Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Estudio de una metodología de trabajo para la realización de auditorías integradas de sistemas de información

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Eloy Millet Colomar

Tutor: Ignacio Gil Pechuán

2014-2015

Resumen

El gobierno y la seguridad de los sistemas de información empresariales son conceptos claves que habilitan la generación de valor para la empresa a través de la tecnología. En el contexto actual, existen gran cantidad de marcos de trabajo y/o normativas que establecen buenas prácticas y controles aplicables a diferentes ámbitos del proceso de gobierno y gestión de TI. El presente TFG tiene como objetivo primario establecer un marco integrado de auditoría de sistemas de información, mediante el mapeo del marco de trabajo COBIT5 de ISACA con las normas ISO 20.000-1:2011, ISO 27002:2013, PMBOK5 y CMMI-DEV 1.3.

Palabras clave: auditoría, sistemas de información, COBIT, seguridad, gobierno, ISO, PMBOK, CMMI, ISACA.

Abstract

The governance and the security of enterprise information systems are key concepts that enable the creation of business value through technology. In the current context, there are plenty of frameworks and / or regulations that establish best practices and controls applicable to different areas of the process of governance and management of IT. This TFG aims to establish an integrated information systems auditing framework by mapping framework COBIT5 by ISACA with ISO standards 20.000-1:2011, ISO 27002:2013, PMBOK5 and CMMI-DEV 1.3

Keywords: audit, information systems, COBIT, security, government, ISO 27000, ISO 20000, PMBOK, CMMI, ISACA.

Tabla de contenidos

1. Objetivos y contexto del TFG

1.1. Introducción

Desde hace aproximadamente un año he tenido la oportunidad de introducirme a nivel laboral en el mundo de la consultoría y de la auditoría de Sistemas de Información, concretamente en el área de seguridad de la información de la mano de la empresa Auren.

Previamente, ya había despertado en mí el interés por este apasionante sector y durante mi labor como consultor y auditor de sistemas de información he tenido la oportunidad de conocer de primera mano los intereses, las necesidades y las inquietudes que las empresas y organizaciones españolas muestran respecto a la seguridad, la privacidad y la gestión de los sistemas de información.

Ha sido durante este periodo en el que he detectado ciertos campos en los que las empresas del sector tienen debilidades en cuanto a la oferta de productos o servicios que aporten un valor extra a las organizaciones y en base a ello se define el presente Trabajo Final de Grado, el cual se desarrolla en los apartados siguientes.

1.2. Justificación del TFG

Como se ha esbozado previamente, las empresas han venido adoptando a un ritmo casi vertiginoso diferentes soluciones informáticas y sistemas de información con el objetivo de mejorar sus procesos de gestión, fabricación o contabilidad entre otros y para optimizar las operaciones y los servicios prestados. La introducción de los sistemas de información, en efecto han logrado mejorar la competitividad de las empresas hasta el punto en el que hoy en día no se puede concebir una empresa sin que ésta se apoye en la tecnología.

Paralelamente, esta presencia masiva de sistemas informáticos, la mayoría de ellos interconectados de algún modo a través de la Red ha originado nuevas preocupaciones tales como el buen gobierno de las tecnologías, la seguridad, la disponibilidad y la confidencialidad de la información. Estas preocupaciones han motivado la aparición de multitud de normas, leyes o estándares que pretenden guiar a las empresas en diferentes áreas relacionadas con el uso de la informática.

En la actualidad, las empresas han adoptado e implantado en mayor o menor medida y con mayor o menor éxito algunos de los marcos de trabajo o leyes existentes ya sea por imperativo legal o por la búsqueda de la excelencia y la diferenciación respecto a sus competidores.

La presencia (tal vez excesiva) de normas y marcos de trabajo en el sector y dado el hecho constatado de que ciertas de éstas normas son más o menos reconocidas

dependiendo del país o continente en el que se opere ha supuesto que coexistan en las empresas.

El presente TFG surge de la observación de los problemas y las necesidades que experimentan las empresas que disponen de varios sistemas de gestión de TI implantados, donde todos ellos requieren de revisiones o auditorías periódicas de cumplimiento de sus requisitos. Adicionalmente, el trabajo con estas normativas ha permitido comprobar que ciertos puntos de las mismas se solapan motivo por el cual surge la idea de alinear aquellos controles semejantes para crear una herramienta de trabajo que permita a los auditores de sistemas de información realizar su labor de forma optimizada, a la vez que se presta un servicio de calidad y con valor a las empresas.

