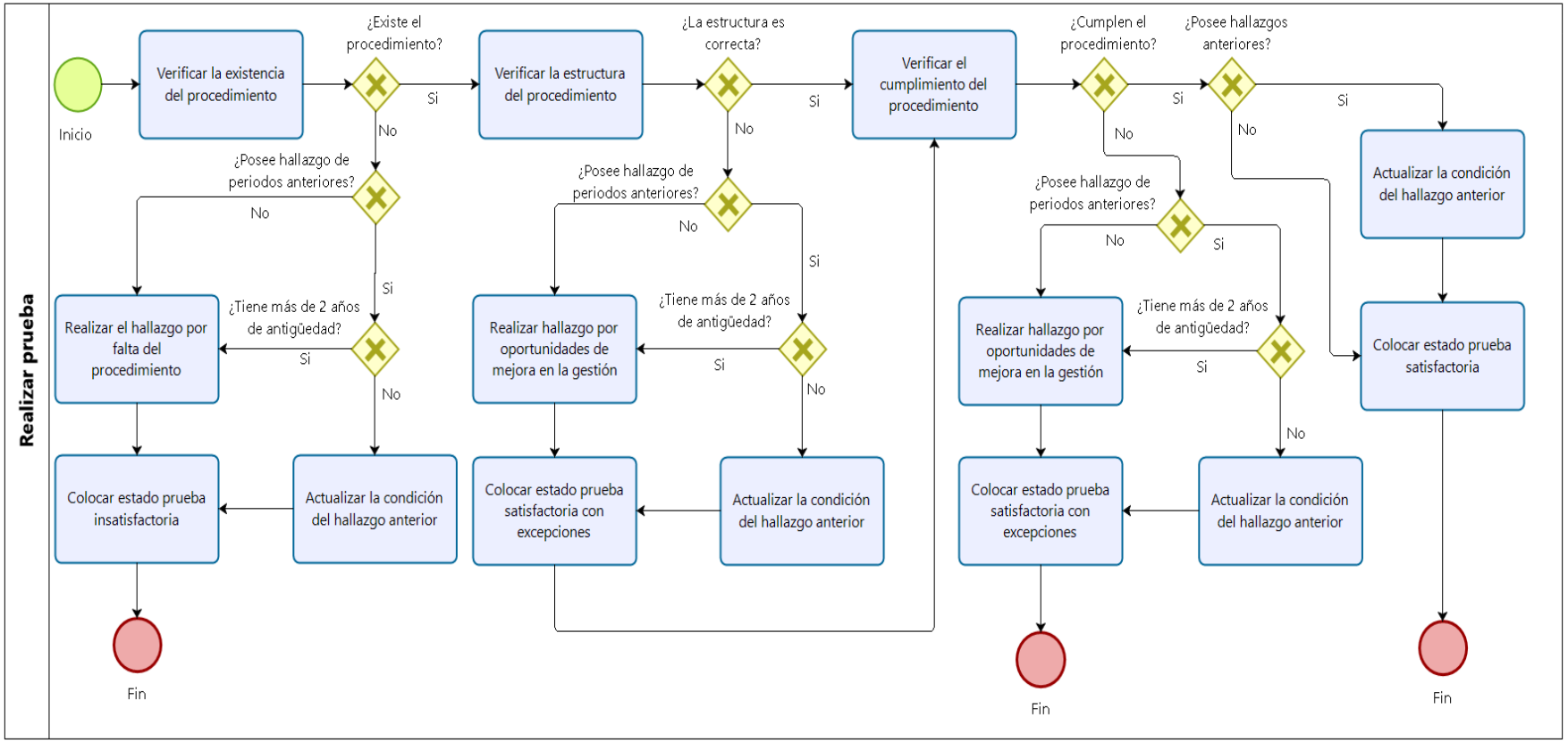
Figura 5.3 Fase de Ejecución



Fuente: Elaboración propia.

Además, el procedimiento específico de realizar una prueba de auditoría se puede observar en la Figura 5.4, no obstante, es una representación estándar, para observar la representación de cada tema por favor dirigirse al Apéndice L: Propuesta manual de auditoría de TI.

Figura 5.4 Proceso estándar para realizar una prueba

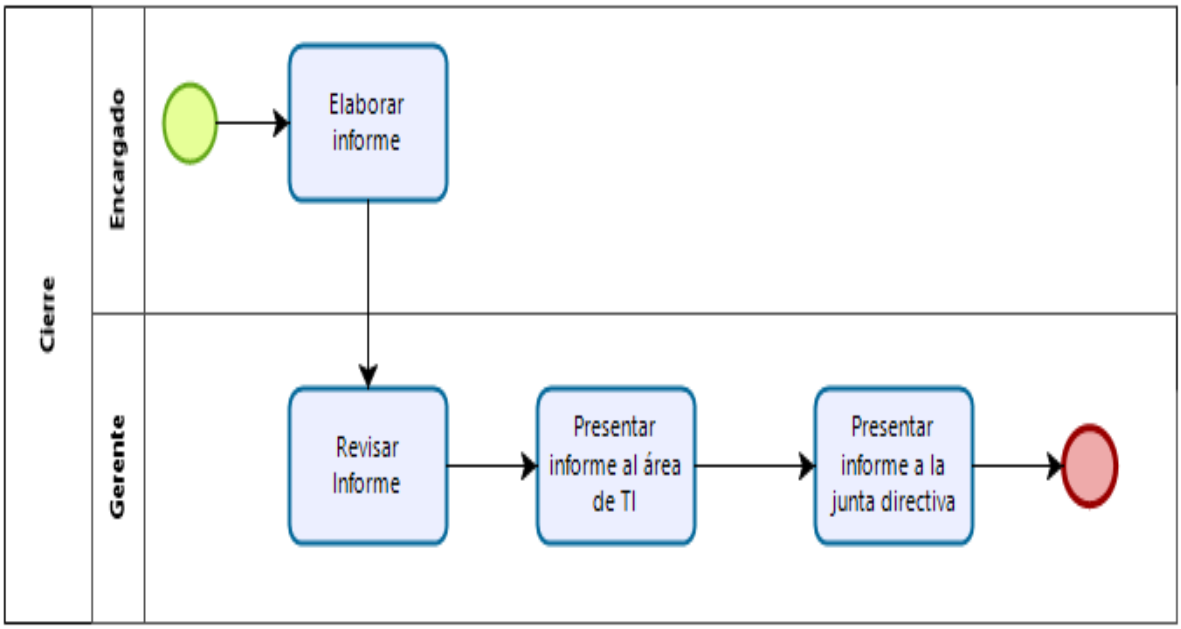


Fuente: Elaboración propia.

5.5.3 Fase de cierre

En la fase de cierre la actividad principal es la elaboración del informe, no obstante, hay dos presentaciones del informe a la organización dónde se realizó la auditoría, el gerente se encarga de la coordinación de las presentaciones y en caso de que se requiera de la presencia de un encargado o asistente él avisa al equipo de auditoría, en esta fase se documentan las reglas para realizar el informe para que cumpla con los lineamientos del despacho, en la Figura 5.5 se observa su representación gráfica.

Figura 5.5 Fase de cierre

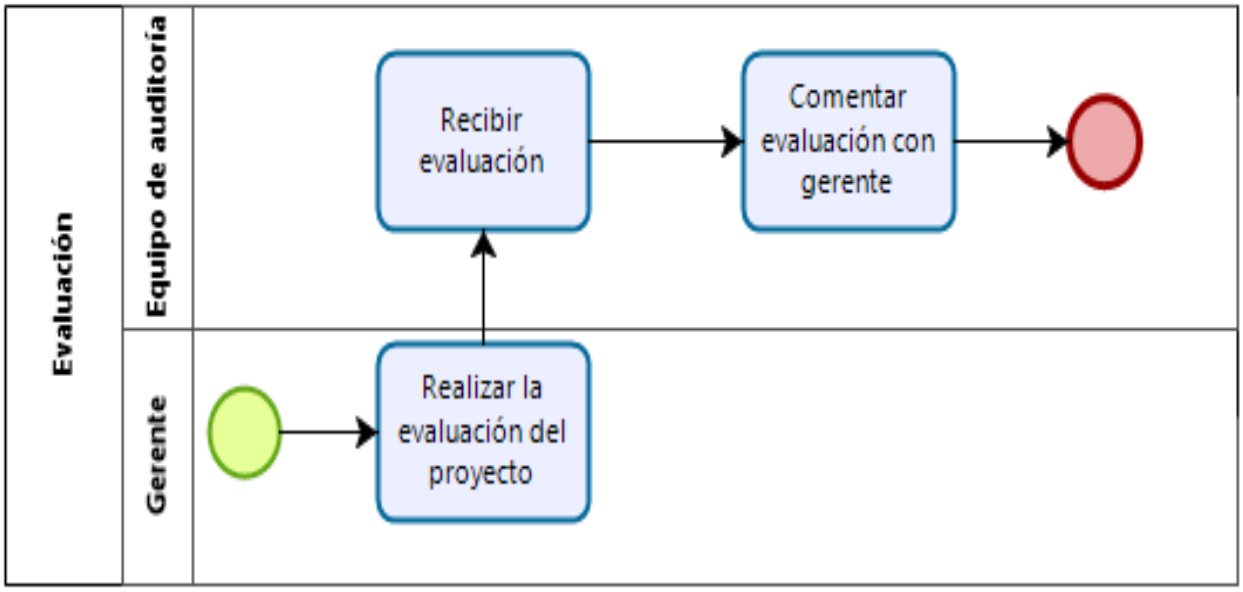


Fuente: Elaboración propia.

5.5.4 Fase de evaluación

En la fase de evaluación se procedió a explicar la evaluación utilizada actualmente, de tal manera que el auditor conozca con anticipación cuáles son los factores por evaluar, y como realizar su trabajo de la mejor manera de tal forma que la evaluación sea positiva, es importante mencionar que se evalúa el proyecto y no el desempeño de auditor solamente, por lo cual hay aspectos que no son responsabilidad directamente del equipo de auditoría, aun así se debe procurar que estas actividades sean ejecutadas satisfactoriamente, en la Figura 5.6 se observa su representación gráfica.

Figura 5.6 Fase de evaluación



Fuente: Elaboración propia.

Capítulo VI

Conclusiones

6. Conclusiones

En el presente capítulo se presentan las conclusiones producto del trabajo realizado, tomando en cuenta la información obtenida, el análisis aplicado y el seguimiento de la metodología propuesta, las conclusiones siguen el orden de los objetivos iniciando por los específicos y finalizando con el objetivo general.

6.1 Actualmente, el departamento de auditoría de TI no cuenta con un procedimiento formalmente establecido para la capacitación de los colaboradores, por lo cual se utiliza material complementario de otros autores y fuentes como *ITIL* o *COBIT* 5, además de la normativa vigente. El proceso de capacitación para los nuevos colaboradores depende del encargado asignado y la metodología que él defina.

6.2 Se identificó que el despacho cuenta con un sitio propio de *E-learning,* no obstante, este actualmente no está en funcionamiento, por lo cual no existe un mecanismo de capacitación y evaluación para detectar las áreas débiles de los colaboradores.

6.3 Se determinó que el proceso actual de auditoría no está formalmente documentado, no obstante, si se cuenta con las instrucciones del gerente y los encargados, los cuales se encargan de comunicarlo a los asistentes, al ser transmitido verbalmente se tienen tareas que se realizan diferente según el encargado asignado.

6.4 Al realizar la comparación del ciclo actual de auditoría de TI, se determinó que está alineado con las mejores prácticas del sector como lo es la *ISO* 19011 y el proceso de evaluación establecido por *COBIT* 5, no obstante, producto del análisis realizado se ajustó el procedimiento documentado con las mejores prácticas, las cuales fueron aprobadas por el gerente de TI.

6.5 Respecto al procedimiento de las pruebas, se realizó un estudio sobre 172 pruebas de 10 auditorías realizadas por el despacho en diferentes sectores, producto de este estudio se obtiene que los atributos comunes para 25 de los 30 temas seleccionados en el manual son: existencia del procedimiento, estructura y cumplimiento de este, por lo que se concluye que el 83.33% de las pruebas consisten en revisar un procedimiento, metodología o lineamiento.

6.6 Al confeccionar los procedimientos de aplicación para las pruebas de auditoría de TI, se determina que los atributos establecidos para evaluar el tema en estudio están basados en la normativa aplicable, las cuales están alineados a *COBIT* 5, sin embargo, en el momento de evaluar la estructura y proceder a realizar el hallazgo en caso de que sea insatisfactoria o no se tenga, se realiza las recomendaciones del hallazgo con base en *COBIT* 5 e *ITIL*, en casos como PETI, arquitectura de TI, y gobierno de TI, se toma como referencia libros específicos del tema, los cuales son indicados en la propuesta del manual de auditoría de TI.

6.7 Respecto a la fuente información de *Google* se obtiene que en el 50% de las pruebas un auditor de TI consultaría esta fuente, en el 36.67 % dos auditores consultarían y el restante 13.34% se divide en partes iguales correspondiente a dos pruebas dónde tres auditores consultarían, y solamente en dos pruebas los auditores no tendrían necesidad de consultar este buscador, con lo que se concluye que los auditores a pesar de conocer fuentes como *ITIL* o *COBIT* 5 acuden al buscador por material más entendible y aplicable a las organizaciones evaluadas.

6.8 Se evidenció que el 75% de los auditores de TI no han aplicado una prueba referente al gobierno corporativo de TI, y solamente el 25% consultaría en una fuente específica del tema como lo es la *ISO* 38500 y *King* III, el 75% restante desconocía de estas fuentes.

6.9 Se logró la integración de los procedimientos creados para los temas abarcados y el ciclo de auditoría, por lo cual el departamento de TI contará con un proceso de capacitación de manera guiada y estandarizada para su aplicación posterior.

6.10 Producto del formulario aplicado por medio de la herramienta *Google form*, se determinó que en el 100% de las pruebas, los auditores consultan a una fuente externa, si la fuente consultada no está disponible o no resuelve su duda, el auditor debe esperar la disponibilidad del encargado o del gerente de TI. Con el manual propuesto de auditoría de TI las dudas que tengan los auditores relacionadas a la aplicación técnica serán inmediatamente resueltas.

6.11 Para finalizar, se concluye que el ciclo de auditoría de TI no está automatizado, ya que el control se realiza por correo electrónico y la gestión de las actividades se lleva en plantillas de Excel propias de cada auditor.

Capítulo VII

Recomendaciones

7. Recomendaciones

Producto de realizar el trabajo final de graduación se indican las recomendaciones identificadas, las cuales permitirán mejorar las actividades de la organización con base en la problemática planteada y objetivos establecidos.

7.1 Se recomienda aplicar el procedimiento establecido en la propuesta del manual de auditoría de TI para la capacitación de los colaboradores, de tal forma que el procedimiento por aplicar de aquí en adelante sea estandarizado y sin ambigüedades.

7.2 Se deben establecer indicadores de desempeño del proceso de auditoría de TI tales como: tiempo de realizar la prueba, tiempo de corrección, pruebas realizadas por período, los cuales están relacionadas al proceso de auditoría de TI, permitiendo obtener mejores resultados durante las aplicaciones de las auditorías futuras.

7.3 Gestionar la habilitación del *e-learning,* para apoyar el proceso de capacitación de los auditores de TI, además se recomienda, agregar un apartado de evaluaciones para verificar el conocimiento adquirido por los auditores.

7.4 Dentro del proceso de mejora continua, se recomienda actualizar el manual de auditoría de TI cada vez que se detecte una oportunidad de mejora, considerando las mejores prácticas y normas sobre procesos de gestión de auditoría, de tal manera que permita al despacho contar con procedimientos actualizados.

7.5 En caso de nuevas actualizaciones a la normativa nacional o *COBIT* e *ITIL*, se debe verificar si es requerido agregar un nuevo tema y de ser así gestionar su inclusión de manera inmediata.

7.6 Dentro del manual de auditoría de TI se incluye el apartado de material complementario, el cual abarca fuentes específicas de información por cada tema, se recomienda actualizarlos anualmente con el fin de actualizar las fuentes incluidas, las cuales incluyen libros, estándares, normas, reglamentos entre otros.

7.7 Cuando las fuentes de *ITIL* y *COBIT* 5 no resuelvan las dudas de los auditores, se recomienda la lectura del apartado de fuentes complementarias, eliminando el uso del buscador *Google* para prevenir información de fuentes inexactas y con información errónea.

7.8 Se recomienda la aplicación de una capacitación a los colaboradores del departamento de TI actuales y futuros relacionado con el de tema gobierno corporativo de TI, tomando como referencia *King* III y la *ISO* 38500.

7.9 Se recomienda someter el manual en su totalidad a una revisión a principios de cada año, con el fin de verificar y actualizar los temas incluidos en este, producto de los cambios que se presenten relacionados con las buenas prácticas y normativa de TI.

7.10 Se recomienda automatizar las actividades del ciclo de auditoría de TI, permitiendo un control más preciso de la gestión de las auditorías de TI, y de las actividades realizadas por los auditores.

7.11 Se recomienda realizar un repositorio de información, en el mismo se debe almacenar el material de estudio referente a cada tema.

7.12 Para finalizar, se recomienda al gerente de TI realizar reuniones mensuales entre los miembros del departamento de TI, en los cuales se pueda conversar acerca de las debilidades y oportunidades de mejora detectadas en las aplicaciones de las auditorías de TI.

Lista de Referencias

8. Lista de referencias

AENOR. (2009). *ISO/IEC 20000. Guía completa de aplicación para la gestión de los servicios de tecnologías de la información.* España: AENOR.

Aguayo, P. (21 de Noviembre de 2013). *Los manuales administrativos como herramienta clave*. Obtenido de https://www.gestiopolis.com/los-manuales-administrativos-como-herramienta-clave

Álvarez, A. J. (2017). *Propuesta de definición de controles de auditoría y pruebas sustantivas para la evaluación del proceso de Gestión del Cambio en las organizaciones auditadas, Caso JM Auditores.* Cartago: Tecnológico de Costa Rica.

Arens, A., Elder, R., & Beasley, M. (2007). *Auditoría un enfoque integral* (11 ed.). Naucalpan de Juárez México: Pearson Edication.

Auditoría Superior del Estado de Chihuahua. (2013). *Auditoriachihuahua.gob.mx*. Obtenido de http://www.auditoriachihuahua.gob.mx/portal/wp-content/uploads/2013/08/GUIA_DE_AUDITORIA_DE_TI.pdf

Bon, J., Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Veen, A., & Verheijen, T. (2008). *Gestión de Servicios TI basado en ITIL® V3 - Guia de Bolsillo.* Zaltbommel: Van Haren Publishing.

Cámara Valencia. (2018). *Tecnología para los negocios*. Obtenido de https://ticnegocios.camaravalencia.com/servicios/tendencias/la-importancia-de-hacer-una-auditoria-de-tecnologia-en-las-pymes/

Cannon, D., Wheeldon, D., Lacy, S., & Hanna, A. (2013). *ITIL service strategy.* London: TSO.

Cassidy, A. (2006). *A Practical Guide to Information System Strategic Planning* (Segunda ed.). 6000 Broken Sound Parkway NW, Suite 300: Auerbach Publications.

Cesár, J. (23 de Septiembre de 2012). *Modelado de Negocios: BPMN (Business Process Modeling Notation)*. Obtenido de

https://juliocesarfx.wordpress.com/2012/09/23/modelado-de-negocios-bpmn-business-process-modeling-notation/

Chiavenato, I. (2009). *Comportamiento organizacional* (2 ed.). Colonia Desarrollo Santa FE, México: McGraw Hill.

CONASSIF. (2010). *Consejo Nacional de Supervisión del Sistema Financiero*. Obtenido de http://conassif.fi.cr/

Contraloría General de la República. (2007). *Normas técnicas para la gestión y el control de las tecnologías de información.*

Contraloría General de la República de Perú. (2010). *Orientaciones Básicas para el Fortalecimiento del Control Interno en Gobierno Locales.* Los Incas 172.

Contraloria.gob.ec. (s.f.). Obtenido de http://www.contraloria.gob.ec/documentos/normatividad/MGAG-Cap-VI.

Corte de Cuentas de la República. (2011). *http://bibliotecavirtual.olacefs.com/gsdl/cgi-bin/library.cgi?l=es*. Obtenido de Manual de Auditoría de Gestión a las Tecnologías de Información y Comunicaciones: http://bibliotecavirtual.olacefs.com/gsdl/collect/guasyman/archives/HASH0155.dir/ManualAuditoriaGestionTICs.pdf

Despacho Carvajal. (2018). *Firma de Contadores Públicos en Costa Rica | Despacho Carvajal*. Obtenido de Carvajalcr.com: https://www.carvajalcr.com/

Dle.rae.es. (2017). *Diccionario de la lengua española*. Obtenido de Definición de Auditoría: http://dle.rae.es/?id=4NVvRTc

Dle.rae.es. (2017). *Dicicionario de la lengua española*. Obtenido de Definición de Manual: http://dle.rae.es/?id=UErw6id

Echenique, J. A. (2001). *Auditoría en informática* (2 ed.). México: McGraw-Hill.

Editorial Definición MX. (11 de Abril de 2014). *Definición MX*. Obtenido de https://definicion.mx/manual/

Escuela Europea de Excelencia. (2016). *Nuevas Normas ISO*. Obtenido de https://www.nueva-iso-9001-2015.com/

Espinoza, S. (2009). *Auditoría de aplicaciones informáticas* (1 ed.). San José: Editorial UCR.