1.3. Objetivos

Dentro del área de las tecnologías de la información y, en concreto, de la auditoría de sistemas informáticos existen numerosas áreas de trabajo y campos en los que es posible trabajar en la actualidad. En el panorama de hoy en día, existe un gran número de organizaciones, sobretodo de tamaño medio/grande que tratan de mejorar sus procesos de gestión, entrega y/o desarrollo de sistemas de información mediante la implantación de marcos de trabajo, normativas o estándares. En numerosas ocasiones se presenta la obligación, que puede venir impuesta por un tercero o ser un requisito interno, de realizar evaluaciones acerca del grado de cumplimiento respecto a una determinada referencia.

Existen numerosas entidades y empresas que ofrecen entre sus servicios la auditoría de diferentes normas, pero en la gran mayoría de los casos estas se circunscriben a una norma o un framework determinado. Dada la necesidad de ofrecer productos acorde a la situación del mercado actual, se considera necesaria la creación de nuevas herramientas y metodologías de trabajo que permitan concentrar esfuerzos y reducir costes de cara a realizar auditorías integradas de sistemas de información.

Es por tanto que se define el objetivo principal del presente trabajo como la creación de una metodología de trabajo para la realización de auditorías integradas a sistemas de información. Para la primera aproximación se han considerado normas y marcos de trabajo que son referentes dentro del escenario actual, tomando como referencia principal y como base a COBIT 5 de ISACA.

Para poder alcanzar el objetivo general presentado anteriormente, se definen una serie de metas que son las siguientes:

- Seleccionar las normas y marcos de trabajo más relevantes a incluir.
- Identificar los controles pertinentes para el fin perseguido de dichas normas.
- Estudiar y definir una metodología para el mapeo de controles.
- Realizar el mapeo de los controles de todas las normas seleccionadas.
- Generar una herramienta de trabajo que permita al auditor realizar una auditoría de forma integrada

- Estudiar la aplicabilidad y los resultados que se pueden obtener mediante la herramienta generada

La finalidad última que se pretende lograr mediante el presente trabajo es evitar y eliminar duplicidades, optimizar recursos y simplificar al máximo la gestión de todos los sistemas de gestión implantados en las empresas, mejorando así su rendimiento de forma global. La reducción de costes y la optimización del tiempo requerido para desarrollar una auditoría junto con el aporte de valor extra para los clientes, pueden ser la clave para elevar el nivel de competitividad de una empresa prestadora de servicios en un entorno económicamente complejo como el actual.

2. Contexto: Informática y auditoría

El ser humano siempre ha tenido normas y procedimientos que establecen los parámetros de la convivencia. De estas normas se deriva la necesidad de controlar, observar y validar acciones y comportamientos. Implícitamente, se han venido desarrollando acciones de vigilancia para evitar errores y fraudes durante toda la historia de la humanidad por lo cual la figura de la auditoría siempre ha existido.

El origen de la auditoría entendida en los términos actuales se atribuye a Reino Unido. Debido la Revolución Industrial y a varias quiebras sufridas por pequeños ahorradores, se desarrolló la auditoría con el objeto de garantizar la confianza en inversores. Este concepto no tardó en extenderse a otros países y actualmente su alcance es mayor que nunca.

Actualmente, podemos definir la auditoría en términos generales como "un examen objetivo y sistemático de uno o más aspectos de una organización que comprare lo que ha realizado la organización con un conjunto de criterios o requerimientos establecidos". (Gantz, S., 2013)

La auditoría informática o de sistemas de información surge con la aparición de las los primeros computadores que se implantan en las empresas para mecanizar y automatizar partes de su proceso de gestión de las finanzas. El trabajo del auditor que siempre se había basado en leer y escuchar deja de ser el mismo en el momento en que la información se encuentra en un soporte y formato que no entienden, y del que no se fían. El objetivo general y el alcance de una auditoría en un entorno de sistemas informáticos es el mismo que el citado anteriormente. En este caso el ordenador procesa y guarda la información de una forma distinta a la tradicional, por lo que algunos de los procedimientos seguidos por los auditores han cambiado acorde.

2.1. Fundamentos de la auditoría de S.I.

Actualmente, vivimos en un momento en el que la penetración de los sistemas de información es total dentro de las organizaciones empresariales y en las sociedades desarrolladas. Hoy en día no se concibe la viabilidad de ninguna empresa sin hacer uso de los sistemas de información, es más, en muchos casos el uso que haga una organización de la tecnología puede ser determinante para competir en un mercado cada vez más complejo y globalizado.

La información y las tecnologías asociadas a ella se han convertido en activos críticos para cualquier empresa, tanto pública como privada y de cualquier sector. Así pues, las empresas tienen un gran interés en asegurarse de que los recursos tecnológicos que emplean cumplen con su cometido de forma efectiva y que su protección frente a errores o acciones maliciosas es correcta.

Se puede afirmar que la auditoría de los sistemas de información ya se ha desligado de la auditoría financiera y constituye un área de conocimiento con entidad propia que evoluciona muy rápidamente en conjunción con la llamada Sociedad de la Información.

Se puede definir la auditoría informática como "el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos."(Piatini, M., 2001)

Las auditorías informáticas pueden abarcar toda la organización o centrarse en un área o proceso determinado. Cualquiera que sea el alcance de una auditoría informática y del método utilizado, ésta se enfrentará a uno o más de los siguientes elementos tecnológicos:

- Centros de datos
- Redes
- Telecomunicaciones
- Sistemas operativos
- Bases de datos
- Sistemas de almacenamiento
- Entornos virtualizados
- Servidores Web y de aplicaciones
- Paquetes de software
- Interfaces de usuario
- Dispositivos móviles
- Entornos cloud

La figura del auditor informático debe ser una persona con un conocimiento tanto de los métodos de auditoría general como de los específicos del área de aplicación. No existe una regulación que determine el camino formativo que un auditor informático debe seguir, por tanto se puede alcanzar el éxito como auditor informático siguiendo diferentes caminos, tal y como ilustra Stephen Gantz en su libro "Basics of IT Audit":

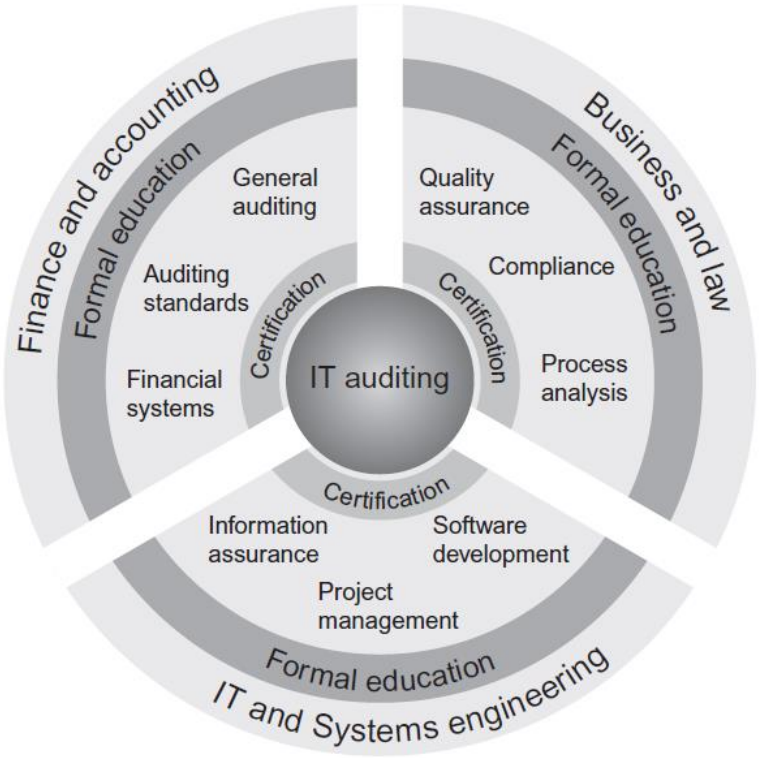

Ilustración 1: Caminos para la formación de auditores informáticos. (Gantz, S., 2013)

2.2. Auditoría interna y externa

Hoy en día se pueden distinguir dos tipos de auditoría de SI que comparten características pero que se distinguen claramente por la naturaleza y alcance de sus funciones. Tanto la interna como la externa tienen un rol importante a la hora de asegurar la integridad y la validez de los datos en entornos informatizados.