Franklin, E. B. (2007). *Auditoría administrativa. Gestión estratégica del cambio* (2 ed.). Naucalpan de Juárez, México: PEARSON EDUCACIÓN,.

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la investigación* (6 ed.). México: McGraw-Hill.

Hitpass, B. (2017). *Business Process Management (BPM) Fundamentos y Conceptos de Implementación* (Cuarta ed.). Santiago de Chile: BHH Ltda.

Hunnebeck, L. (2013). *ITIL Service Design.* London: TSO, The Stationery Office.

Instituto de normas técnicas de Costa Rica. (2012). *INTE/ISO/IEC 27005:2012* (Primera ed.). INTECO.

ISACA. (2012). *COBIT 5 Implementación.* Rolling Meadows, IL 60008 EE.UU.

ISACA. (2012). *COBIT 5 para Seguridad de la Información.* Rolling Meadows, IL 60008 EE.UU.

ISACA. (2012). *COBIT 5: Procesos Catalizadores.* Rolling Meadows, IL 60008 EE.UU.

ISACA. (2012). *COBIT 5: Un Marco de Negocio de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Rolling Meadows, IL 60008 EE.UU.

ISACA. (2013). *COBIT 5 para Aseguramiento.* Rolling Meadows, IL 60008 EE.UU.

ISACA. (2013). *COBIT 5 para Riesgos.* Rolling Meadows, IL 60008 EE.UU.

ISACA. (2013). *COBIT Guía del Evaluador: Usando COBIT 5.* Rolling Meadows, IL 60008 EE.UU.

ISO. (2003). *Iso.org*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso:10007:ed-2:v1:es

ISO. (2011). *ISO 19011 Directrices para la auditoría de Sistemas de Gestión.* Suiza.

Iso27000.es. (2005). *Iso27000.es*. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

Lloyd, V., Wheeldon, D., Lacy, S., & Hanna, A. (2013). *ITIL continual service improvement.* London: TSO.

Madariaga, J. (2004). *Manual Práctico de Auditoría.* Barcelona: Ediciones Deusto.

Mantilla, S. (2003). *Auditoría 2005* (1 ed.). Colombia: Ecoe Ediciones.

Martínez, H. (2012). *Metodología de la investigación.* Col. Cruz Manca, Santa Fe: Cengage Learning Editores.

Rance, S., Rudd, C., Lacy, S., & Hanna, A. (2013). *ITIL Service Transition.* London: TSO.

SUGEF. (2017). *SUGEF 14-17 Reglamento general de gestión de la tecnología de información.*

Terry, G. (1984). *Principios de administración* (6 ed.). Buenos Aires: El Ateneo.

Terry, G., & Franklin, S. (1999). *Principios de administación* (4 ed.). México D.F.: Editorial Continental.

Toro, R. (22 de enero de 2016). *Nuevas Normas ISO*. Obtenido de ISO 9001 2015 Diferencias entre proceso y procedimiento: https://www.nueva-iso-9001-2015.com/2016/01/iso-9001-2015-diferencia-proceso-procedimiento/

Torres Hernández, Z. (2014). *Teoría general de la administración* (2 ed.). Colonia San Juan Tlihuaca: Grupo Editorial Patria.

Ulate Soto, I., & Vargas Morúa, E. (2016). *Metodología para elaborar una tesis.* San José, Costa Rica: EUNED.

Umc.edu.ve. (2011). Obtenido de http://www.umc.edu.ve/pdf/calidad/normasISO/Norma_ISO_19011-2011_Espanol.pdf

Van Bon, J., & Redwood, Q. W. (2010). *Fundamentos de ITIL® V3.* [Netherlands]: Van Haren Publishing.

Glosario

9. Glosario

- Auditor: Persona que efectúa una auditoría.
- Auditoría: Examen de las operaciones de una empresa por especialistas ajenos a la operación y con objetivos de evaluar el ambiente de control y la situación de esta.
- Bases de Datos: Colección de datos organizados para que a través de las aplicaciones y programas la computadora pueda acceder rápidamente a ella.
- COBIT: Objetivos de Control para la Información y las Tecnologías Relacionadas.
- Confidencialidad: Se refiere a que la información sólo puede ser conocida por individuos autorizados.
- Control Interno: Conjunto de objetivos, políticas, procedimientos y registros con el propósito de procurar mecanismos adecuados de operación, acordes con las estrategias y fines de las instituciones, que permitan identificar, dar seguimiento y evaluar los riesgos que puedan derivarse de las actividades del negocio, con propósito de reducir las pérdidas en que puedan incurrir en la realización de actos o hechos voluntarios o involuntarios.
- Hardware: Conjunto de dispositivos físicos de los que consiste un sistema. Comprende componentes tales como el teclado, el mouse, las unidades de disco, el monitor, cada una de las partes físicas que forman un ordenador, incluidos sus periféricos.
- Integridad: La habilidad de determinar que la información recibida es la misma que la información enviada.
- Investigación: Representa la obtención de información, datos y comentarios de los funcionarios y empleados de la empresa.
- I.S.A.C.A: *Information Systems Audit and Control Association* (Asociación de Auditoría y Control de Sistemas de Información).
- ISO: (Organización Internacional para la Normalización) Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática y las

comunicaciones. Está formada por las organizaciones de normalización de sus 89 países miembro.

- Medidas: Son medidas cuantitativas del desempeño del negocio utilizado por la alta gerencia para supervisar el negocio, obtener información y proporcionar retroalimentación. Una medida es efectiva cuando es parte de un proceso de supervisión que incluye objetivos y parámetros de acción o de excepción.
- Metodología: Conjunto de pasos utilizados para lograr un objetivo.
- Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- Observación: Presencia física de cómo se realizan ciertas operaciones o hechos.
- Papeles de trabajo: Registro del trabajo del auditor, el cual contiene la evidencia del trabajo realizado, sus observaciones y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado y para respaldar la opinión del auditor. Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.
- Planeación: Consiste en prever cuales procedimientos de auditoría va a emplearse, la extensión y oportunidad en que van a ser utilizados y el personal que debe intervenir en el trabajo.
- Política: Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.
- Procedimiento: Método o sistema estructurado para la ejecución de actividades.
- Proceso: Conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.
- Programa: Secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.
- Seguridad de la Información: Se refiere a la confidencialidad, integridad y disponibilidad de la información y datos, independientemente de la forma, los datos pueden ser: electrónicos, impresos, audio u otras formas.

- Servidor: Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin.
- Software: Componentes inmateriales del ordenador: programas, sistemas operativos, etc. Son aquellos programas que nos ayudan a tareas específicas como edición de textos, imágenes, cálculos, etc. también conocidos como aplicaciones.
- TI: Tecnologías de Información. Conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.
- Auditoría de Tecnologías de Información: Se encarga de la verificación de los controles internos establecidos en el área de sistemas del ente, así como estudios de seguridad de la información, hardware y software.
- Recursos Informáticos: Son todos aquellos componentes de hardware y software, así como el personal que labora en él, o para el área de sistemas.

Apéndices

10. Apéndices

Esta sección contiene todos los elementos que permiten apoyar el entendimiento de este trabajo y fueron desarrollados en este proyecto.

Apéndice A: Formato de entrevistas

A continuación, se procede a indicar el formato utilizado para documentar las entrevistas realizadas durante el proyecto.

Tema de la entrevista:		
Entrevista N°:		
Tipo de entrevista:		
Modalidad:		
Lugar:		
Fecha:		
Hora de inicio:		
Hora de finalización:		
Participantes:	**Participante:**	**Puesto:**
Preguntas		
1. ¿Pregunta #1?		
Respuesta:		
2. ¿Pregunta #2?		
Respuesta:		
3. ¿Pregunta #3?		
Respuesta:		
4. ¿Pregunta #4?		
Respuesta		

Apéndice B: Entrevista ciclo actual de auditoría

En el siguiente apéndice se procede a documentar la entrevista que se obtuvo con uno de los encargados del despacho, su finalidad es conocer el ciclo actual de auditoría de TI.

Tema de la entrevista: Ciclo actual de auditoría de TI		
Entrevista N°:	1	
Tipo de entrevista:	Semi estructurada	
Modalidad:	Presencial	
Lugar:	Despacho Carvajal	
Fecha:	21/9/2018	
Hora de inicio:	08:00 a.m.	
Hora de finalización:	09:30 a.m.	
Participantes:	**Participante:**	**Puesto:**
	Carlos Ramírez Cerdas	Desarrollador del proyecto
	Diego Sánchez Quirós	Encargado de auditoría
Preguntas		
1. ¿Se cuenta con un procedimiento de auditoría formalmente establecido?		
Respuesta:	Actualmente no se cuenta con un procedimiento formalmente establecido, sin embargo, el gerente de TI y los auditores encargados nos encargamos de enseñar el procedimiento seguido a los nuevos asistentes. El conocimiento del proceso de auditoría es tácito, por lo que existe una dependencia de personal con experiencia para replicar los procesos. Sin embargo, al no existir un estándar, algunas actividades se pueden interpretar de diferente, por lo que en algunas ocasiones se deben corregir pruebas o añadir más información.	

2. ¿Cuáles son las fases del ciclo de auditoría actualmente?	
Respuesta:	Se cuenta con tres fases principales las cuales son: -Planificación. -Ejecución. -Cierre.
3. ¿Cuáles son las actividades que se realizan en la primera fase?	
Respuesta:	Dentro de las actividades realizadas en la fase de planificación se encuentran las siguientes: -Conocimiento de la organización y del área de tecnología de información. -Análisis de riesgos de TI y organizacional. -Análisis y evaluación de la situación actual. -Definición requerimientos iniciales del periodo auditado. -Elaboración del plan de trabajo. (Se realizan las actividades de pruebas, entrevistas, cronogramas y se asignan responsables).
4. ¿Cuáles son las actividades que se realizan en la segunda fase?	
Respuesta:	Dentro de las actividades realizadas en la fase de ejecución se encuentran las siguientes: -Presentación del personal de trabajo, tanto de la auditoría como de la organización, para establecer los contactos requeridos para ejecutar el estudio. -Verificar requerimientos iniciales. -Solicitar requerimientos adicionales. -Ejecución de las pruebas de cumplimiento y sustantivas. -Revisión de los sistemas de información. -Seguimiento recomendaciones de períodos anteriores. -Redacción del informe.
5. ¿Cuáles son las actividades de la tercera fase?	
Respuesta	Dentro de la fase de cierre se encuentran las siguientes actividades: -Discusión del informe preliminar de auditoría con el cliente. -Discusión del estado de los hallazgos. -Generación del informe de auditoría final. -Presentación del informe al gerente del despacho. -Presentación del informe ante el área de TI. -Presentación del informe a la junta directiva.

6. ¿Cuáles son las actividades de la cuarta fase?	
Respuesta	Cabe mencionar que estas etapas no están documentadas formalmente, por lo que se puede decir a grandes rasgos que son 3 fases, no obstante, desde el punto de vista de otra persona, el proceso se puede dividir en más fases, eso depende cómo se clasifiquen las tareas o actividades mencionadas. Se podría decir que una cuarta fase es el control que realiza el gerente de auditoría de TI a lo largo de todo el proyecto.
7. ¿Cómo evalúan a los auditores después de realizado el proyecto?	
Respuesta	Se está empezando un mecanismo de evaluación por auditoría. Dicha evaluación consiste en una herramienta con las actividades de cada una de las fases anteriormente indicadas a las cuales se les da una calificación entre 1 y 5 puntos, siendo este último la mejor calificación para la actividad. El objetivo de esta herramienta no es evaluar el desempeño del auditor, sino que busca medir la mayor cantidad de variables que pudieron afectar el proyecto, de modo que se puedan determinar las lecciones aprendidas y se pueda mejorar el proceso de auditoría. Este proceso se encuentra recién implementado, por lo que no se ha determinado la efectividad de esta.
8. ¿Qué otro aspecto considera importante dentro del ciclo de auditoría?	
Respuesta	-Proceso de revisión y retroalimentación por parte del Gerente de Auditoría de TI. -Revisión de la seguridad física y ambiental del cuarto de servidores. -Respaldo de la información de auditoría (quemar un CD con la información de auditoría para que el despacho resguarde la información del proyecto junto con los resultados.

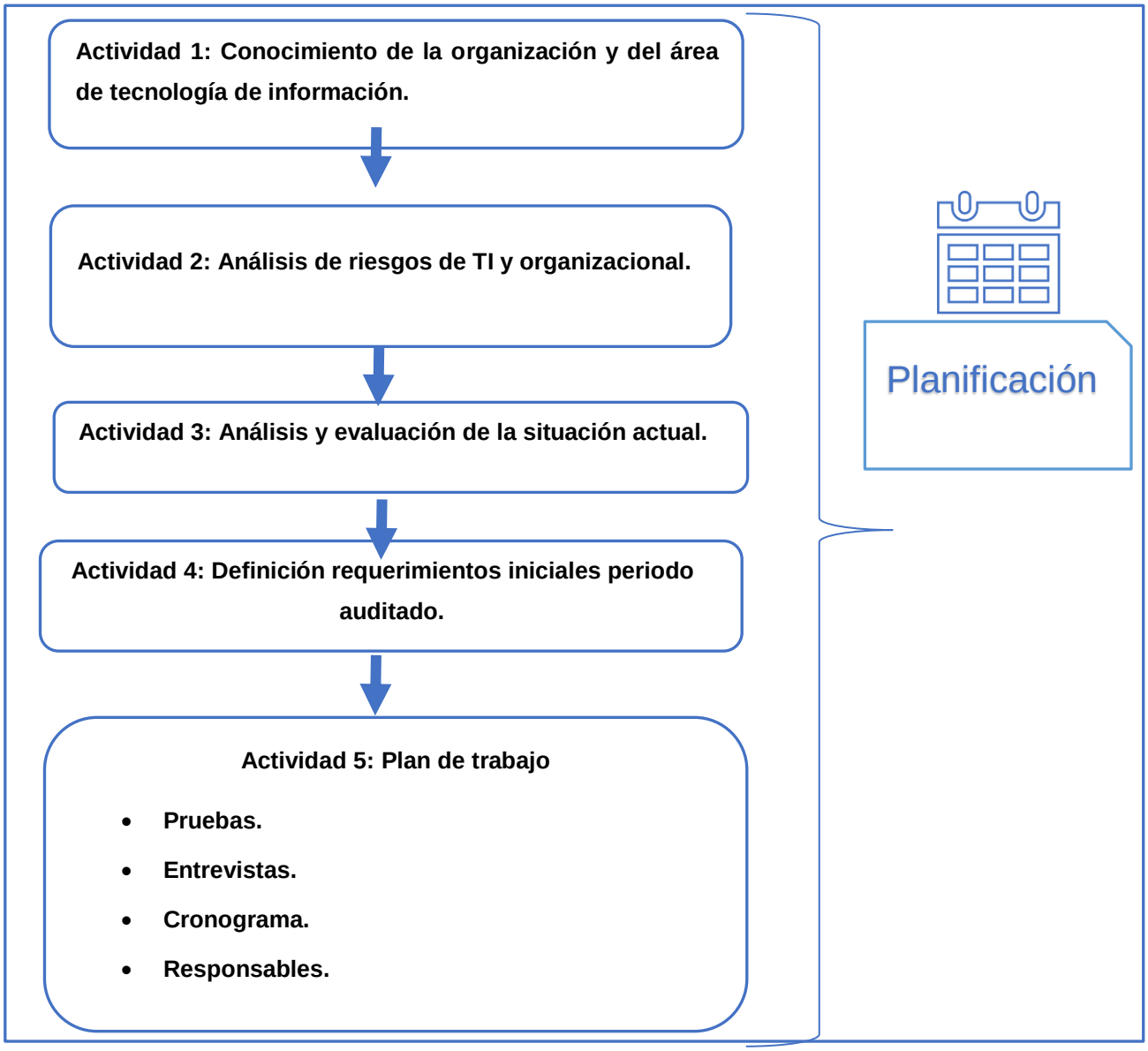
Apéndice C: Entrevista proceso de capacitación.

Tema de la entrevista: Proceso de capacitación		
Entrevista N°:	2	
Tipo de entrevista:	Semi estructurada	
Modalidad:	Presencial	
Lugar:	Despacho Carvajal	
Fecha:	26/09/2018	
Hora de inicio:	14:00	
Hora de finalización:	14:30	
Participantes:	**Participante:**	**Puesto:**
	Carlos Ramírez Cerdas	Desarrollador del proyecto
	Nancy Saborío Alfaro	Auditora de TI
Preguntas		
1. ¿Como fue su proceso de capacitación al ingresar al despacho?		
Respuesta:	Mi proceso de capacitación en el despacho inició con una inducción de las normativas internas de la empresa, luego recibí capacitación por parte de los encargados aproximadamente de una semana de las plantillas de pruebas como completar la información, esquemas de trabajo, actividades administrativas, entre otras tareas.	
2. ¿Se cuenta con un procedimiento formal de capacitación?		
Respuesta:	No se cuenta con un procedimiento formal de capacitación, los encargados realizan la capacitación con base a su experiencia.	
3. ¿Se tienen definido prioridades de capacitación, temas o áreas?		
Respuesta:	Desconozco el tema de priorización en las capacitaciones.	
4. ¿Hay un plan de capacitación establecido?		
Respuesta:	En el proceso de inducción del despacho, me comentaron que una vez al año realizan capacitaciones a los colaboradores. Si embargo, no tengo conocimiento del plan de capacitación.	

Apéndice D: Ciclo actual de auditoría

Se procede a explicar las actividades del ciclo actual de auditoría.

Etapa de planificación



Fuente: Elaboración propia con base en Despacho Carvajal (2018).

La primera etapa de las auditorías es la planificación, se puede decir que la parte de negociación o participación del concurso de licitación en el caso del sector público es una pre-fase, sin embargo, se incluirá como parte de la planificación.

A continuación, se procede a mencionar las actividades principales de la fase de planificación.

Mercadeo

Si bien es cierto esta actividad no forma parte del ciclo de auditoría, si es importante completarla con éxito para poder iniciar una auditoría en los clientes. Por lo que se procede a explicarla.

Existen dos tipos de clientes, cuando el cliente es del sector público, la participación se realiza por licitación pública, para este caso el gerente, junto a otros miembros del Despacho están pendientes de las licitaciones para así participar y presentar una propuesta de acuerdo con lo solicitado en el cartel. En el caso de los clientes privados se realiza según las condiciones establecidas por el cliente, ya sea por reuniones, propuestas, concursos u otros, para esto el gerente es el encargado de cerrar el trato de una manera positiva.

Conocimiento de la organización y del área de tecnología de información

Una vez ganada la licitación o cerrado un trato con un cliente privado, se realiza una investigación rápida de la organización, a que se dedica, si ha sido cliente en periodos anteriores, dónde se ubican las oficinas, dónde se va a ubicar el equipo de trabajo, quién es el encargado del área tecnológica, ya que las auditorías por lo general son solicitadas por la junta directiva.

Seguimiento de hallazgos y recomendaciones de informes de auditorías anteriores

Se solicitan los informes de periodos anteriores con el fin de ver su situación anterior.

Análisis y evaluación de la situación actual

Se evalúan los requerimientos actuales y su contexto en la organización.