Auditoría interna

El *Institute for Internal Auditors* la define formalmente como "Actividad de aseguramiento y consultoría independiente y objetiva diseñada para añadir valor y mejorar las operaciones de las organizaciones". En este caso, personal interno de la organización desarrolla la actividad de auditoría para asegurar que la organización cumple con los criterios de calidad y los requerimientos legales que se han establecido. El auditor interno es el encargado de controlar día a día el funcionamiento de la empresa de acuerdo a las reglas y exigencias que se marcan desde la dirección. La correcta definición y seguimiento de los controles internos establecidos es la tarea clave a desarrollar por parte del auditor interno.

Todos los estándares de auditoría establecen que un auditor debe desarrollar su actividad de forma objetiva e independiente. En este caso la objetividad debe mantenerse, aun cuando los intereses son comunes y en ocasiones puede haber

conflictos. A este respecto, la norma "UNE-EN ISO 19011:2012 Directrices para la auditoría de los sistemas de gestión" establece que Los auditores son independientes de la actividad que es auditada y están libres de sesgo y conflicto de intereses. Los auditores mantienen una actitud objetiva a lo largo del proceso de auditoría para asegurarse de que los hallazgos y conclusiones de la auditoría estarán basados sólo en la evidencia de la auditoría. Otras instituciones como ISACA o el ya mencionado Institute of Internal Auditors también hacen referencia al principio de imparcialidad del auditor interno.

Stephen Gantz establece que los beneficios de las auditorías internas son los siguientes:

- Soporte al gobierno de IT, gestión del riesgo y programas de cumplimiento.
- Verificación de la adherencia de la organización a las políticas, procedimientos y estándares definidos internamente.
- Satisfacer requerimientos para alcanzar o mantener los procesos de calidad, madurez y gestión.
- Preparación anticipada para auditorías externas.

Auditoría externa

En este caso, la figura del auditor externo se representa mediante alguien ajeno a la organización que evaluará el cumplimiento de una serie de normas o requerimientos definidos externamente a la organización. Las organizaciones típicamente contratan servicios de auditoría externa para evaluar el cumplimiento de requisitos legales, de calidad o de certificación. Así pues, el auditor externo evaluará a la organización en un momento de tiempo determinado, mientras que el interno lo hacía en un periodo de tiempo continuado. Esta modalidad representa un segmento distinto dentro de los servicios profesionales ofrecidos por empresas especializadas cuyo negocio se basa en ofrecer servicios de auditoría a las empresas.

Las auditorías externas son necesarias para las organizaciones ya que al superarlas, otros grupos de interés (clientes, proveedores y gobiernos) son conscientes de que se cumple con una u otra norma de calidad o requisito legal establecido. La credibilidad de las auditorías externas generalmente es mayor que en el caso de las internas, aun cuando se hayan utilizado los mismos procedimientos y criterios.

Uno de los desafíos a los que se enfrenta un auditor externo cuando actúa en una organización, es el de tener acceso a todos los datos relacionados con la actividad implicada y asegurarse que esos datos son los correctos.

2.3. Tipos de auditoría informática

La enorme explosión de las tecnologías de la información y su implantación masiva tanto en las organizaciones como en las sociedades introducen constantemente nuevas áreas de actividad para los auditores de sistemas de información. El término auditoría informática se refiere al proceso de revisión de todo aquello en lo que un sistema

informático tenga un rol relevante. Con esta definición, el lector se podrá hacer una idea de que las áreas de actividad o tipologías relativas a la auditoría informática son muy amplias, por lo que tratar de hacer una clasificación rigurosa y completa probablemente acabe en fracaso. Antonio Minguillón, en su obra titulada "La auditoría de sistemas de información integrada en la auditoría financiera" del año 2010, obra galardonada con el VIII Premio de Investigación Mestre Racional recoge una posible clasificación basada en los objetivos fijados específicamente para cada auditoría.

Algunos tipos posibles de auditorías informáticas son:

Auditoría de la administración electrónica

Con la entrada en vigor de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos aparece también la necesidad de auditar si las administraciones afectadas cumplen con la ley y en qué grado. Esta es un área reciente pero que puede suponer una importante fuente de trabajo en un futuro próximo.

Auditoría de gestión de datos personales

El artículo 96 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, estableció la obligatoriedad de realizar determinadas auditorías para los niveles de protección medio y alto. Actualmente, los datos de carácter personal (así como los no personales) suelen ser manejados por entornos informatizados por lo que este tipo de auditorías se ha convertido en una especialidad propia, principalmente llevada a cabo por auditores no vinculados al sector público.