Definición requerimientos iniciales periodo auditado

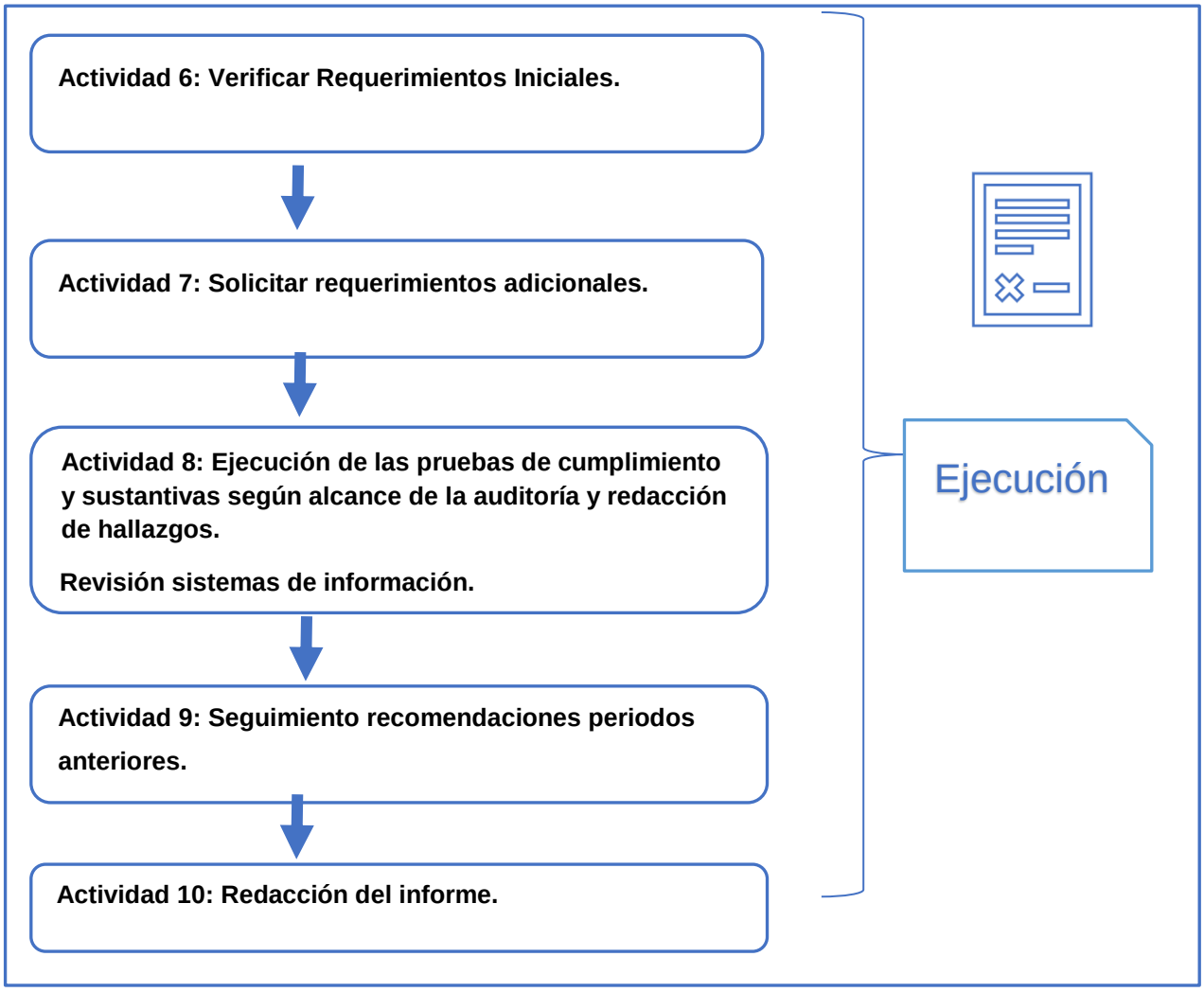
A partir de los informes anteriores y la situación actual se definen los requerimientos iniciales, con los cuales la auditoría empezaría a trabajar.

Plan de trabajo

El plan de trabajo es responsabilidad del encargado de la auditoría, para esto cuenta con dos asistentes, el cual definirá la forma de trabajar, definiendo los siguientes puntos:

- Pruebas: Cuáles pruebas se van a realizar, unificando requerimientos iniciales.
- Entrevistas: Tanto de los sistemas en producción como el centro de datos.
- Cronograma: Fechas límites tanto para los asistentes como para la entrega del informe actual.
- Responsables: Asigna quién va a realizar las pruebas y entrevistas.

Etapa de ejecución



Fuente: Elaboración propia con base en Despacho Carvajal (2018).

Esta etapa es las más importante ya que es dónde el asistente de auditoría se desarrollará como colaborador.

Verificar requerimientos iniciales

Al iniciar las auditorías lo primero que se debe hacer es verificar los requerimientos iniciales asignados por el encargado, en esta actividad solamente es verificar que la información suministrada por TI corresponda a lo que se está solicitando, de no ser así, se le hace la aclaración a TI que la información no corresponde, o incluso que está pendiente de su entrega.

Solicitar requerimientos adicionales

Una vez verificado el requerimiento inicial, se procede a revisar en profundidad el documento entregado, el cual puede ser un proceso, una metodología, una política, un lineamiento u otro, se procede a identificar requerimientos adicionales que permitan justificar su cumplimiento, por ejemplo, aprobaciones, diagramas, oficios, correos, reportes, certificaciones y cualquier otro documento necesario.

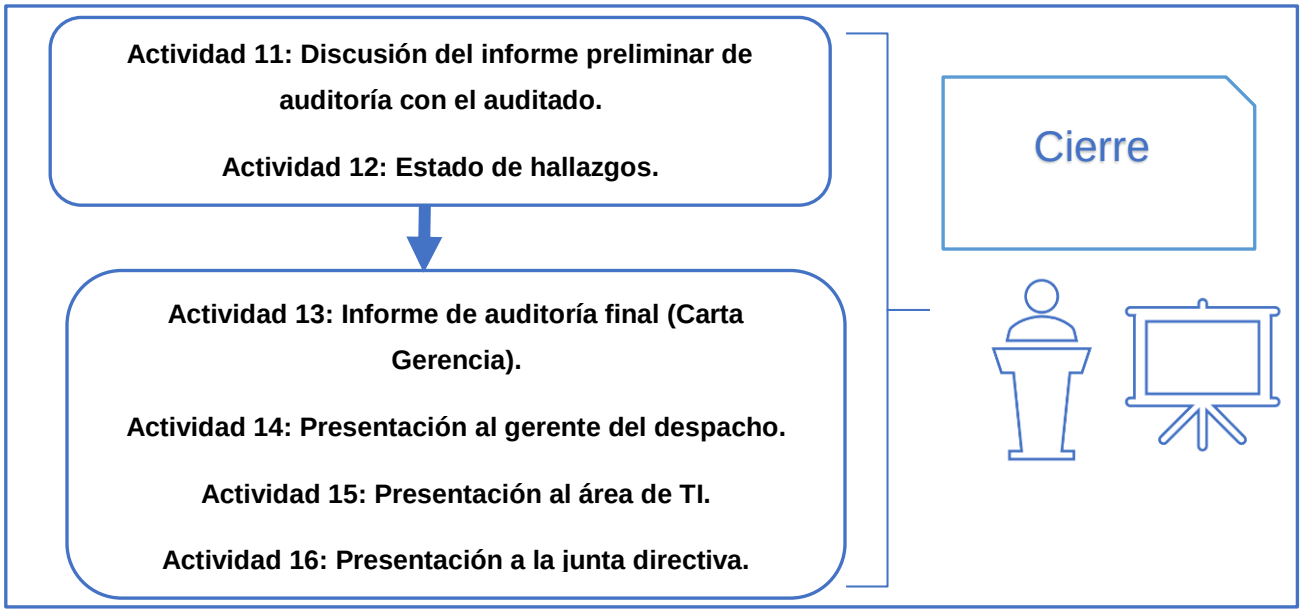
Ejecución de las pruebas y redacción de hallazgos

En el Anexo 1: Plantilla actual de pruebas, se indica la plantilla actual para realizar las pruebas de auditoría, como se mencionó en el alcance de este documento, aplica para clientes regulados por la CGR o que adopten *COBIT* 5 como marco de referencia.

Seguimiento periodos anteriores

Aquí se explicará de igual manera como darles seguimiento a periodos anteriores, la plantilla también se ubica en el Anexo 1: Plantilla actual de pruebas.

Etapa de cierre



Fuente: Elaboración propia con base en Despacho Carvajal (2018).

En la etapa de cierre, cómo se verá a continuación el asistente no tendrá participación, sin embargo, es importante documentarla y explicarla para que el asistente tenga una visión integral del ciclo de auditoría. La fase de cierre a cómo puede durar una semana, se puede extender por incluso un mes o más tiempo.

Revisión de resultados obtenidos

Se hace una revisión a lo interno por parte del encargado sobre equipo de trabajo para asegurarse cumplir con todos los requerimientos iniciales y demás requisitos para finalizar la auditoría.

Estado de pruebas

El encargado revisa que las pruebas estén realizadas y aprobadas, además que cuenten con su respectivo hallazgo.

Informe de auditoría (Carta Gerencia)

El encargado construirá el informe de auditoría con base en la información obtenida de las fases anteriores, aunque esta no es una actividad de los asistentes, se explicará en el manual las partes que contiene un informe de auditoría.

- Introducción.
- Hallazgos.
- Seguimiento.
- Matriz de riesgos.

Presentación al gerente del Despacho

El encargado de la auditoría le presentará el informe al gerente para su respectiva revisión y aprobación. En caso de realizar cambios se valora si es responsabilidad del encargado o los asistentes.

Presentación al área de TI

Una vez aprobado el informe, se le presentará al área de TI de la organización, ya sea el gerente o el encargado, para corroborar que los hallazgos de verdad correspondan a la situación actual de TI.

Presentación a la junta directiva

El gerente en ocasiones acompañado con el encargado de la auditoría hará la presentación de los resultados obtenidos ante la junta directiva de la organización, de ser aceptado aquí, terminará el ciclo del periodo de la auditoría, si no se deben hacer los cambios pertinentes para su aceptación.

Apéndice E: Temas por explicar

Para seleccionar los temas se realizó un estudio con el programa de Excel, de tal manera que se abarcará la normativa aplicable para las empresas costarricenses, como lo es lar normas técnicas y el acuerdo SUGEF 14-17, además de las organizaciones privadas que adoptan COBIT 5 como marco de referencia, se resultado se observa en a continuación.

Selección de pruebas Manual de Auditoría de TI							
N°	**##**	**PRUEBA**	**SUGEF 14-17**	**COBIT 5**	**ITIL**	**Normas Técnicas**	**Otros**
6	1	Gestión de la estrategia de TI.	2.1 Gestiona el marco de gestión de TI.	APO01 Gestiona el marco de gestión de TI.	Generación de la estrategia Mejora continua del servicio.		ISO 20000 ISO 27002
7	1	Gestión de la estrategia de TI. PETI.	2.2 Gestionar la estrategia.	APO02 Gestionar la estrategia.	Generación de la estrategia.	1.6 Decisiones sobre asuntos estratégicos de TI. 2.1 Planificación de las tecnologías de información. 5.1 Seguimiento de los procesos de TI.	ISO 20000
12	1	Gestión de la estrategia de TI.	2.7 Gestionar las relaciones.	APO08 Gestionar las relaciones.	Gestión de la Demanda.		ISO 20000

N°	##	PRUEBA	SUGEF 14-17	COBIT 5	ITIL	Normas Técnicas	Otros
17	2	Gestión de riesgos.	2.11 Gestionar el riesgo.	APO12 Gestionar el riesgo.		1.3 Gestión de riesgos.	ISO 31000 ISO 27002
9	3	Catálogo de servicios.	2.4 Gestionar el portafolio.	APO05 Gestionar la cartera.	Gestión del Portafolio de Servicios Gestión del catálogo de servicios.		ISO 20000
14	4	Acuerdos de niveles de servicio.	2.8 Gestionar los acuerdos de servicio.	APO09 Gestionar los acuerdos de servicio.	Gestión del Catálogo de Servicios Gestión del Nivel del Servicio.	4.1 Definición y administración de acuerdos de servicio.	ISO 20000
15	5	Gestión de proveedores.	2.9 Gestionar los proveedores.	APO10 Gestionar los proveedores.	Gestión de proveedores.	3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura. 4.6 Administración de servicios prestados por terceros.	ISO 20000

N°	##	PRUEBA	SUGEF 14-17	COBIT 5	ITIL	Normas Técnicas	Otros
22	6	Gestión de la capacidad y desempeño Planes para el mantenimiento periódico de la infraestructura de TI. Monitoreo de la infraestructura tecnológica.	3.4 Gestionar la disponibilidad y la capacidad.	BAI04 Gestionar la disponibilidad y la capacidad.	Gestión de la capacidad.	3.3 Implementación de infraestructura tecnológica. 4.2 Administración y operación de la plataforma tecnológica.	ISO 20000
23	7	Gestión de la disponibilidad.	3.4 Gestionar la disponibilidad y la capacidad.	BAI04 Gestionar la disponibilidad y la capacidad.	Gestión de la disponibilidad.	4.2 Administración y operación de la plataforma tecnológica.	ISO 20000
39	8	Respaldos y recuperaciones.	4.4 Gestionar la continuidad.	DSS04 Gestionar la Continuidad.	Gestión de la continuidad del servicio de TI.	4.2 Administración y operación de la plataforma tecnológica.	
43	8	Respaldos y recuperaciones Administración medios de almacenamiento.	4.6 Gestionar controles de proceso de negocio.	DSS06 Gestionar controles de proceso de la empresa.		4.3 Administración de los datos.	

N°	##	PRUEBA	SUGEF 14-17	COBIT 5	ITIL	Normas Técnicas	Otros
24	9	Gestión de cambios.	3.5 Gestionar los cambios.	BAI06 Gestionar los cambios.	Gestión de cambios.		ISO 20000
37	10	Gestión de incidentes y solicitudes.		BAI08 Gestionar el conocimiento.	Gestión del conocimiento.		
29	10	Gestión de incidentes y solicitudes.	4.2 Gestionar las peticiones e Incidentes de Servicio.	DSS02 Gestionar las peticiones e Incidentes de Servicio.	Gestión de incidencias. Gestión de peticiones.	4.4 Atención de requerimientos de los usuarios de TI. 4.5 Manejo de incidentes.	ISO 20000 ISO 27002
30	11	Gestión de problemas.	4.3 Gestionar problemas.	DSS03 Gestionar problemas.	Gestión de problemas.	4.5 Manejo de incidentes.	ISO 20000
29	12	Gestión de eventos.	4.1 Gestionar las operaciones.	DSS01 Gestionar las operaciones.	Gestión de eventos.		
11	13	Gestión del personal Plan de Capacitación funcionarios de TI.	2.6 Gestionar los recursos humanos.	APO07 Gestionar los recursos humanos.		2.4 Independencia y recurso humano de la Función de TI.	ISO 27002

N°	##	PRUEBA	SUGEF 14-17	COBIT 5	ITIL	Normas Técnicas	Otros
26	14	Gestión de activos Licencias.	3.7 Gestionar los activos.	BAI09 Gestionar los activos.	Gestión de la configuración y de activos de servicio.		
27	15	Gestión de la configuración.	3.8 Gestionar la configuración.	BAI10 Gestionar la configuración.	Gestión de la configuración y de activos de servicio.		ISO 20000
16	16	Gestión de la calidad.	2.10 Gestionar la calidad.	APO11 Gestionar la calidad.	Mejora continua del servicio.	1.2 Gestión de la calidad.	ISO 9001
34	16	Gestión de la calidad.	5.1 Supervisar, evaluar y valorar el rendimiento y la conformidad.	MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad.	Informes del Servicio Medida del Servicio.	5.1 Seguimiento de los procesos de TI. 5.3 Participación de la auditoría interna.	ISO 20000
19	17	Gestión de proyectos.	3.1 Gestión de programas y proyectos.	BAI01 Gestionar los programas y proyectos.		1.5 Gestión de proyectos.	PMBOK
20	17	Gestión de proyectos.	3.2 Gestionar la definición de requisitos.	BAI02 Gestionar la definición de requisitos.		3.1 Consideraciones generales de la implementación de TI. 4.4 Atención de requerimientos de los usuarios de TI.	

N°	##	PRUEBA	SUGEF 14-17	COBIT 5	ITIL	Normas Técnicas	Otros
21	18	Implementación de software Estándar para el desarrollo de software.	3.3 Gestionar la identificación y construcción de soluciones.	BAI03 Gestionar la identificación y construcción de soluciones.		3.2 Implementación de software.	
25	18	Implementación de software Estándar para el desarrollo de software.	3.6 Gestionar la aceptación del cambio y la transición.	BAI07 Gestionar la aceptación del cambio y la transición.			ISO 20000 PMBOK
38	19	Gestión de accesos (Roles, perfiles, usuarios activos).	4.5 Gestionar servicios de seguridad.	DSS05 Gestionar servicios de seguridad.	Gestión de accesos.	1.4.5 Control de accesos.	
8	20	Arquitectura.	2.3 Gestionar la arquitectura empresarial.	APO03 Gestionar la arquitectura empresarial.		2.2 Modelo de arquitectura de información. 2.3 Infraestructura tecnológica.	TOGAF
31	21	Gestión de la continuidad. Plan de pruebas Capacitaciones.	4.4 Gestionar la continuidad.	DSS04 Gestionar la continuidad.	Gestión de la continuidad del servicio de TI.		ISO 20000 ISO 27002
18	22	Gestión de la seguridad de la información.	2.12 Gestionar la seguridad.	APO13 Gestionar la seguridad.	Gestión de la seguridad de la información.	1.4 Gestión de la seguridad de la información.	ISO 27002

N°	##	PRUEBA	SUGEF 14-17	COBIT 5	ITIL	Normas Técnicas	Otros
32	22	Gestión de la seguridad de la información Clasificación de la información Estudio vulnerabilidad de la red Uso adecuado equipo de cómputo, internet y correo electrónico.	4.5 Gestionar servicios de seguridad.	DSS05 Gestionar servicios de seguridad.	Gestión de la seguridad de la información.	1.4 Gestión de la seguridad de la información.	ISO 20000 ISO 27002
41	23	Seguridad física.	4.5 Gestionar servicios de seguridad.	DSS05 Gestionar servicios de seguridad.	Gestión de la seguridad de la información.	1.4 Gestión de la seguridad de la información.	ISO 20000 ISO 27002
42	24	Sistemas de información. Revisión de sistemas. Pistas de auditoría.	3.3 Gestionar la identificación y construcción de soluciones.	BAI03 Gestionar la Identificación y la Construcción de Soluciones.	Mejora continua del servicio.	1.4 Gestión de la seguridad de la información. 3.2. Implementación de Software.	ISO 20000 ISO 27002
28	25	Gestión de operaciones.	4.1 Gestionar las operaciones.	DSS01 Gestionar las operaciones.	Gestión de operaciones.	4.2 Administración y operación de la plataforma tecnológica.	

N°	##	PRUEBA	SUGEF 14-17	COBIT 5	ITIL	Normas Técnicas	Otros
33	25	Gestión de operaciones (Revisión inconsistencias bases de datos).	4.6 Gestionar controles de proceso de negocio.	DSS06 Gestionar controles de proceso de la empresa.		4.3 Administración de los datos.	
36	26	Cumplimiento de la normativa aplicable.	5.3 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.	MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.		1.7 Cumplimiento de las obligaciones relacionadas con la gestión de TI.	
35	27	Control.	5.2 Supervisar, evaluar y valorar el sistema de control interno.	MEA02 Supervisar, evaluar y valorar el sistema de control interno.		5.2 Seguimiento y evaluación del control interno en TI. 5.3 Participación de la auditoría interna.	
40	28	Comité de TI.	2.1 Gestiona el marco de gestión de TI.	APO01 Gestiona el marco de gestión de TI.		1.6 Decisiones sobre asuntos estratégicos de TI.	
44	28	Divulgación de la normativa relacionada con TI	2.1 Gestiona el marco de gestión de TI.	APO01 Gestionar el Marco de Gestión de TI.		1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI.	

N°	##	PRUEBA	SUGEF 14-17	COBIT 5	ITIL	Normas Técnicas	Otros
10	29	Plan adquisición de TI	2.5 Gestionar el presupuesto y los costos.	APO06 Gestionar el presupuesto y los costos.	Gestión Financiera	2.5 Gestión de recursos financieros.	ISO 20000
1	30	Gobierno de TI.	1.1 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.	EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno.		1.1 Marco estratégico de TI	ISO 38500 King III 5.1 King III 5.3
2	30	Gobierno de TI.	1.2 Asegurar la entrega de beneficios.	EDM02 Asegurar la entrega de beneficios.			ISO 38500 King III 5.2 King III 5.4
3	30	Gobierno de TI.	1.3 Asegurar la optimización del riesgo.	EDM03 Asegurar la optimización del riesgo.			ISO 38500 King III 5.5 King III 5.7
4	30	Gobierno de TI.	1.4 Asegurar la optimización de recursos.	EDM04 Asegurar la optimización de los recursos.			ISO 38500 King III 5.6
5	30	Gobierno de TI.	1.5 Asegurar la transparencia hacia las partes interesadas.	EDM05 Asegurar la transparencia hacia las partes interesadas.			ISO 38500 King III

Dando como resultado los siguientes temas:

1. Gestión de la estrategia de TI.
2. Gestión de riesgos.
3. Gestión del Catálogo de servicios.
4. Acuerdos de niveles de servicio.
5. Gestión de proveedores.
6. Gestión de la capacidad y desempeño.
7. Gestión de la disponibilidad.
8. Respaldos y recuperaciones.
9. Gestión de cambios.
10. Gestión de incidentes y solicitudes de servicio.
11. Gestión de problemas.
12. Gestión de eventos.
13. Gestión del personal.
14. Gestión de activos.
15. Gestión de la configuración.
16. Gestión de la calidad.
17. Gestión de proyectos.
18. Implementación de software.
19. Gestión de accesos.
20. Arquitectura Empresarial.
21. Gestión de la continuidad.
22. Gestión de la seguridad de la información.
23. Seguridad Física.
24. Sistemas de información.
25. Administración de bases de datos.
26. Cumplimiento de la normativa aplicable.
27. Control interno.
28. Marco de gestión de TI.
29. Plan adquisición de TI.
30. Gobierno de TI.

Apéndice F: Plantilla gestión de cambios

Se procede a indicar la plantilla utilizada para la gestión de cambios.

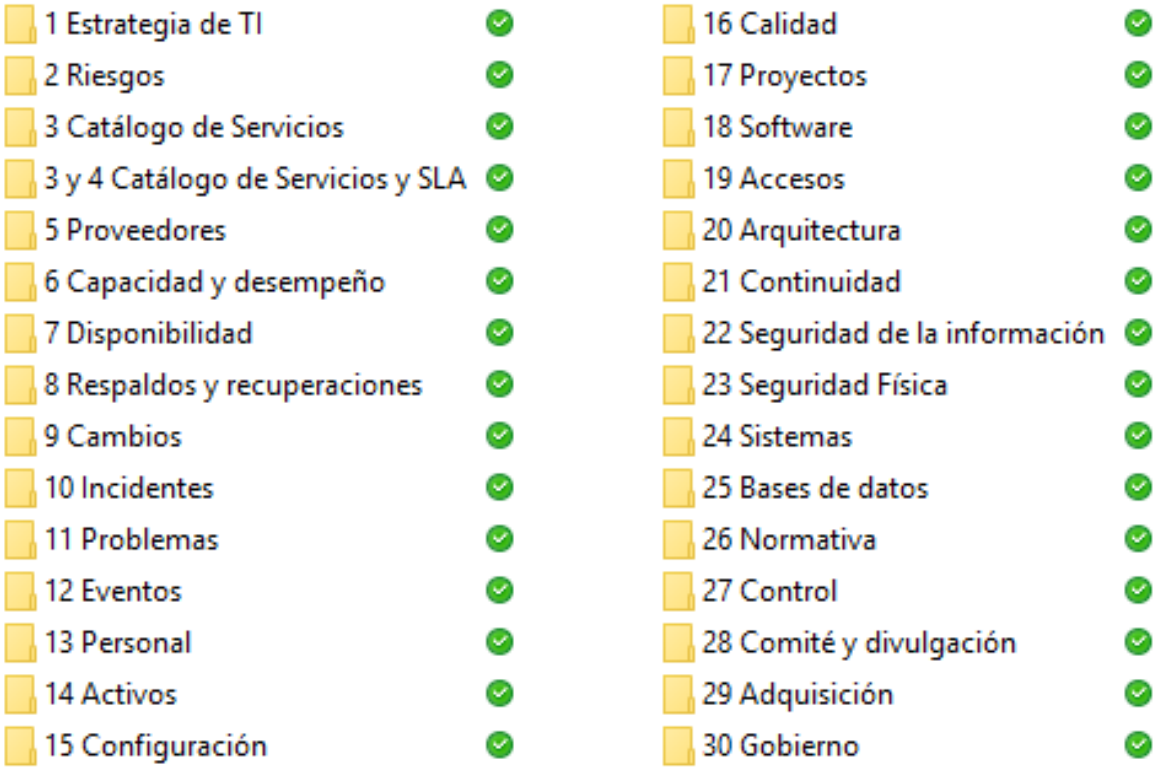
CONTROL DE CAMBIOS	Solicitud N° ##
Nombre del Proyecto:	**Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho**
Solicitante del cambio:	
Responsable del cambio:	
Fecha:	Día: Mes: Año:
Descripción del cambio	Ítems modificados
Involucrados:	• • •
Duración del cambio:	
Representa un atraso en el cronograma establecido: Si ( ) No ( )	
Observaciones:	
Solicitante	(Firma)
Aprobación por parte del gerente	(Firma)
Aprobación por parte del profesor tutor	(Firma)

Fuente: Elaboración propia.

Apéndice G: Repositorio de pruebas

A continuación, se procede a mostrar la estructura realizada para realizar la revisión documental de las pruebas seleccionadas.

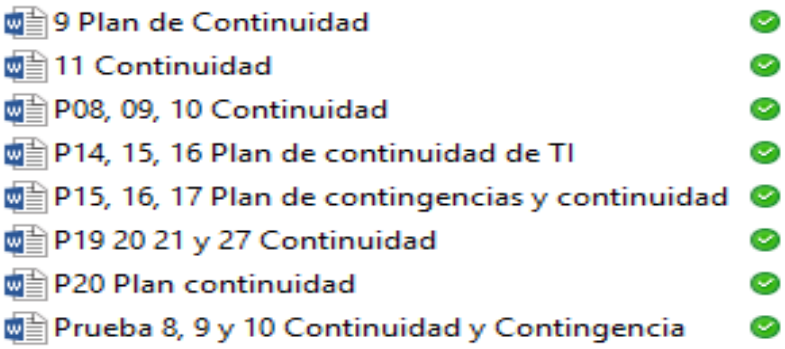
Primeramente, se crea una carpeta por cada tema seleccionado para el manual.



Fuente: Elaboración propia.

El siguiente paso es acomodar las pruebas por carpeta, en total se recolectaron 172 pruebas de las 10 auditorías seleccionadas. En la siguiente página se muestra un ejemplo con el tema 21, Gestión de la continuidad.

A continuación, se muestra las pruebas analizadas para el tema de gestión de la continuidad.

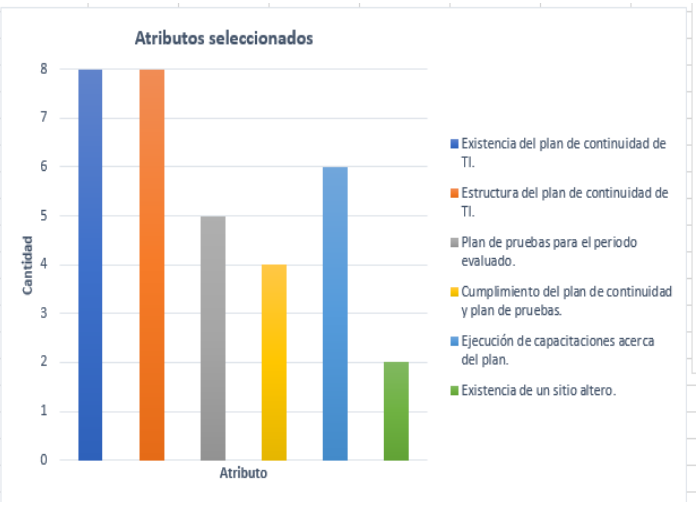


Fuente: Elaboración propia.

Y, por último, como se mencionó en el marco metodológico, se creó un Excel para graficar la selección de los atributos, y así poder analizar la tendencia de cada tema, además de considerar estos atributos como base de la propuesta y mediante el estudio de las mejores prácticas de TI, modificarlos o complementarlos.

Siguiendo con el tema de gestión de la continuidad se procede a ejemplificar en la grafico realizado para este tema.

Atributo	Cantidad
Existencia del plan de continuidad de TI.	8
Estructura del plan de continuidad de TI.	8
Plan de pruebas para el periodo evaluado.	5
Cumplimiento del plan de continuidad y plan de prue	4
Ejecución de capacitaciones acerca del plan.	6
Existencia de un sitio altero.	2



Fuente: Elaboración propia.

Además para el analisis de resultados se utilizo la informacin índicada en las pruebas.

RESULTADOS Y CONCLUSIONES DE LA PRUEBA

Atributo probado	✓ - ✗ - ✗	Resultado	Papeles de trabajo
Existencia del plan de continuidad de TI.	✗	El Departamento de Administración de Tecnologías de Información no cuenta con un plan de continuidad de TI.	• Auditoría Externa Gestión de TI.
Estructura del plan de continuidad.	✗	Dado que no posee un plan, no se puede verificar su estructura.	
Ejecución de un plan de pruebas.	✗	Al no contar con un plan de continuidad de TI, no existe evidencia de pruebas sobre el mismo.	
Ejecución de capacitaciones acerca del plan.	✗	Al no poseer un plan no existen capacitaciones sobre este.	
Existencia de un sitio alterno para el procesamiento de datos.	✗	No existe un sitio alterno para el procesamiento de datos.	
Conclusión de la prueba:			
Dado lo anterior, se concluye que la prueba es insatisfactoria.			

Fuente: Despacho Carvajal (2018).

RESULTADOS Y CONCLUSIONES DE LA PRUEBA

Atributo probado	✓ - ✗ - ✗	Resultado	Papeles de trabajo
Determinar la existencia del plan de contingencia y continuidad (aprobado y actualizado).	✗	Producto de la revisión se determinó que en la organización existe un plan de continuidad de Sistemas de Información denominado Plan de Aseguramiento de Procesos y Contingencia Informática (PCTI) actualizado a agosto 2012.	•
Verificar la estructura del plan de contingencia y continuidad.	✓	En el plan de continuidad se definieron los siguientes aspectos: Introducción, objetivo principal y generales, compromiso de la administración, enfoque, estructura organizacional, alcance, mantenimiento, prueba, comunicación y entrenamiento, administración del plan y equipos de continuidad de TI. Adicionalmente existe 47 acciones registrada en una matriz de plan de continuidad y acciones para el seguimiento a las recomendaciones del plan de aseguramiento de procesos y contingencia informática donde se indica la acción, referencia, periodo, inversión estimada en dólares, ejecutores, responsables, nivel de riesgo, inicio estimado, nivel de avance, facilidad de resolución, comentarios adicionales y encargado.	•
Verificar la existencia del plan de pruebas	✗	Se aporto la evidencia de la prueba de las acciones tomadas por salida de operación de la planta eléctrica de la sede en mayo 2017. Prueba realizada el día 05/05/2018: En las revisiones realizadas nos hemos dado cuenta de que, si se presenta por parte del proveedor de corriente un pico, la transferencia se enclava y no permite su funcionamiento normal. Se revisaron parámetros de funcionamiento y se revisó su parte mecánica y todo esta normal. Para este trabajo coordino con ustedes para que este martes 9 de mayo a las 7 pm podamos realizar el trabajo. Para este trabajo requerimos quitar el fluido eléctrico lo que nos va significar que	•

Fuente: Despacho Carvajal (2018).

Apéndice H: Encuestas de procesos

A continuación, se procede a indicar la encuesta utilizada para obtener los datos del equipo de trabajo del departamento, se hicieron las tres preguntas presentes para cada uno de los temas indicados en el Apéndice E: Temas por explicar.

Primeramente, se indica el formato general utilizado para cada uno de los 30 temas, y seguidamente se presentan los resultados obtenidos.

Por favor contestar las siguientes preguntas, el formulario se compone de 30 secciones y cada sección posee tres preguntas.

Este tema abarca principalmente la prueba del PETI y su alineación con el PEI.

¿Ha realizado una prueba de auditoría relacionada con el tema en estudio? *
Marca sólo un óvalo.

- ◯ Sí
- ◯ No

¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema? * Marca sólo un óvalo.

- ◯ Sí
- ◯ No Pasa a la pregunta 4.

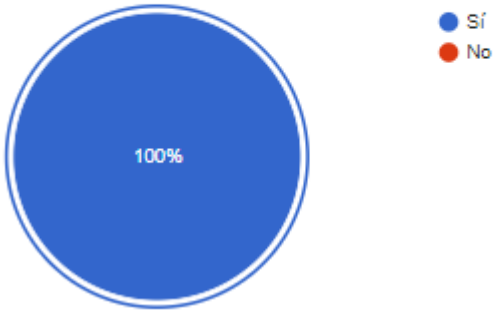
¿A cuál fuente de información acudiría para realizar la prueba? *
Selecciona todos los que correspondan.

- ☐ ITIL
- ☐ COBIT 5
- ☐ Google
- ☐ Encargado o gerente
- ☐ Otro:

Gestión de la estrategia de TI

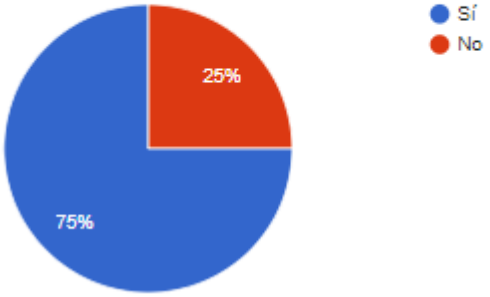
¿Ha realizado una prueba de auditoría relacionada con gestión de la estrategia de TI?

4 respuestas



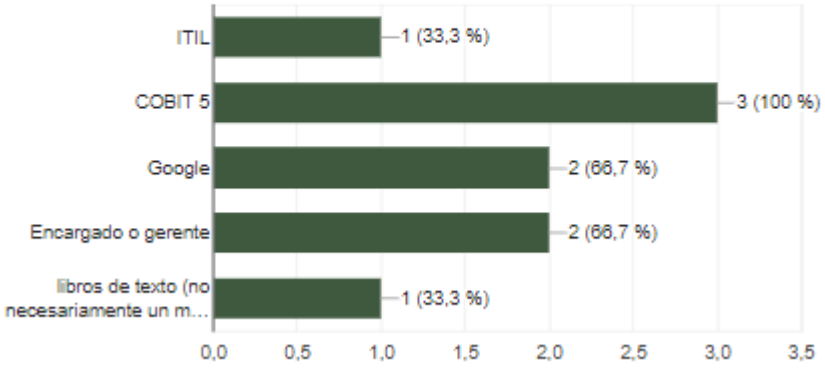
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

3 respuestas



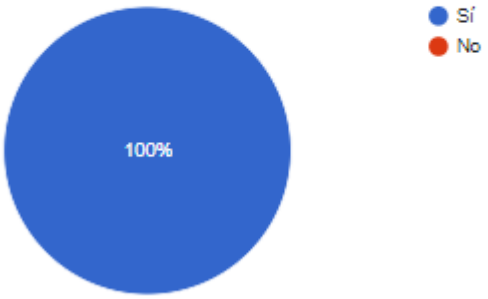
Gestión de riesgos

¿Ha realizado una prueba de auditoría relacionada con gestión de riesgos?

4 respuestas

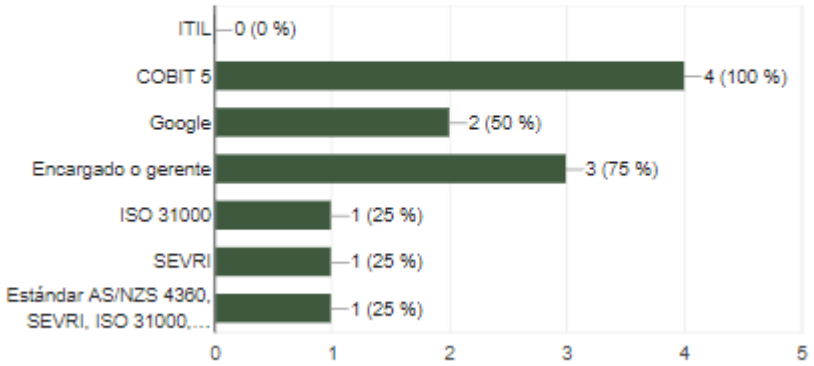
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

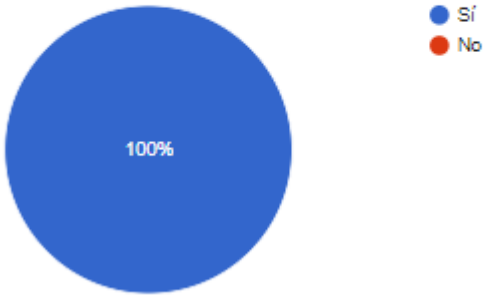
4 respuestas



Gestión del catálogo de servicios

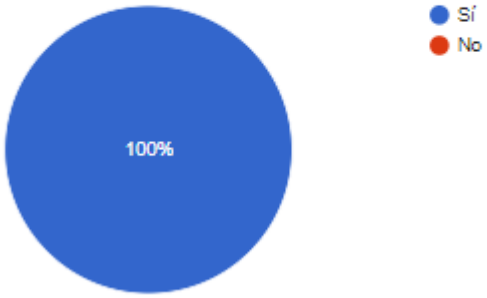
¿Ha realizado una prueba de auditoría relacionada con gestión del catálogo de servicios?

4 respuestas



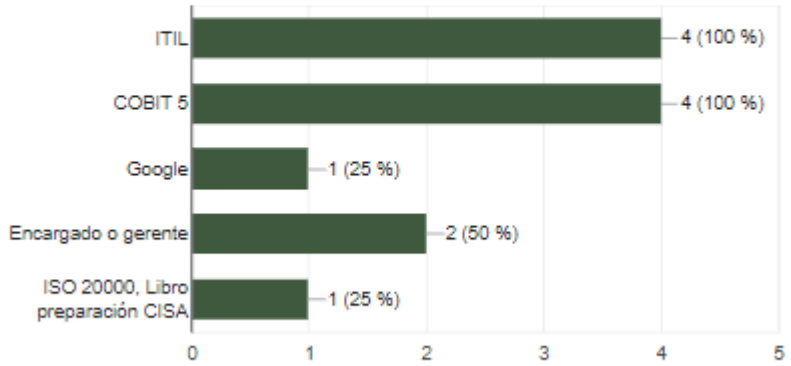
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

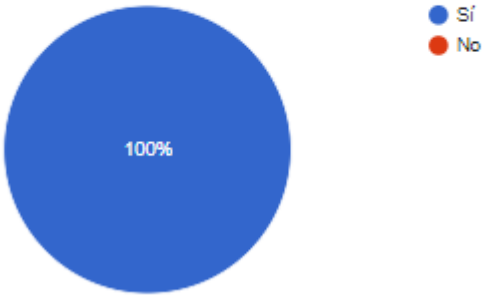
4 respuestas



Acuerdos de niveles de servicio

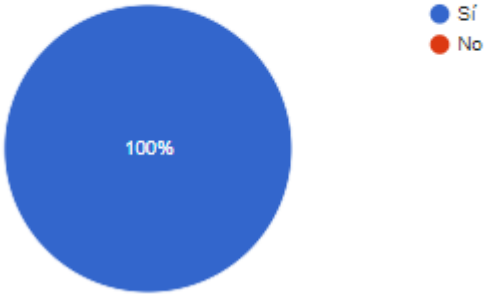
¿Ha realizado una prueba de auditoría relacionada con acuerdos de nivel de servicio?

4 respuestas



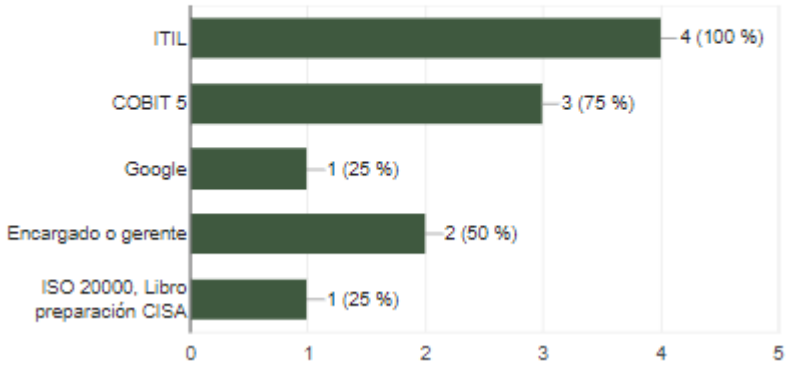
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

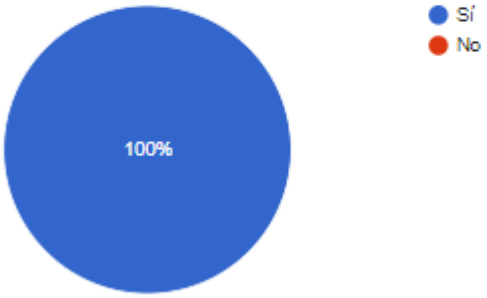
4 respuestas



Gestión de la capacidad y desempeño

¿Ha realizado una prueba de auditoría relacionada con gestión de la capacidad y desempeño?

4 respuestas

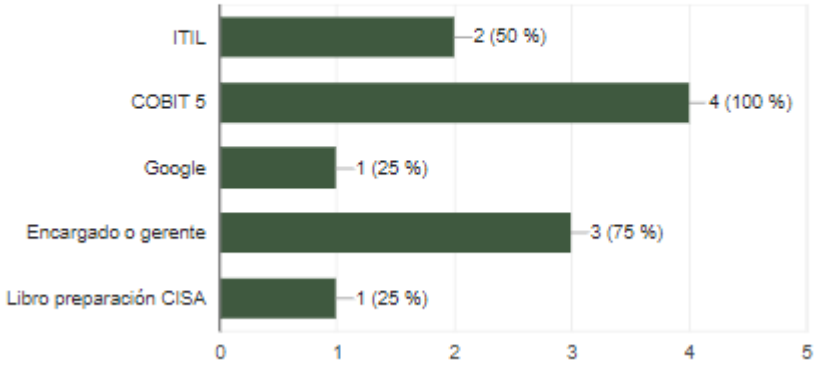


¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas

¿A cuál fuente de información acudiría para realizar la prueba?

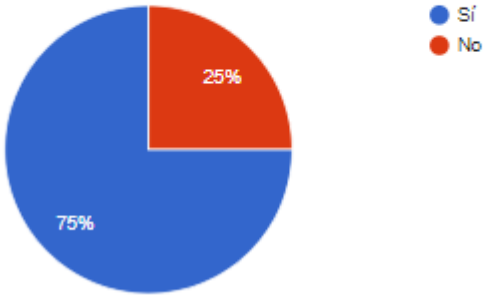
4 respuestas



Gestión de la disponibilidad

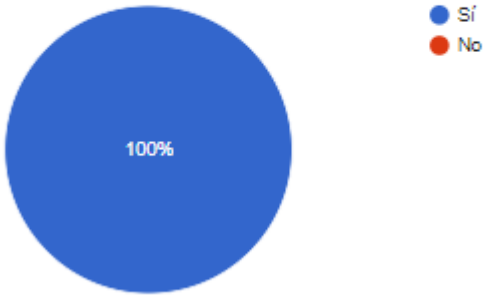
¿Ha realizado una prueba de auditoría relacionada con gestión de la disponibilidad?