Auditoría forense

Cuando existen sospechas de que se haya podido producir un fraude o una actuación ilícita sobre un dispositivo informático, existe la posibilidad de realizar investigaciones específicas para tratar de obtener evidencias, que después de ser analizadas ayudarán a esclarecer la naturaleza jurídica del acto investigado. Esta es un área que está cobrando importancia actualmente debido a que la forma en la que nos comunicamos involucra algún medio informático. Este tipo de actuaciones se realizan tanto por los cuerpos de seguridad del estado como por agentes privados.

Auditoría de gestión

Examen de un sistema informático para evaluar si los objetivos previstos al implementar el sistema han sido alcanzados efectivamente, con criterios de economía y eficiencia.

Auditorías específicas sobre adquisición de equipos y sistemas

Dada la complejidad y el elevado coste de desarrollo y adquisición de los sistemas informáticos que se implantan en grandes empresas y/o gobiernos, este tipo de auditorías son realizadas con frecuencia tanto en el sector público como en el privado. El riesgo en este tipo de adquisiciones es elevado, así que auditando los requerimientos y necesidades de la organización es posible mitigarlos y que la adquisición sea acertada.

Auditoría de seguridad informática

Como ya se ha comentado previamente, la información es un activo crítico para muchas organizaciones, por lo que asegurar que se mantiene la confidencialidad, la integridad y la disponibilidad tanto de los datos como de los sistemas constituye un área propia dentro del campo de auditoría de sistemas de información. Los sistemas informáticos presentan constantes vulnerabilidades y esto obliga a empresas e instituciones públicas a invertir grandes cantidades de recursos en asegurarlos. Esta área será en la cual se encuadrará la segunda parte del presente trabajo.

Auditoría de aplicaciones informáticas/sistemas de información y auditorías limitadas sobre controles generales y de aplicación

Análisis de las operaciones llevadas a cabo por un sistema informático para evaluar el grado de confianza que puede depositarse en las transacciones procesadas por el sistema.

Auditoría de sistemas de información realizada en el marco de una auditoría financiera

Aunque se sitúe como la última de la lista, no por ello debemos darle menos importancia a esta área, ya que así fue como nació el concepto de auditoría informática. La adopción generalizada de sistemas de información como base para la gestión de la información en las empresas ha requerido que se auditen estos sistemas de información para verificar que los datos que contienen son confiables de cara a efectuar una auditoría financiera.

2.4. Principios deontológicos del auditor informático

Ejercer la profesión de auditor informático conlleva la aceptación en todos los casos de una serie de principios deontológicos o códigos de conducta. El comportamiento profesional exigible a un auditor informático conlleva dos facetas (Mario Piatini, p 174) íntimamente ligadas.

La primera corresponde a la aplicación de sus conocimientos técnicos con la finalidad de determinar, en base a los mismos, las condiciones de seguridad, fiabilidad y calidad de los medios, elementos o productos que conforman el sistema informático a auditar y recomendar las medidas que estime convenientes para su mejora.

La segunda debe poner de manifiesto la aplicación de los fundamentos humanísticos que como persona y como profesional le son éticamente exigibles.

La Asociación de auditores informáticos ISACA (Information Systems Audit and Control Association), establece un Código de Ética Profesional para guiar la conducta profesional y personal de los miembros y/o poseedores de certificaciones de la asociación. Las normas que rigen a los profesionales asociados a ISACA son las siguientes:

Los miembros y los poseedores de certificaciones de ISACA deberán:

1. Respaldar la implementación y promover el cumplimiento con estándares y procedimientos apropiados del gobierno y gestión efectiva de los sistemas de información y la tecnología de la empresa, incluyendo la gestión de auditoría, control, seguridad y riesgos.

2. Llevar a cabo sus labores con objetividad, debida diligencia y rigor/cuidado profesional, de acuerdo con estándares de la profesión.

3. Servir en beneficio de las partes interesadas de un modo legal y honesto y, al mismo tiempo, mantener altos niveles de conducta y carácter, y no involucrarse en actos que desacrediten su profesión o a la Asociación

4. Mantener la privacidad y confidencialidad de la información obtenida en el curso de sus deberes a menos que la divulgación sea requerida por una autoridad legal. Dicha información no debe ser utilizada para beneficio personal ni revelada a partes inapropiadas.