4 respuestas



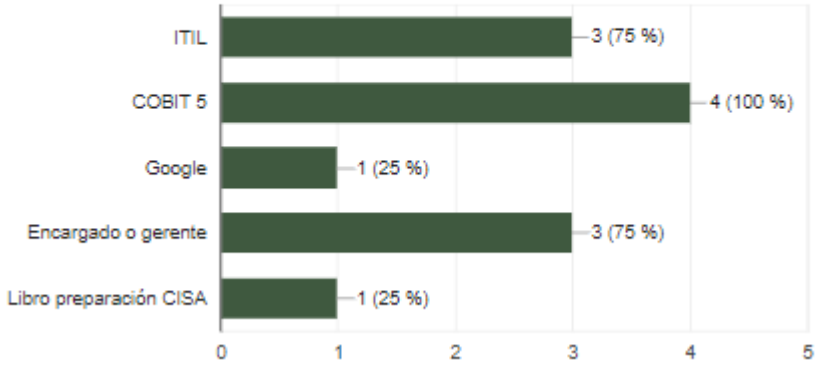
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

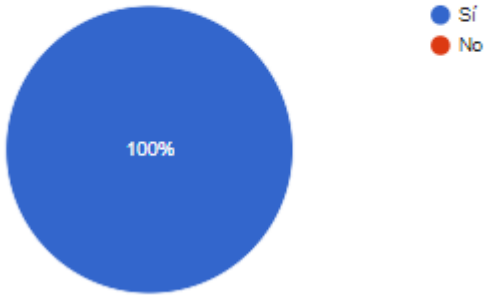
4 respuestas



Respaldos y recuperaciones

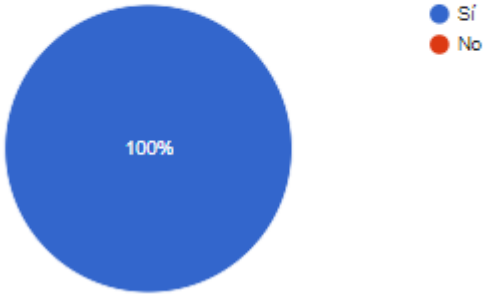
¿Ha realizado una prueba de auditoría relacionada con respaldos y recuperaciones?

4 respuestas



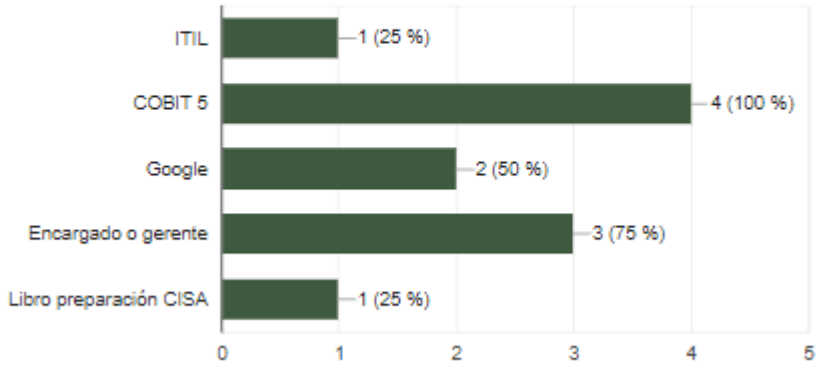
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

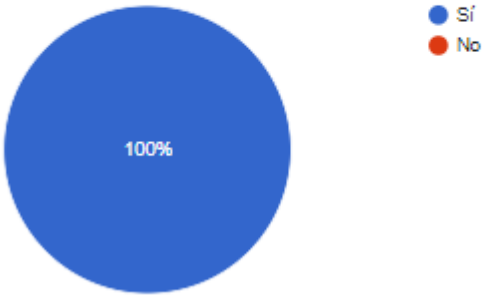
4 respuestas



Gestión de proveedores

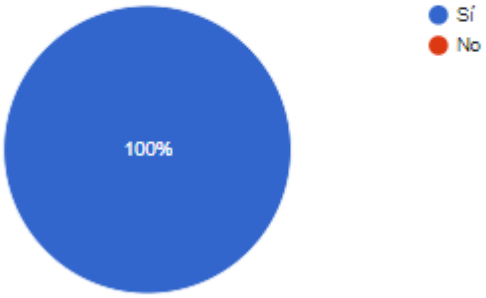
¿Ha realizado una prueba de auditoría relacionada con gestión de proveedores?

4 respuestas



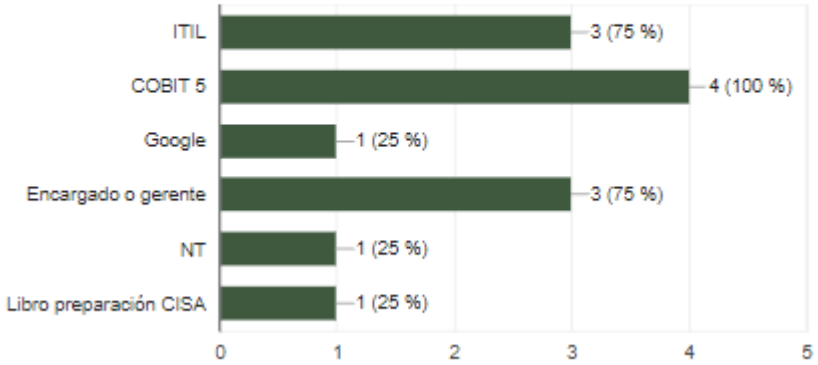
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

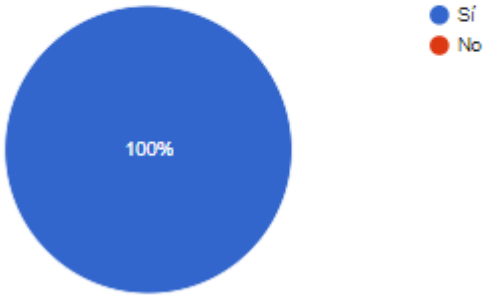
4 respuestas



Gestión de cambios

¿Ha realizado una prueba de auditoría relacionada con gestión de cambios?

4 respuestas

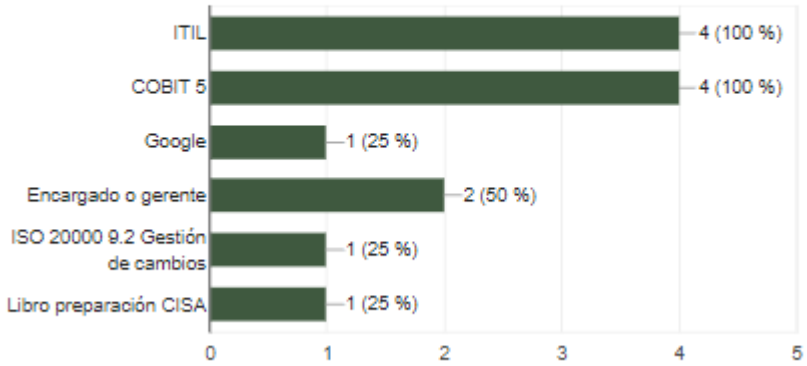


¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas

¿A cuál fuente de información acudiría para realizar la prueba?

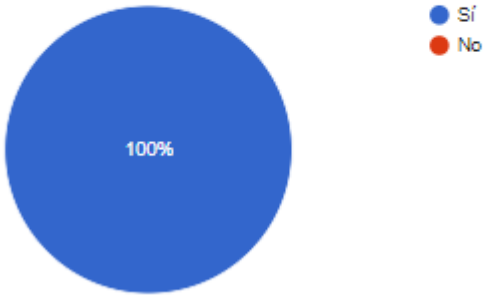
4 respuestas



Gestión de incidentes y solicitudes de servicio

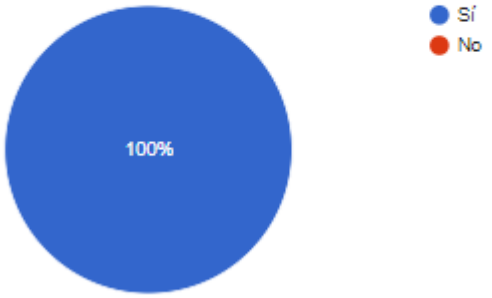
¿Ha realizado una prueba de auditoría relacionada con gestión de incidentes y solicitudes de servicio?

4 respuestas



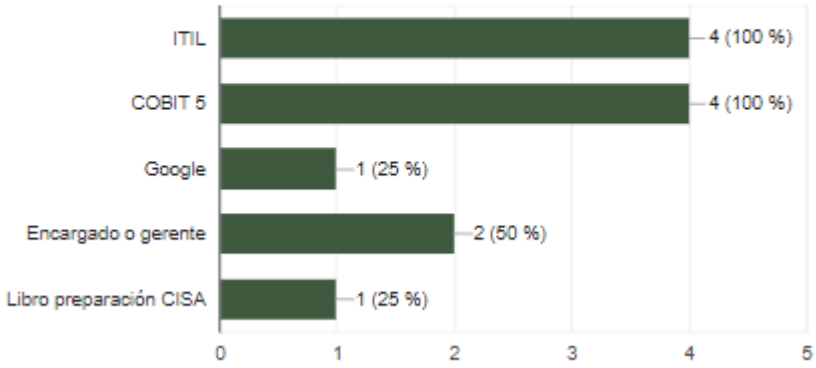
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

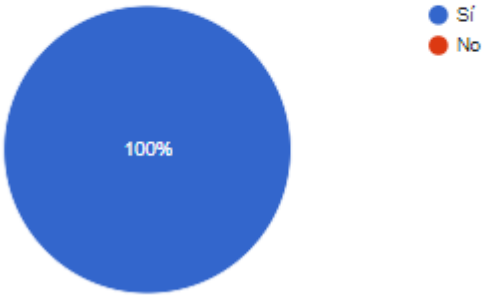
4 respuestas



Gestión de problemas

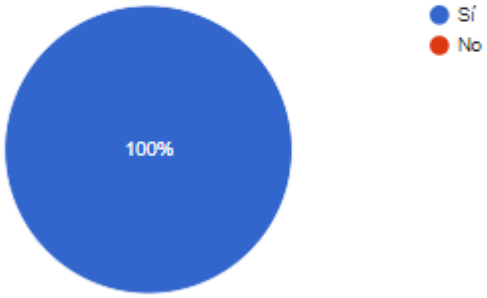
¿Ha realizado una prueba de auditoría relacionada con gestión de problemas?

4 respuestas



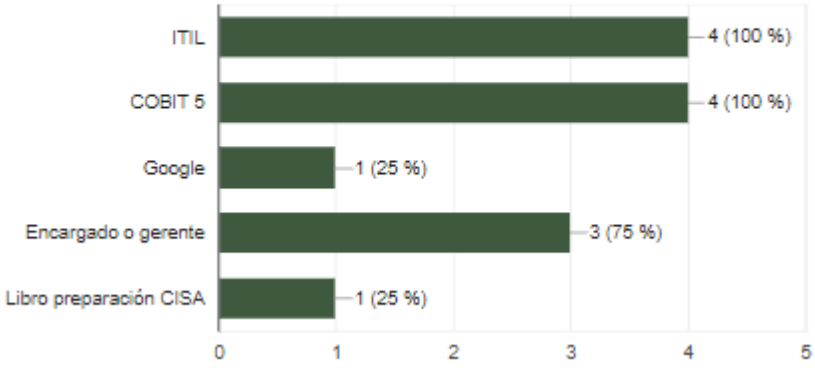
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

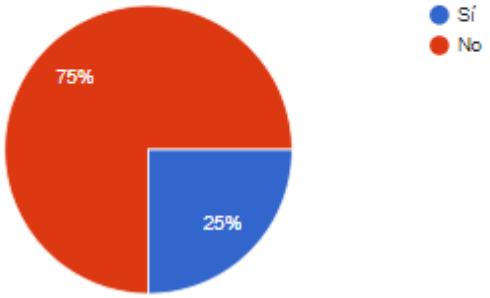
4 respuestas



Gestión de eventos

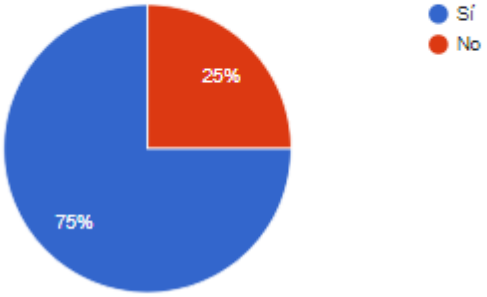
¿Ha realizado una prueba de auditoría relacionada con gestión de eventos?

4 respuestas



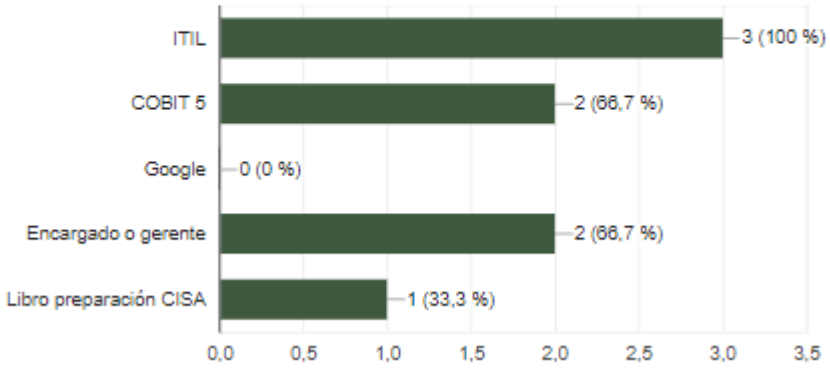
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

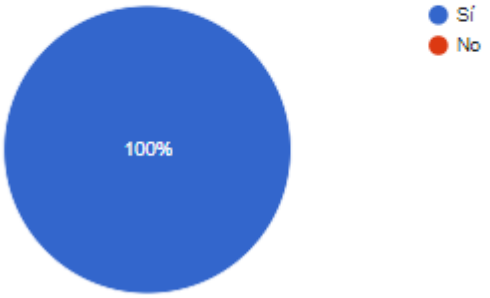
3 respuestas



Gestión del personal

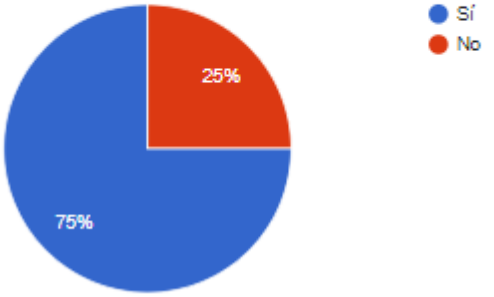
¿Ha realizado una prueba de auditoría relacionada con gestión del personal?

4 respuestas



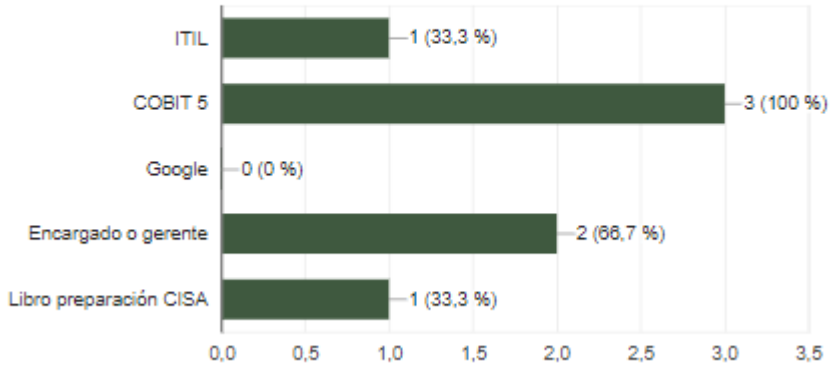
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

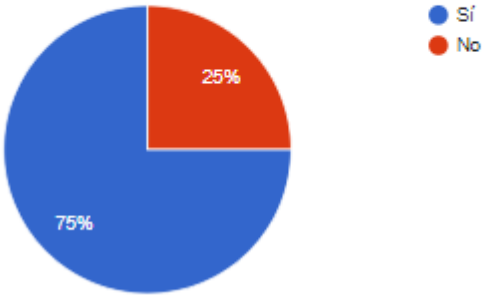
3 respuestas



Gestión de activos

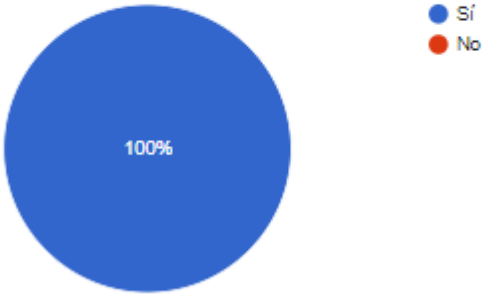
¿Ha realizado una prueba de auditoría relacionada con gestión de activos?

4 respuestas



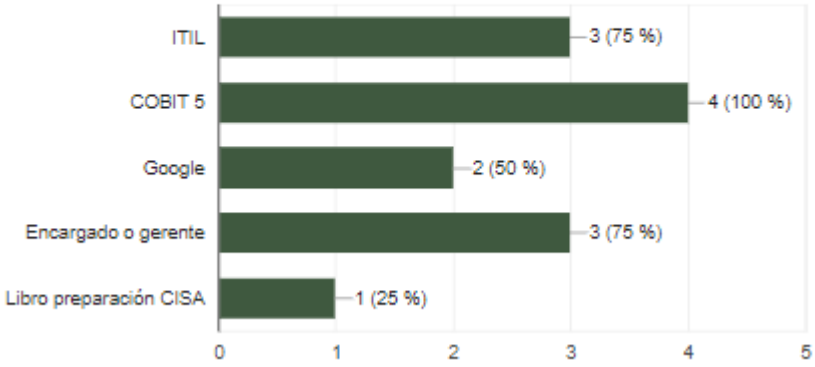
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

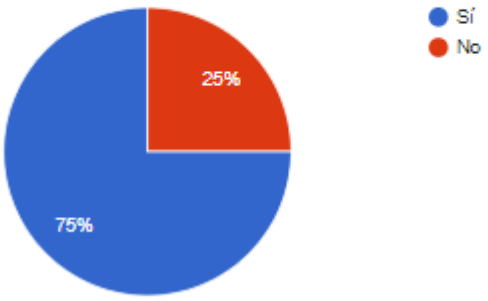
4 respuestas



Gestión de la configuración

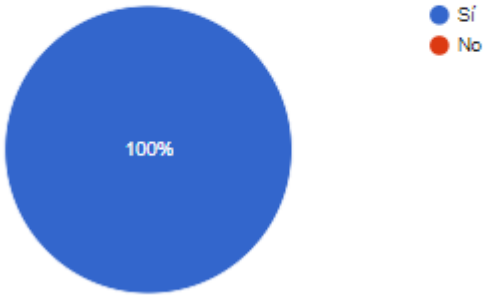
¿Ha realizado una prueba de auditoría relacionada con gestión de configuración?

4 respuestas



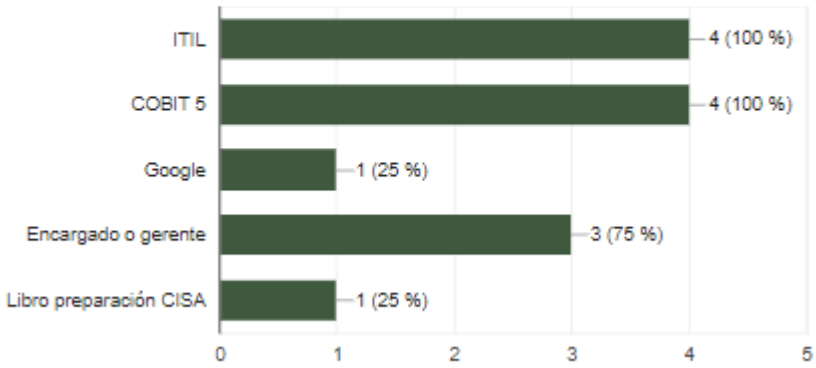
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

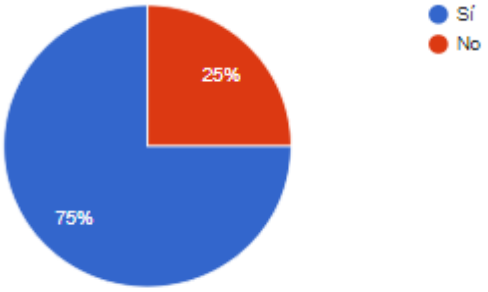
4 respuestas



Gestión de la calidad

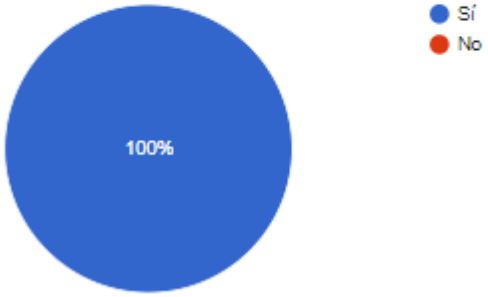
¿Ha realizado una prueba de auditoría relacionada con gestión de la calidad?

4 respuestas



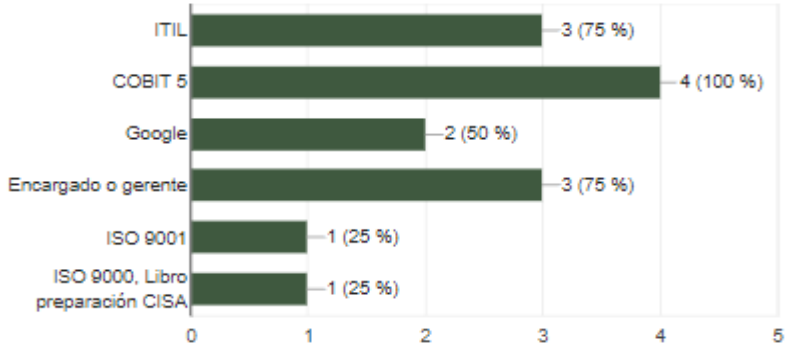
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

4 respuestas



Gestión de proyectos

¿Ha realizado una prueba de auditoría relacionada con gestión de proyectos?

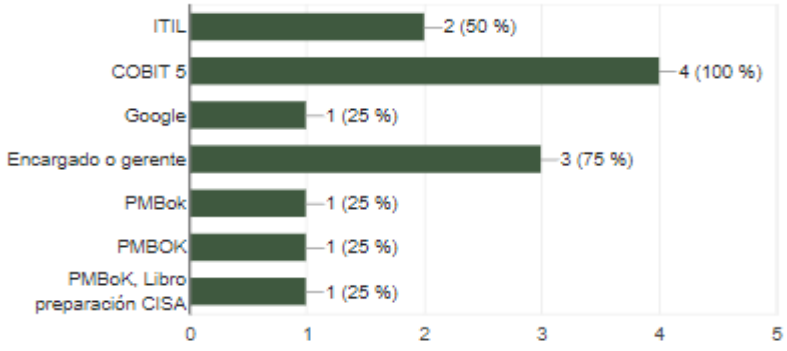
4 respuestas

¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas

¿A cuál fuente de información acudiría para realizar la prueba?

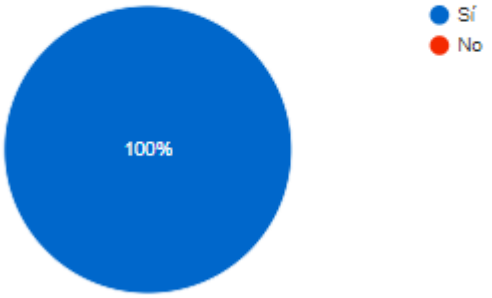
4 respuestas



Implementación de software

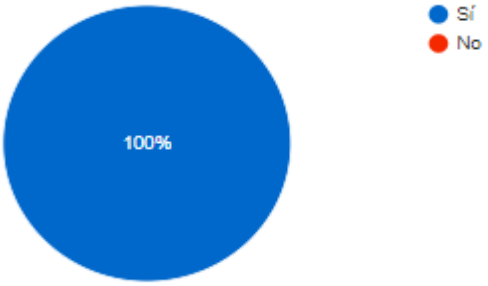
¿Ha realizado una prueba de auditoría relacionada con implementación de software?

4 respuestas



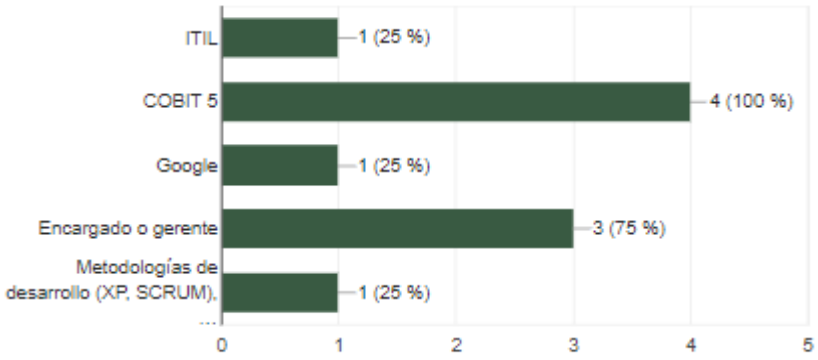
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

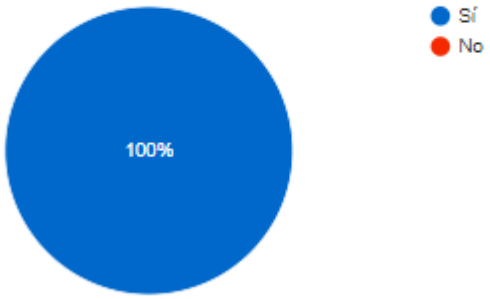
4 respuestas



Gestión de accesos

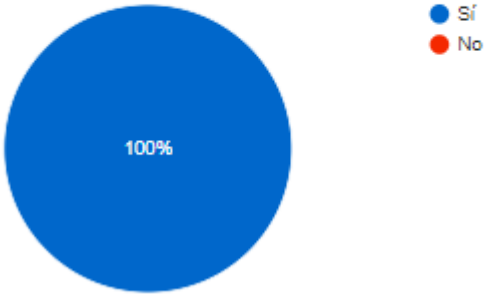
¿Ha realizado una prueba de auditoría relacionada con gestión de accesos?

4 respuestas



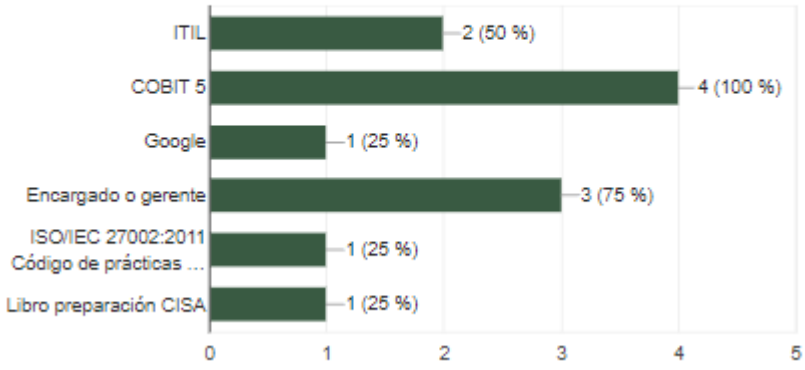
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

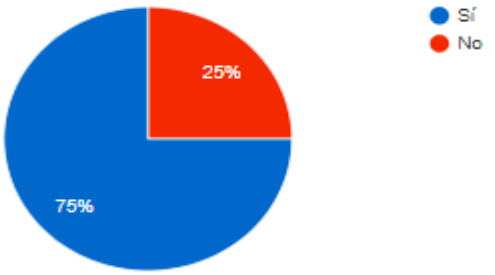
4 respuestas



Arquitectura empresarial

¿Ha realizado una prueba de auditoría relacionada con Arquitectura empresarial?

4 respuestas

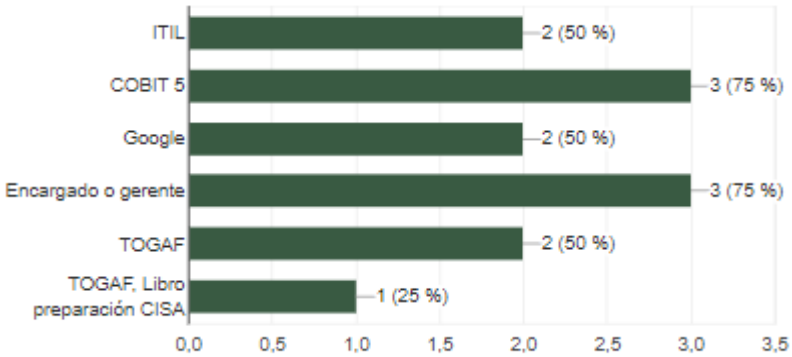


¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas

¿A cuál fuente de información acudiría para realizar la prueba?

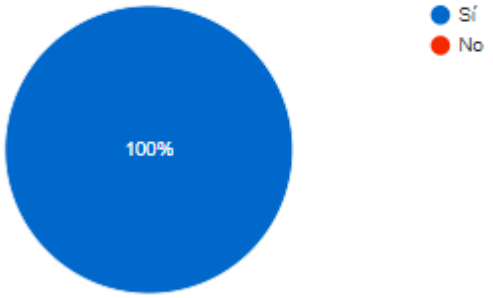
4 respuestas



Gestión de la continuidad

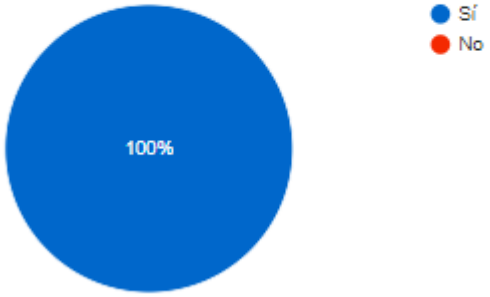
¿Ha realizado una prueba de auditoría relacionada con gestión de la continuidad?

4 respuestas



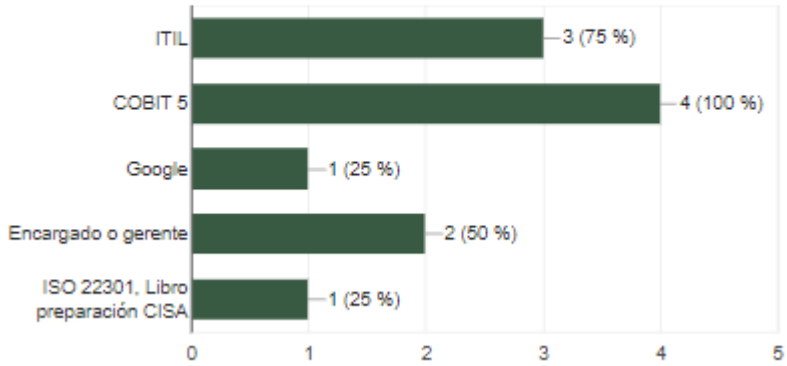
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

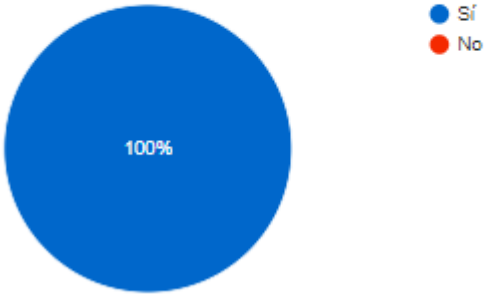
4 respuestas



Gestión de la seguridad de la información

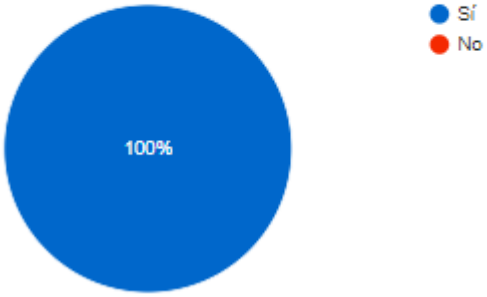
¿Ha realizado una prueba de auditoría relacionada con gestión de la seguridad de la información?

4 respuestas



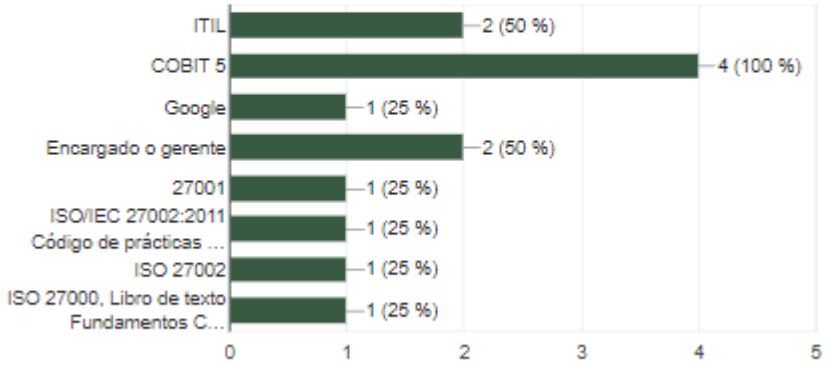
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

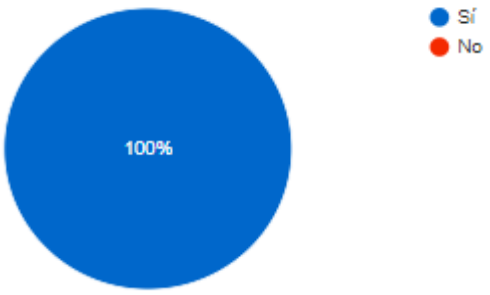
4 respuestas



Seguridad Física

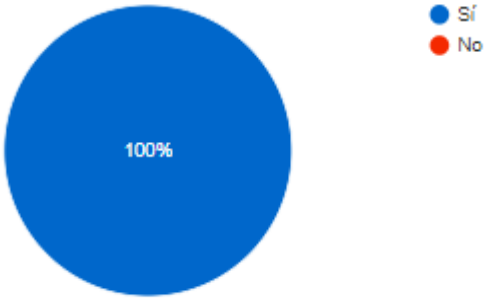
¿Ha realizado una prueba de auditoría relacionada con seguridad física?

4 respuestas



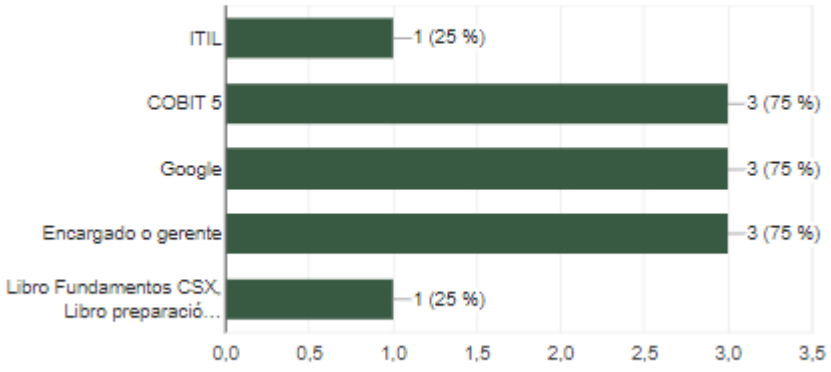
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

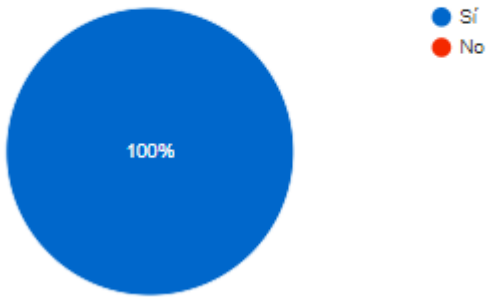
4 respuestas



Sistemas de información

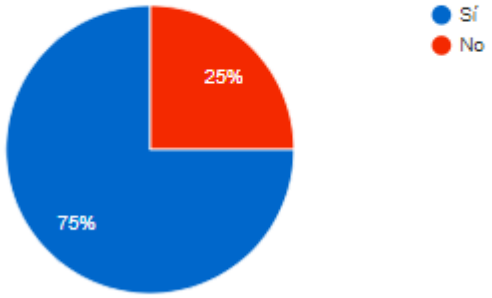
¿Ha realizado una prueba de auditoría relacionada con sistemas de información?

4 respuestas



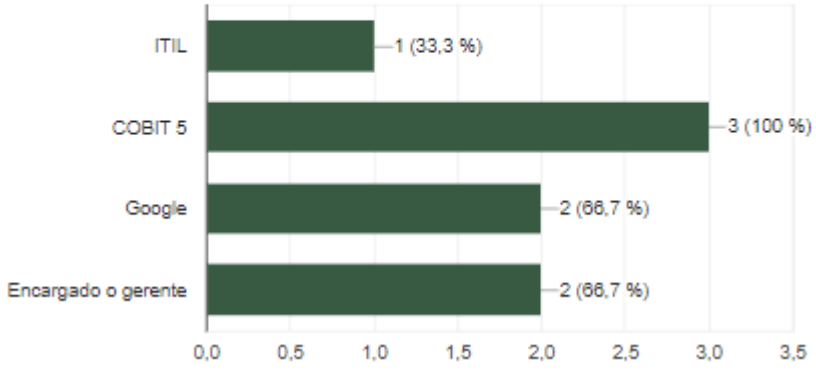
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



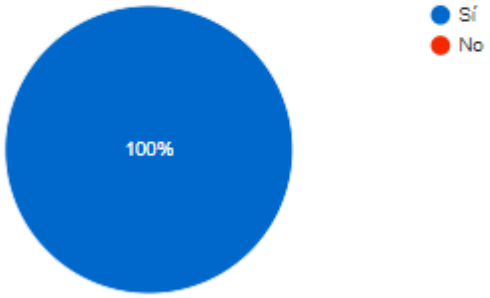
¿A cuál fuente de información acudiría para realizar la prueba?

3 respuestas



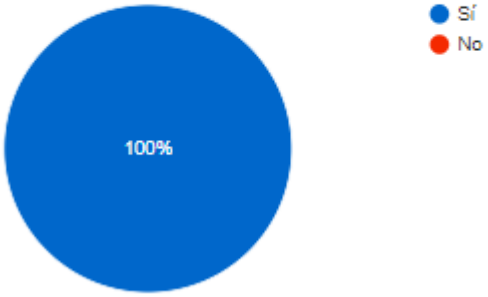
¿Ha realizado una prueba de auditoría relacionada con administración de bases de datos?

4 respuestas



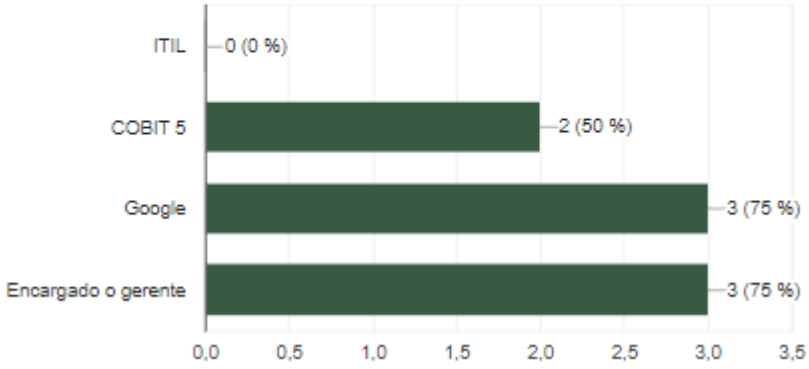
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

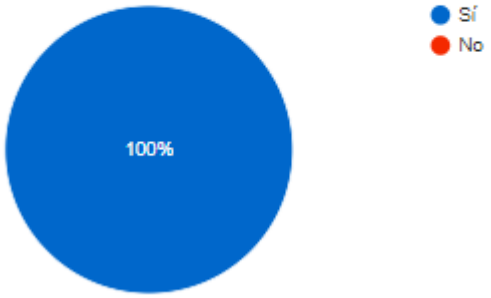
4 respuestas



Cumplimiento de la normativa aplicable

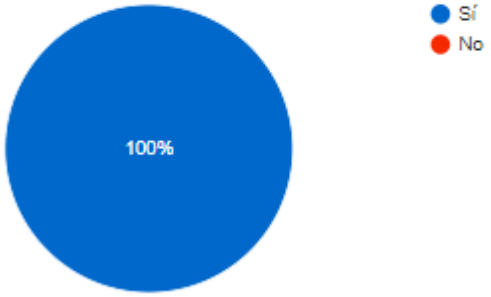
¿Ha realizado una prueba de auditoría relacionada con el cumplimiento de la normativa aplicable?

4 respuestas



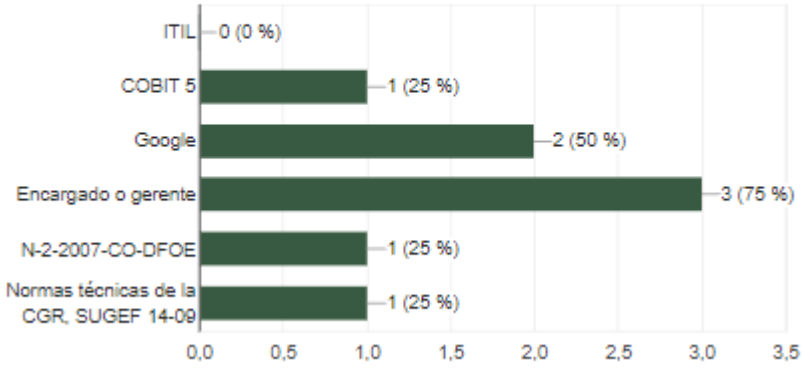
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

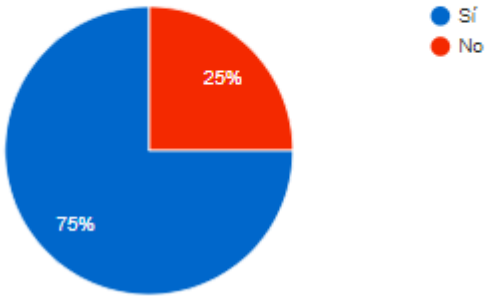
4 respuestas



Control Interno

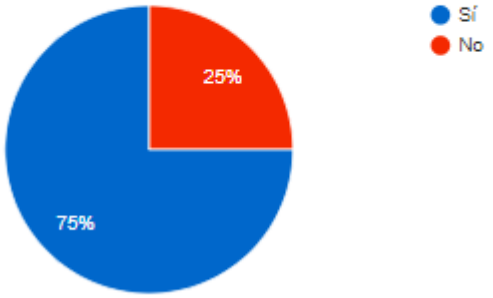
¿Ha realizado una prueba de auditoría relacionada con control interno?