5. Mantener la aptitud en sus respectivos campos y asumir sólo aquellas actividades que razonablemente esperen completar con las habilidades, conocimiento y competencias necesarias.

6. Informar los resultados del trabajo realizado a las partes apropiadas, incluyendo la revelación de todos los hechos significativos sobre los cuales tengan conocimiento que, de no ser divulgados, pueden distorsionar el reporte de los resultados.

7. Respaldar la educación profesional de las partes interesadas para que tengan una mejor comprensión del gobierno y la gestión de los sistemas de información y la tecnología de la empresa, incluyendo la gestión de la auditoría, control, seguridad y riesgos.

El incumplimiento de este Código de Ética Profesional puede acarrear una investigación de la conducta de un miembro y/o titular de la certificación y, en última instancia, medidas disciplinarias.

2.5. Marco legal y normativo

Actualmente, debido a la creciente complejidad de las organizaciones y de los sistemas de información presentes en ellas, el marco legal y normativo por el cual se rigen estas organizaciones es amplio y en ocasiones confuso. Las empresas deben cumplir con ciertos requerimientos de cara a posicionarse en un mercado determinado, ya sea porque lo exige la ley o porque los clientes y los proveedores lo demandan. Las empresas deben establecer planes de mejora continua y de innovación para ser competitivas y eso les conduce a la necesidad de evaluar si su gestión de las TI, su seguridad y sus riesgos son correctos.

Dentro de este marco se engloban tanto requerimientos legales establecidos por las autoridades como requerimientos de mercado en forma de certificaciones y estándares de calidad. Todos estos requerimientos son susceptibles de ser auditados interna o

externamente para determinar el progreso y afrontar acciones de mejora. El marco de desarrollo del presente Trabajo final de Grado es la Comunitat Valenciana y el Estado Español, por lo que el resto del apartado se referirá a requerimientos aplicables dentro del mismo.

En la siguiente tabla se enumeran algunos de los requerimientos que pueden conducir a la realización de una auditoría de sistemas de información en una empresa, ya sea como actividad única o como apoyo.

Requerimiento	Categoría	Descripción
LOPD	Ley	Ley 15/1999 de Protección de Datos de Carácter Personal. Tiene como objeto garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas en lo que concierne al tratamiento de sus datos personales.
Ley de Administración Electrónica	Ley	Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. Esta ley confiere unos derechos concretos a los ciudadanos en lo referente a su forma de comunicarse con la Administración Pública.
LSSI	Ley	Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico. Ley que regula las actividades de los proveedores de servicios a través de Internet
ISO 9001	Norma	Norma que determina los requisitos para un sistema de gestión de la calidad.
ISO 14001	Norma	Estándar internacional de gestión ambiental.
ISO 20000	Norma	Norma para gestión de servicios de TI
ISO 27001	Norma	Norma que especifica los requisitos para la implantación de un sistema de gestión de la seguridad de la información.
ISO 19011	Norma	Detalla los requisitos para la realización de auditorías de sistemas de gestión ISO 9001 e ISO 14001.
ISO 38500	Norma	Norma que se aplica a los procesos de gestión de las TI en todo tipo de organizaciones. Proporciona una serie de principios para que la dirección de las organizaciones los utilices al evaluar, dirigir y monitorear el uso de las TI.
ITIL	Framework	Modelo de buenas prácticas ampliamente aceptado a nivel mundial para la gestión de servicios de TI.
COBIT	Framework	Framework desarrollado por ISACA dirigido al control y gestión de los sistemas de información en las empresas. El presente trabajo hará uso de COBIT como metodología de trabajo debido a la amplia aceptación y prestigio de que dispone a nivel global.

Esta tabla no pretende ser una relación completa de requerimientos influyentes a la hora de realizar una auditoría de sistemas de información, sino una mera referencia a los puntos más importantes en el entorno actual. Todas las referencias anteriores

pueden constituir el alcance de una auditoría de sistemas de información y por tanto son relevantes para el marco de este trabajo.