4 respuestas



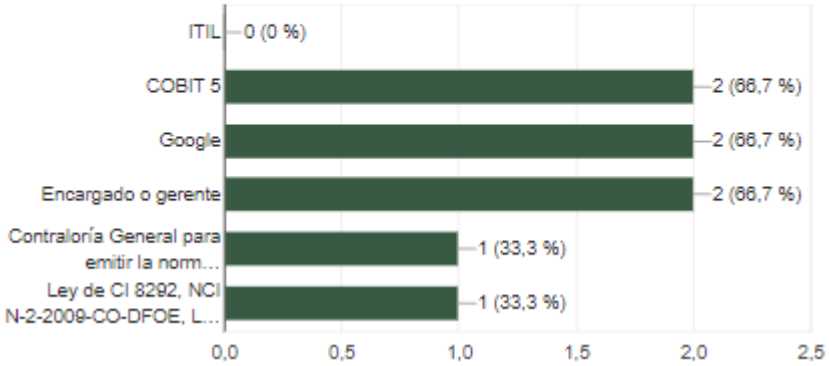
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

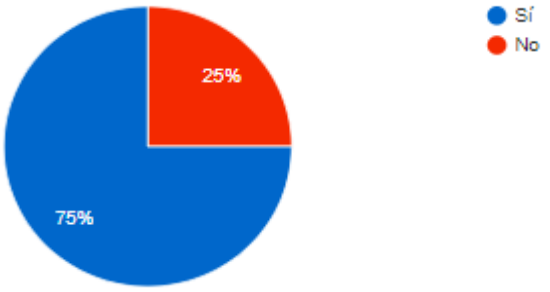
3 respuestas



Marco de gestión de TI

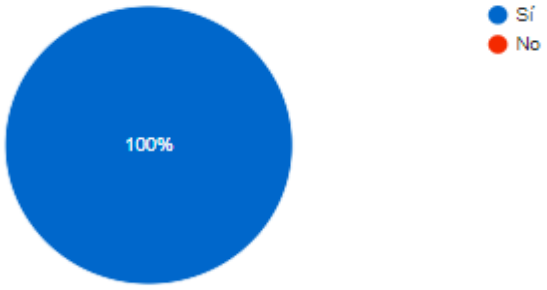
¿Ha realizado una prueba de auditoría relacionada con el marco de gestión de TI?

4 respuestas



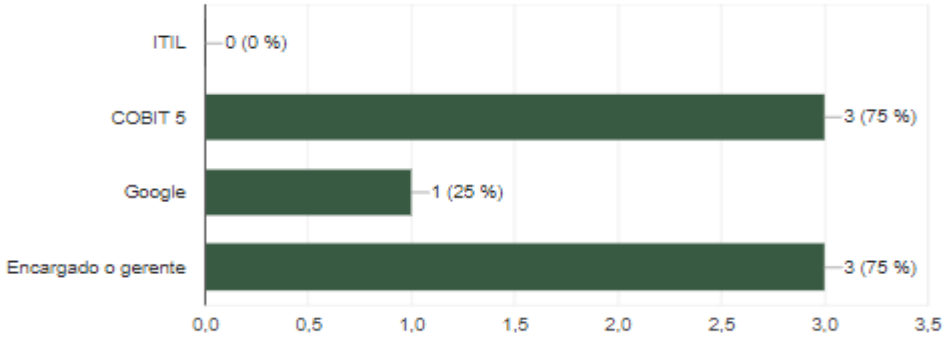
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

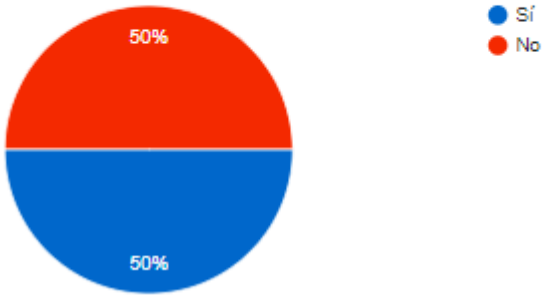
4 respuestas



Plan de adquisición de TI

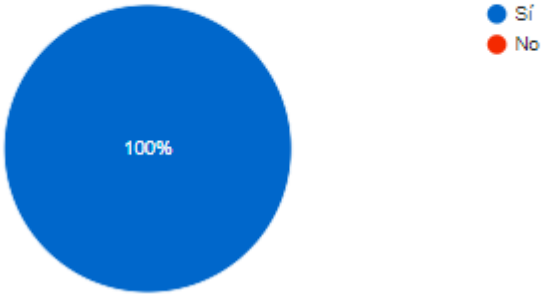
¿Ha realizado una prueba de auditoría relacionada con el plan de adquisición de TI?

4 respuestas



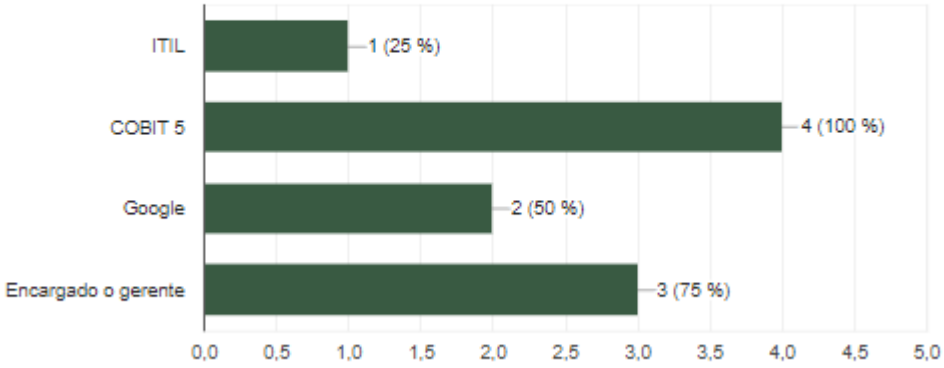
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

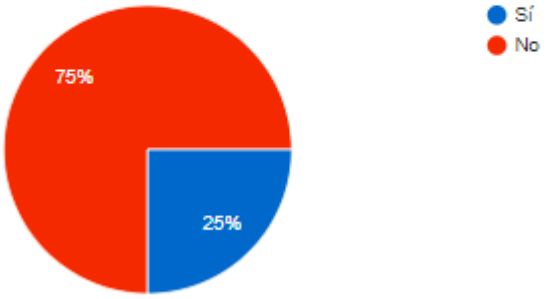
4 respuestas



Gobierno de TI

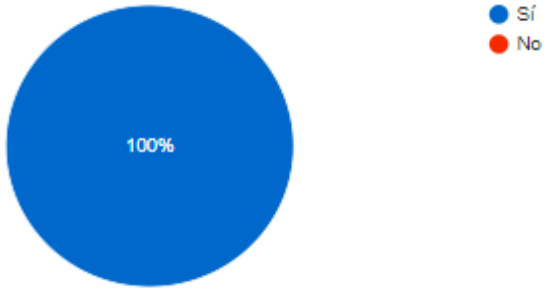
¿Ha realizado una prueba de auditoría relacionada con el gobierno de TI?

4 respuestas



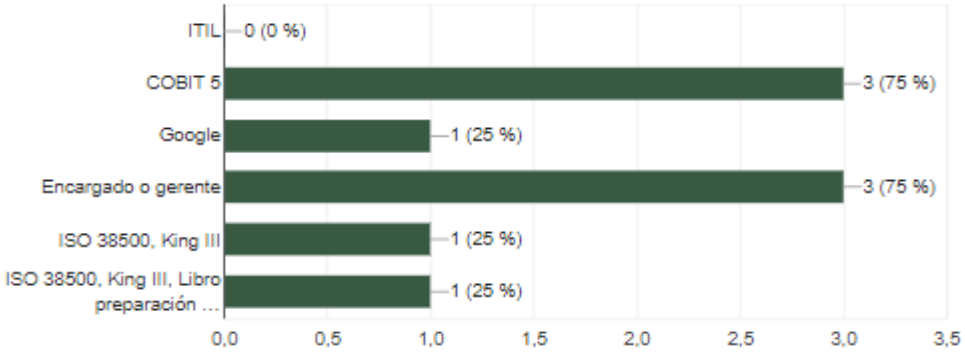
¿Acudiría a una fuente externa para realizar una prueba relacionada con este tema?

4 respuestas



¿A cuál fuente de información acudiría para realizar la prueba?

4 respuestas



Apéndice I Minuta de reunión N°1 con Gerente de TI

TEC | Tecnológico de Costa Rica

MINUTA DE REUNIÓN

Proyecto: Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho

Reunión No.	01	**Fecha:**	31-08-2018
Lugar:	Despacho Carvajal	**Hora Inicio/Finalización:**	04:30 p.m. / 5:30 p.m.
Objetivo de la reunión:	Comentar y revisar el avance general del proyecto, para así brindar la realimentación respectiva. Los documentos para esta reunión se le entregaron a Fabián con antelación para su revisión.		
Participantes:	Fabián Cordero Navarro _____. Carlos Ramírez Cerdas _____.		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Revisión selección de temas.	Se entrega una lista preliminar de temas que se abarcaran en el manual. El cual es aprobado para su desarrollo.	Avanzar con el desarrollo de los temas. **Responsable: Carlos Ramírez Cerdas**
2	Revisión plantilla para la explicación de los temas.	Se comenta el tema de gestión de la configuración completo, para tomarlo como base en el desarrollo de los demás temas. Fabián comenta la opción de agregar el procedimiento por medio de una representación gráfica para facilitar su entendimiento.	Agregar los procedimientos gráficos por tema. **Responsable: Carlos Ramírez Cerdas**
3	Manual de auditoría de TI.	Se comenta la estructura propuesta, se evalúa la opción de actividades de autoevaluación para verificar la comprensión de los temas estudiados.	Analizar la opción de agregar una parte de autoevaluación. **Responsable: Carlos Ramírez Cerdas**

Próxima reunión

Temas por tratar	Fecha	Convocados
Segundo avance manual de auditoría de TI.	03-10-2018	Carlos Ramírez Cerdas. Fabián Cordero Navarro.

Uso Confidencial Pág. 1/1

Apéndice J Minuta de reunión N°2 con Gerente de TI

TEC | Tecnológico de Costa Rica

MINUTA DE REUNIÓN

Proyecto: Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho

Reunión No.	02	**Fecha:**	03-10-2018
Lugar:	Despacho Carvajal	**Hora Inicio/Finalización:**	02:00 p.m. / 2:45 p.m.
Objetivo de la reunión:	Comentar y revisar el avance general del proyecto, para así brindar la realimentación respectiva. Los documentos para esta reunión se le entregaron a Fabián un día antes para su revisión.		
Participantes:	Fabián Cordero Navarro _____. Carlos Ramírez Cerdas _____.		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Dudas sobre los temas abarcados en el manual.	Se le consulta a Fabián como fortalecer la necesidad de una metodología de implementación de software, y no considerarlo como un proyecto más de TI, Fabián indica las diferencias en la gestión de ambos. Se le consulta a Fabián por qué el inventario de licencias y programas de TI tiene un enfoque diferente al enfoque del inventario de activos, a lo que él hace la justificación por medio del decreto ejecutivo N° 37549-JP, el cual obliga a las instituciones públicas a llevar un control estricto de los programas instalados en las computadoras de las instituciones. Se le consulta a Fabián las diferencias del plan de continuidad de TI y el plan de continuidad del Negocio, a lo que él responde que el plan de continuidad de TI solo es una parte del plan de continuidad del negocio, por lo cual debe haber una alineación bilateral entre ambos planes.	Aplicar las recomendaciones brindadas por el Fabián. **Responsable: Carlos Ramírez Cerdas**

Uso Confidencial Pág. 1/2

TEC | Tecnológico de Costa Rica

MINUTA DE REUNIÓN

Proyecto: Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho

2	Eliminación de las tablas de *COBIT* 5.	Se comenta la posibilidad de eliminar las tablas de *COBIT* 5, para reducir el contenido en el manual, y agregarlo como referencia solamente.	Eliminar las tablas de *COBIT* 5 del manual. **Responsable: Carlos Ramírez Cerdas**
3	Avance general del manual de auditoría de TI.	Se comenta el avance realizado en los temas abarcados en el manual, se valida los atributos abarcados en las pruebas de auditoría de TI.	Avanzar con el desarrollo de los temas. **Responsable: Carlos Ramírez Cerdas**

Próxima reunión		
Temas por tratar	**Fecha**	**Convocados**
Tercer avance manual de auditoría de TI.	23-10-2018	Fabián Cordero Navarro. Carlos Ramírez Cerdas.

Apéndice K Minuta de reunión N°3 con Gerente de TI

TEC | Tecnológico de Costa Rica

MINUTA DE REUNIÓN

Proyecto: Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho

Reunión No.	03	**Fecha:**	23-10-2018
Lugar:	Despacho Carvajal	**Hora Inicio/Finalización:**	01:30 p.m. / 2:30 p.m.
Objetivo de la reunión:	Validar el avance realizado sobre el manual de auditoría de TI.		
Participantes:	Fabián Cordero Navarro _____. Carlos Ramírez Cerdas _____.		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Revisión procedimientos de las pruebas.	Se revisa una representación gráfica estándar para la evaluación de pruebas que involucren un procedimiento de por medio.	Desarrollar las representaciones graficas para las pruebas restantes. **Responsable: Carlos Ramírez Cerdas**
2	Pruebas específicas.	Se comenta el material que se debe considerar para los siguientes temas: • Seguridad. • Vulnerabilidad de la red. • Etapa de planificación. • Regulación de TI en Costa Rica.	Agregar el material suministrado por Fabián a los temas indicados. **Responsable: Carlos Ramírez Cerdas**
3	Entrega manual de auditoría de TI.	Se comenta la entrega para la primera versión del manual de auditoría de TI. Se va a realizar en semana 15, para tener una semana en caso de que sea necesario aplicar cambios en el documento.	Entregar la primera versión del manual de auditoría de TI para el 02-11-2018. **Responsable: Carlos Ramírez Cerdas**

Próxima reunión

Temas por tratar	Fecha	Convocados
N/A	N/A	N/A

Uso Confidencial Pág. 1/1

Apéndice L: Propuesta manual de auditoría de TI

En el siguiente apéndice se procedió a indicar la primera versión del manual de auditoría de TI. El mismo formó parte de la propuesta de solución. La propuesta la posee el despacho.

Anexos

11. Anexos

En este capítulo se presentan los documentos que soportan o amplían temas abarcados en el desarrollo de este trabajo.

Anexo 1: Plantilla actual de pruebas

A continuación, se muestra la plantilla principal para realizar las pruebas de auditoría.

CARVAJAL	Documento de prueba
	RESULTADO DE LA PRUEBA

ORGANIZACIÓN:	
PERIODO AUDITADO:	
ÁREA:	
ESTADO DE LA PRUEBA	

FECHA	ROL	NOMBRE
	Elaborar	
	Revisar	
	Aprobar	

CRITERIO			
Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE)		Control Objectives for Information and related Technology 5 (COBIT 5)	
PROCESO		PROCESO	
SUBPROCESO		PRÁCTICA DE GESTIÓN	

Lista de Requerimientos evaluados	
ID	Requerimiento

Métodos de indagación	
	Entrevista
	Inspección
✓	Revisión documental
	Otro:

PROCEDIMIENTO DE LA PRUEBA

RESULTADOS Y CONCLUSIONES DE LA PRUEBA

Atributo probado	✓ - ✗ - ✘	Resultado	Papeles de trabajo
Conclusión de la prueba:			
Dado lo anterior, se concluye que la prueba es Elija un elemento.			

HALLAZGOS DE PERIODOS ANTERIORES			
CG	HALLAZGO	ESTADO	MOTIVO

Fuente: Despacho Carvajal (2018).

Anexo 2: Aval de Entrega del Documento de Trabajo Final de Graduación

Aval de Entrega del Documento de Trabajo Final de Graduación

Nota aclaratoria:
Este documento se redacta de acuerdo a las disposiciones actuales de la Real Academia Española con relación al uso del género inclusivo (https://goo.gl/ITVYiN).
Al mismo tiempo, se aclara que estamos a favor de la igual de derechos entre los géneros.

Responsabilidad del Profesor Tutor:

1. A solicitud del estudiante, completar el formulario de Aval de Entrega del Documento de Trabajo Final de Graduación.
2. Devolver una respuesta al estudiante que realizó la solicitud de Aval de Entrega del Documento de Trabajo Final de Graduación. La respuesta debe ser por correo (en formato pdf).

Formulario de Aval de Entrega del Documento de Trabajo Final de Graduación:

Yo Mario Acuña Sánchez Profesor Tutor del Estudiante Carlos Ramírez Cerdas carné 2014159929, hago constar que he revisado exhaustivamente el documento académico final del Trabajo Final de Graduación, realizado en el II semestre del 2018. Asimismo, he verificado la atención de las correcciones realizadas en mi condición de Profesor Tutor. Por lo tanto, autorizo entregar este documento a la Coordinación de Trabajos Finales de Graduación para que se realicen las gestiones correspondientes para la programación de la defensa.

Responsabilidades del estudiante:

1. Solicitar al Profesor Tutor el Aval de Entrega del Documento de Trabajo Final de Graduación. Esta solicitud se debe realizar por correo al Profesor Tutor, después de haber enviado con al menos una semana hábil el documento académico completo para la respectiva revisión integral final.

2. Enviar a la Coordinación de Trabajos Finales de Graduación la respuesta otorgada por el Profesor Tutor según el formato indicado en este documento. Para esto, debe realizar un reenvío del correo a smora@itcr.ac.cr con copia:
   a. El correo del Profesor Tutor y
   b. Al correo soniamora0407@gmail.com

   No se requiere la firma del Profesor Tutor, dado que el reenvío del correo del Profesor Tutor garantiza la identidad del Profesor.

ati Área Académica de Administración de Tecnologías de Información
Lic. Administración de Tecnología de Información

Anexo 3: Minuta de reuniones

A continuación, se procede a indicar la plantilla utilizada para las minutas de reuniones que sucedan durante el proyecto.

TEC | Tecnológico de Costa Rica

MINUTA DE REUNIÓN

Proyecto: Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho

Reunión No.	Es un núm. consecutivo para este proyecto	**Fecha:**	Indicar la fecha exacta de la reunión
Lugar:	Indicar dónde fue la reunión	**Hora Inicio/Finalización:**	xx:00 am. / yy:00 am
Objetivo de la reunión:			
Participantes:	Presentes:		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito
2	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito
3	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito

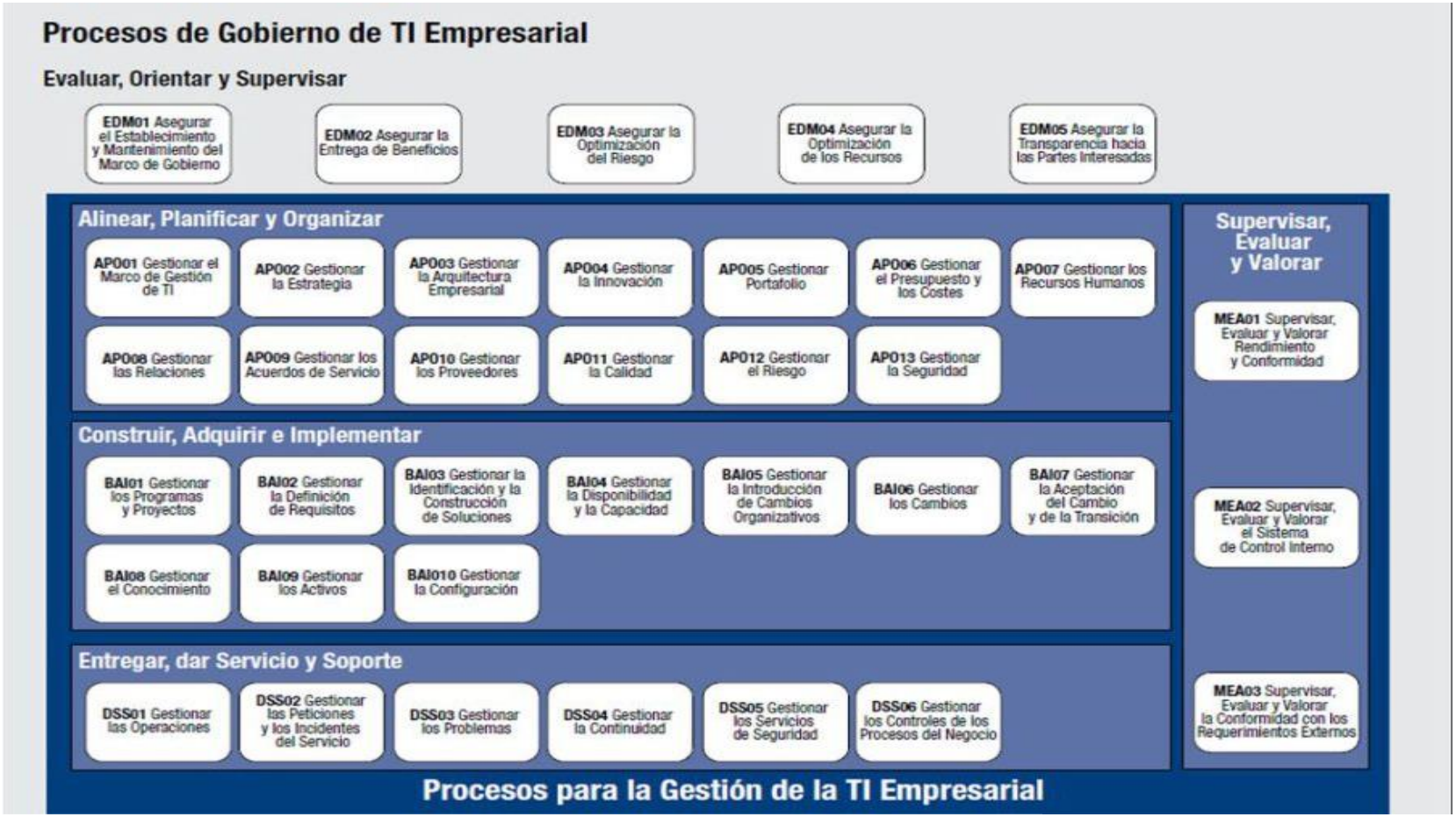
Próxima reunión

Temas por tratar	Fecha	Convocados
En la próxima reunión	indicar	Nombre de quiénes asistirán a esta próxima reunión.

Fuente: Administración de Tecnología de Información (2018).

Anexo 4: Procesos de *COBIT* 5

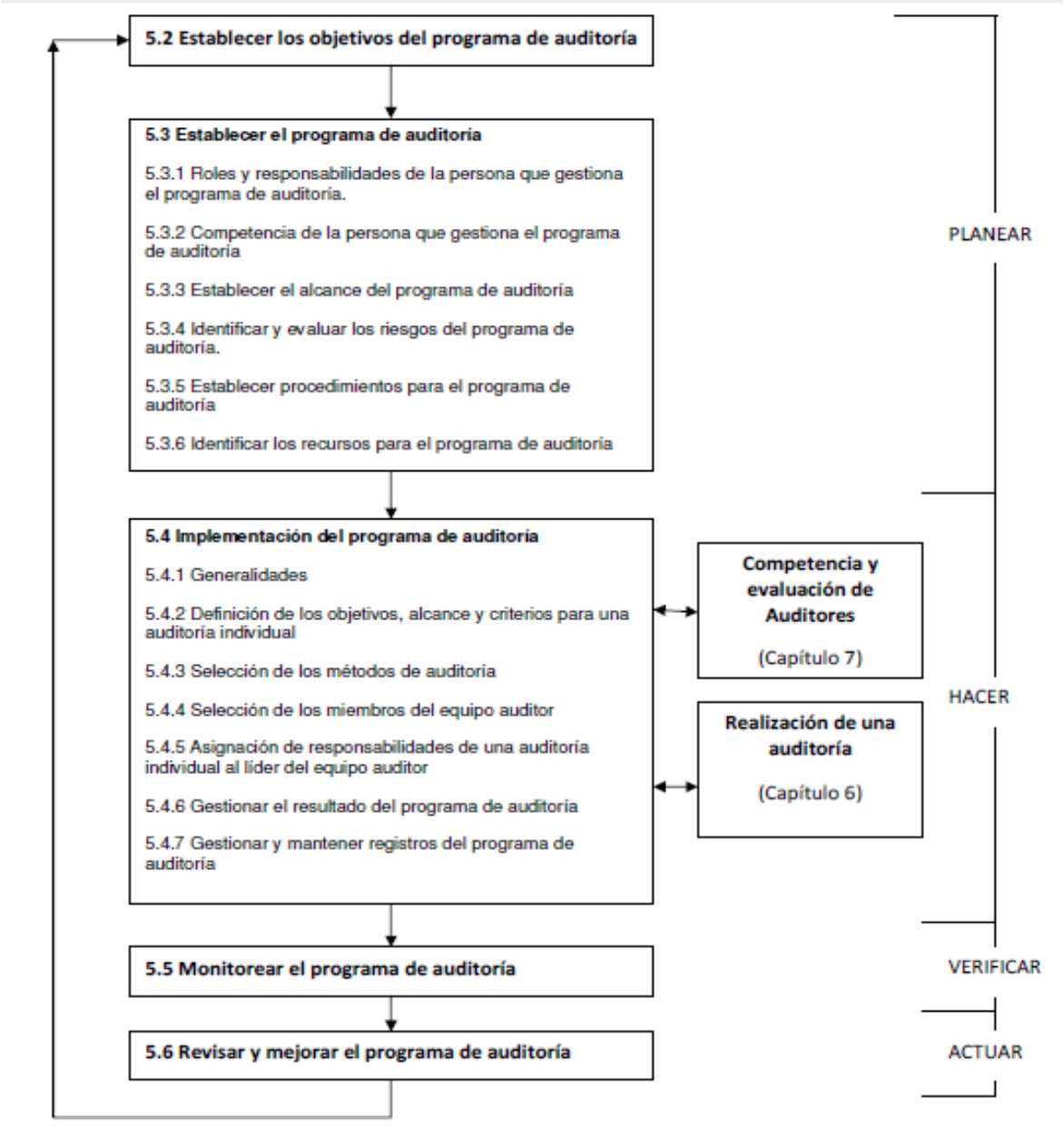
Se indican los 37 procesos de *COBIT 5*, los cuales son la referencia principal de las pruebas que serán incluidas en el manual.



Fuente: *COBIT* 5: Procesos Catalizadores (2012, pág. 24)

Anexo 5: Flujo de proceso para la gestión de un programa de auditoría.

En el siguiente anexo se procede a indicar el flujo de proceso para la gestión de un programa de auditoría según la norma ISO 19011.



Fuente: ISO 2011 (pág. 15).

Anexo 6: Auditorías seleccionadas para identificar los temas del manual

En el presente anexo se indica las auditorías seleccionadas para validar y verificar los temas seleccionados en el manual de auditoría de TI. Con la recomendación del encargado de TI se seleccionó una auditoría de cada sector.

Empresa sector asociaciones solidaristas

1. Último informe de auditoría externa referente a tecnologías de información (periodo 2016).
2. Estudio de vulnerabilidad de la red reciente y evidencia de la remediación de las vulnerabilidades detectadas.
3. Adjuntar los riesgos que sustentan la política de seguridad de la información actualizados para el periodo 2017.
4. Política de seguridad de la información formalmente establecida.
5. Evidencia de las revisiones de cumplimiento efectuadas a la política y controles de seguridad de la información en el periodo 2017.
6. Adjuntar los planes de acción para subsanar los incumplimientos de la política de seguridad de la información, así como para mejorar su efectividad de acuerdo con las revisiones efectuadas.
7. Listado de usuarios Activos en el Active Directory y bases de datos.
8. Reporte emitido por Recursos Humanos de los exfuncionarios que renunciaron, despidieron, fallecieron o se jubilaron durante el 2017.
9. Metodología formalmente aprobada para la gestión de servicios de terceros.
10. Planes formales para el mantenimiento periódico de servidores y equipos. Adjuntar evidencia de su ejecución.
11. Plan de Continuidad de TI, y el plan de pruebas de dicho plan en el periodo 2017.
12. Procedimiento de monitoreo de la infraestructura tecnológica.
13. Plan de capacitación formalmente establecido para los funcionarios de la unidad de tecnologías de información en el periodo 2017 y el respaldo de la ejecución de este.
14. Procedimiento formalmente documentado que mida el desempeño de los funcionarios de T.I y evidencia de su ejecución en el periodo 2017.
15. Plan formal de capacidad y desempeño de la plataforma tecnológica.
16. Metodología para el manejo de incidentes y problemas.
17. Actas del Comité de Informática o su equivalente correspondiente al 2017. Adjuntar además reglamento que regula gestión de este.
18. Políticas en cuanto al uso adecuado del equipo de cómputo, Internet y correo electrónico.
19. Políticas y procedimientos sobre la realización de respaldos y recuperación de datos.
20. Plan estratégico actualizado organizacional.
21. Plan estratégico actualizado de T.I.
22. Procedimiento para definición de perfiles de usuario.
23. Plan anual operativo de T.I. para el periodo 2017.
24. Metodología empleada para la administración del riesgo de tecnologías de información. Adjuntar evidencia de su implementación durante el 2017.
25. Informes de auditoría interna de los últimos doce meses en materia tecnológica emitidos en el 2017, incluir avance de las recomendaciones.
26. Lista de sistemas en producción, indicar el nombre del usuario experto por módulo, así como su correo electrónico.

Empresa sector Municipalidades

1. Metodología empleada para la administración de proyectos en tecnologías de información.
2. Reglamento Interno de la Comisión de Tecnologías de Información y Comunicación (CTIC). Adjuntar las actas de las sesiones realizadas durante el periodo 2017-2018.
3. Informes de Auditoría Interna sobre la gestión de tecnologías de información realizados durante el periodo 2017-2018.
4. Gestiones realizadas para la contratación de un auditor interno para tecnologías de información.
5. Base de datos de activos con corte al 31 de diciembre del periodo 2017.
6. Base de datos de Cuentas x Cobrar con corte al 31 de diciembre del 2017.
7. Base de datos del RUC con corte al 31 de diciembre del 2017.
8. Modelo de arquitectura de información de la municipalidad. Adjuntar evidencia de su aprobación.
9. Metodología para la Gestión de la Calidad de los procesos de T.I. Adjuntar evidencia de su ejecución.
10. Procedimiento/plan documentado para la medición de la capacidad y desempeño de la plataforma tecnológica. Adjuntar evidencia de su ejecución.
11. Usuarios activos definidos a nivel del Active Directory y bases de datos.
12. Lista de funcionarios que cesaron actividades durante el periodo 2017-2018 en la Municipalidad.
13. Metodología o procedimiento para la gestión de incidente y problemas. Adjuntar evidencia de las gestiones para la implementación del System Center Service Manager y capacitación de usuarios.
14. Evidencia de las gestiones realizadas para las revisiones de bitácoras del módulo de activos fijos y del sistema WIZDOM en general.
15. Bitácoras de los respaldos de información del periodo 2017-2018.
16. Planes de pruebas establecidos para los respaldos de información. Adjuntar evidencia de su ejecución y sus revisiones.
17. Política de seguridad de la información.
18. Evidencia de revisiones y capacitaciones efectuadas, para evaluar el cumplimiento y conocimiento de la política de seguridad de la información. Adjuntar resultados de la última evaluación y sus respectivas capacitaciones realizadas en el periodo 2017-2018.
19. Metodologías/procedimiento para la gestión de problemas de TI.
20. Metodología para la gestión de riesgos de TI.
21. Acuerdos de nivel de servicio para aquellos definidos en el catálogo de servicios de TI.
22. Plan de capacitación para los funcionarios de TI. Adjuntar evidencia de la ejecución de las capacitaciones realizadas en el 2017
23. Evidencia de las gestiones realizadas para la integración de los sistemas de RRHH y contabilidad.
24. Evidencia de la implementación de un histórico de intereses por cobrar guardado a nivel de base de datos para las cuentas por cobrar.
25. Evidencia de las gestiones realizadas para la integración del sistema de información geográfica con el sistema de bienes inmuebles.

Empresa sector Superintendencia

1. Procedimiento para el manejo de medios de almacenamiento.
2. Políticas y procedimientos sobre la realización de respaldos y recuperación de datos.
3. Bitácoras de los respaldos del año 2017 y plan de pruebas de los respaldos de información.
4. Plan o lineamiento formal para la administración de la capacidad y desempeño de la plataforma tecnológica.
5. Procedimiento formal para la gestión de cambios. Suministrar un reporte de los cambios realizados en el periodo 2017.
6. Procedimiento formal para la gestión de incidentes.
7. Procedimiento o mecanismo para la divulgación de la normativa relacionada con TI.
8. Cronograma actualizado de la implementación de las Normas Técnicas de la Contraloría General de la Republica.
9. Procedimiento para la gestión y revisión de perfiles de usuarios.
10. Informe de seguimiento por parte de las áreas usuarias relacionado a la revisión de los roles y perfiles del periodo 2017.
11. Plan Estratégico de Tecnologías de Información actualizado. Adjuntar detalle de la ejecución.
12. Plan Estratégico Institucional actualizado.
13. Plan anual operativo de TI del periodo 2017. Adjuntar el detalle de su ejecución.
14. Metodología formal para la gestión de la calidad de los productos y servicios de TI.
15. Plan de contingencias y continuidad de la plataforma tecnológica.
16. Plan de pruebas al plan de contingencias y continuidad para el periodo 2017. Adjuntar detalle de la ejecución de las pruebas realizadas.
17. Capacitaciones realizadas al personal sobre el plan de contingencias y continuidad.
18. Modelo de arquitectura de la información.
19. Política de seguridad de la información.
20. Mecanismo para evaluar el cumplimiento de la política de seguridad de la información. Adjuntar resultados de la última evaluación de su cumplimiento.
21. Metodología o lineamiento para la clasificación de la información.
22. Metodología o procedimiento para la administración de proyectos.
23. Lista de proyectos vigentes y en ejecución de T.I. del periodo 2017.
24. Usuarios definidos a nivel del active directory y bases de datos activos.
25. Reporte del Departamento de Recursos Humanos del personal que abandonó la Institución (despedido, jubilación, renuncia, otros) durante el periodo 2017 a la fecha a nivel institucional. Indicar en el reporte nombre completo, motivo y fecha de salida.
26. Informes de Auditoría Externa de T.I. de periodo 2016.
27. Metodología o lineamiento formal para la gestión de riesgos de T.I.
28. Evaluación de los riesgos de T.I. en el periodo 2017.
29. Planes de capacitación para el personal de T.I. del año 2017, presentar evidencia de su ejecución.
30. Informes de Auditoría Interna, relacionados con tecnologías de la información para el periodo 2017. Adjuntar evidencia de los seguimientos.
31. Reglamento del comité de T.I.
32. Actas firmadas de las sesiones efectuadas por el Comité de T.I. en el periodo 2017.
33. Lista de sistemas en producción, indicando por módulo el usuario experto y el contacto de este (correo y extensión).

Empresa sector Institución pública

1. Plan Estratégico de Tecnologías de Información actualizado. Adjuntar detalle de la ejecución.
2. Plan Estratégico Institucional actualizado.
3. Plan anual operativo de TI del periodo 2017. Adjuntar el detalle de su ejecución.
4. Normativa para el aseguramiento de la calidad de los productos y servicios de TI.
5. Metodología de administración de los riesgos de tecnologías de información. Adjuntar la evaluación de los riesgos de T.I. en el periodo 2017.
6. Política de Seguridad de la Información.
7. Mecanismo para evaluar el cumplimiento de la política de seguridad de la información. Adjuntar resultados de la última evaluación de su cumplimiento.
8. Plan de contingencias y continuidad de la plataforma tecnológica.
9. Plan de pruebas al plan de contingencias y continuidad para el periodo 2017. Adjuntar detalle de la ejecución de las pruebas realizadas.
10. Capacitaciones realizadas al personal sobre el plan de contingencias y continuidad.
11. Metodología o procedimiento para la administración de proyectos.
12. Lista de proyectos vigentes y en ejecución de T.I. del periodo 2017.
13. Reglamento del comité de T.I. 2017.
14. Actas firmadas de las sesiones efectuadas por el Comité de T.I. en el periodo 2017.
15. Plan de capacitación de T.I. para el periodo 2017. Adjuntar respaldo de ejecución.
16. Políticas y procedimientos debidamente documentados sobre la realización de respaldos y recuperación de datos.
17. Plan de pruebas de los respaldos de información.
18. Procedimiento o estándar para el desarrollo de software en dónde se definan, requerimientos, estudios de factibilidad, diseño y pruebas, documentación técnica, conversión de datos y puesta en producción.
19. Lista de sistemas en producción, indicando por módulo el usuario experto y el contacto de este (correo y extensión).
20. Procedimiento para la gestión de roles y perfiles (asignar, actualizar o remover).
21. Listado de roles y perfiles asignados a cada usuario de los sistemas de información.
22. Informe de seguimiento por parte de las áreas usuarias relacionado a la revisión de los roles y perfiles del periodo 2017.
23. Parametrización lógica de los sistemas en producción (composición de la contraseña, vencimiento de contraseña, historial de contraseña, entre otros.)
24. Usuarios definidos a nivel del active directory y bases de datos activos.
25. Reporte del Departamento de Recursos Humanos del personal que abandonó la Institución (despedido, jubilación, renuncia, otros) durante el periodo 2017 a nivel institucional. Indicar en el reporte nombre completo, motivo y fecha de salida.
26. Informe del seguimiento de las pistas de auditoría de los sistemas de información del periodo 2017.
27. Modelo formal de la arquitectura de la información.
28. Informes de Auditoría Externa de T.I. de periodo 2016.
29. Normativa para la atención de incidentes y solicitudes de TI.
30. Base de datos de infracciones con corte al 31-12-2017.
31. Estructura organizacional interna de la ATI.
32. Evidencia de las acciones para subsanar las debilidades sobre los procesos llevados en Excel de Presupuesto e inventarios.
33. Evidencia de las acciones para subsanar la debilidad relacionado con registro de los bienes duraderos llevados en Access.

Empresa sector operadora de pensiones

1. Procedimiento para la gestión de la capacidad y desempeño de la plataforma tecnológica.
2. Procedimiento para la gestión de servicios de TI. Adjuntar el catálogo de servicios de TI y los acuerdos de nivel de servicio establecidos con las áreas usuarias.
3. Inventario de licencias de software adquiridas. Adjuntar un reporte del software instalado en los equipos de la institución.
4. Inventario de activos de TI actualizado.
5. Política de seguridad de la información. Adjuntar evidencia del monitoreo del cumplimiento de la política.
6. Estudio de vulnerabilidad de la red. Adjuntar el plan de acción para subsanar las deficiencias identificadas.
7. Procedimiento para la gestión de roles y permisos en los sistemas. Adjuntar evidencia de la revisión periódica de los perfiles de usuario.
8. Procedimiento para la gestión de la configuración.
9. Procedimiento para la gestión de cambios de TI.
10. Procedimiento para la gestión de incidentes y problemas de TI.
11. Procedimiento de respaldos y recuperación de información. Adjuntar las bitácoras de los respaldos realizados durante el periodo 2018 y evidencia de las pruebas realizadas.
12. Lista de sistemas que se encuentran en producción. Adjuntar la lista de usuarios expertos por cada uno de los módulos de los sistemas.
13. Contratos establecidos con el proveedor de Internet y evidencia de las gestiones legales y administrativas para el cumplimiento de las cláusulas contractuales establecidas.
14. Plan de implementación de las Normas técnicas para la gestión y el control de las Tecnologías de Información. Adjuntar detalle de su ejecución.
15. Lista de contratos vigentes con proveedores de TI. Adjuntar evidencia del seguimiento al cumplimiento contractual.
16. Modelo de arquitectura empresarial y sistemas de información. Adjuntar, además, evidencia de su formalización.
17. Plan de continuidad de TI vigente. Adjuntar evidencia de las pruebas y capacitaciones realizadas durante el periodo 2018.
18. Plan estratégico de TI vigente. Adjuntar evidencia del seguimiento realizado al cumplimiento del plan.
19. Plan anual operativo de TI del periodo 2018. Favor adjuntar evidencia del seguimiento realizado al cumplimiento del plan.
20. Plan presupuestario de TI del 2018. Adjuntar evidencia de su ejecución.
21. Evidencia de la revisión de las pistas de auditoría de los sistemas de información.
22. Metodología para la gestión de riesgos de TI. Adjuntar el análisis de riesgos realizado durante el periodo 2018, así como evidencia de su aprobación.
23. Metodología para la gestión de proyectos de TI. Adjuntar la lista de los proyectos ejecutados durante el periodo 2018.
24. Procedimiento/plan de adquisición de TI del periodo 2018. Adjuntar evidencia de su ejecución.
25. Metodología para la gestión de calidad de TI.
26. Plan de capacitaciones del personal de TI. Adjuntar evidencia de su ejecución.
27. Evaluaciones del desempeño de los colaboradores de TI.
28. Metodología de desarrollo de software. Adjuntar la lista de los proyectos de desarrollo de software realizados durante el periodo 2018.
29. Procedimiento para la gestión del control interno de TI.
30. Informes de auditoría interna emitidos durante el periodo 2018

Anexo 7: Carta revisión filóloga

Astrid Quirós Granados

Filología U.C.R

A quien interese:

Yo, Astrid Quirós Granados, Filóloga de la Universidad de Costa Rica; con cédula de identidad 3-438-182, inscrita en el Colegio Licenciados y Profesores, con el carné N° 80791 y en la Asociación Costarricense de Filólogos, con el carné N° 0096, hago constar que he revisado el trabajo y sus conclusiones. Y he corregido en él, los errores encontrados en redacción, ortografía, gramática y sintaxis. El trabajo se titula:

PROPUESTA DE UN MANUAL DE AUDITORÍA DE TECNOLOGÍA DE INFORMACIÓN. CASO DESPACHO

CARLOS RAMÍREZ CERDAS

Se extiende la presente certificación a solicitud del interesado, en la ciudad de San José a los cinco días del mes de noviembre del dos mil dieciocho. La filóloga no se hace responsable de los cambios que se le introduzcan al trabajo posterior a su revisión.

Astrid Quirós Granados

Teléfono: 8315 95 27 Correo: asqui24@hotmail.es