3. Proceso de auditoría informática

La auditoría informática es un proceso complejo que contempla una gran variedad de diferentes escenarios. Pese a ello, existen metodologías, marcos de trabajo y/o estándares para guiar el proceso de auditoría. Todas estas guías tienen algunos aspectos en común y uno de ellos es la descomposición del proceso en fases o etapas. Generalmente se habla de planificación, ejecución y conclusión o presentación del informe de auditoría. A menudo se usan diferentes nombres más o menos acertados para designar estos pasos, pero el concepto subyacente suele ser idéntico. Stephen Gantz contempla una fase adicional al proceso que es la de respuesta a los hallazgos, en la que el auditor elabora un plan de acciones correctoras para la organización auditada. Otros autores consideran que esta etapa queda fuera del ámbito de la auditoría y entra en el campo de la consultoría por lo que se tendría que desarrollar de forma separada. A continuación se detalla el proceso de auditoría de acuerdo a la descomposición presentada.

3.1. Planificación

Como todo proyecto de envergadura, la planificación siempre es el primer paso a seguir. Esta etapa suele ser crítica en la mayoría de los casos y habitualmente es aceptado el hecho de que con una correcta planificación se pueden alcanzar los objetivos, mientras que sin ella el proyecto tiene pocas posibilidades de ser exitoso. La planificación engloba todas las actividades necesarias para asegurarse de que la auditoría satisface los objetivos de la organización. El conjunto de estas actividades se plasmarán en un plan de auditoría. Este plan contendrá, entre otros, los siguientes aspectos:

1. Alcance. Definir el alcance es importante ya que marcará los objetivos y las áreas funcionales, procesos, departamentos o localizaciones de la organización a auditar. Este trabajo se debe hacer conjuntamente con el cliente o el demandante.

2. Objetivos. Deben quedar claros cuáles son los objetivos de la auditoría. Una correcta definición de objetivos facilita el trabajo de planificación posterior y permite asegurarse de que la auditoría verificará el correcto funcionamiento de las áreas definidas.

3. Contexto. Se definirá el entorno tecnológico en el cual se va a desarrollar la actividad.

4. Calendario y recursos. Se definirá un calendario identificando hitos en los cuales el trabajo se revisará y los recursos a utilizar durante el proceso.

5. Metodología de trabajo. En este punto se especifica la metodología de trabajo que se usará durante el proceso. Suele adoptarse una de las ya definidas por algún

organismo reconocido y aceptadas mundialmente, como por ejemplo el framework COBIT de ISACA.

3.2. Ejecución

Esta etapa central se basa en desarrollar el trabajo de auditoría, ejecutando los controles, entrevistas y análisis pertinentes a los elementos o miembros de la organización indicados para posteriormente compararlos con los requisitos o criterios de referencia para poder emitir el informe de conclusiones. Esta tarea consiste en encontrar y recolectar evidencias in situ para posteriormente analizarlas.

La tarea de recolección de evidencias puede ser ardua y siempre debe desarrollarse teniendo en cuenta el alcance y objetivos de la auditoría. Los procesos, sistemas o elementos examinados deben ser aquellos que nos puedan conducir a la evidencia, sin excederse en exámenes no oportunos que puedan violar los acuerdos establecidos con la organización. El proceso de obtención de evidencias debe quedar documentado en todo momento, siendo en algunos casos necesaria la presencia de un fedatario público que verifique que no se han manipulado las fuentes. Esto sucede por ejemplo en auditorías forenses dónde el proceso de obtención de evidencias es muy delicado y se debe ser muy transparente si se quiere defender un informe posterior ante un juez. En las guías de auditoría que se detallan en la ISO 19011 (Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental) se identifican muchas fuentes de información que los auditores pueden seleccionar para la obtención de evidencias. Se destacan como fuentes de información documentos, entrevistas con el personal adecuado, observación directa, aplicaciones software y test de simulación. En el caso de enfrentarse a volúmenes de datos que excedan la capacidad de procesamiento del equipo auditor se pueden realizar muestreos significativos para tratar de obtener las evidencias. Esto puede reducir el coste notablemente pero también puede ser peligroso por lo que el equipo debe asegurarse de que las técnicas de muestreo garantizan la representatividad del conjunto global de datos.

Posteriormente, con las evidencias recolectadas y debidamente custodiadas, el equipo auditor procederá al análisis en el cual se aplicarán los métodos y las técnicas necesarias para poder evaluar en qué medida se han cumplido o no los objetivos marcados para la auditoría. Los auditores deberán describir los métodos analíticos usados para evaluar la información recolectada. En este paso, el uso de herramientas CAAT (Computer Assisted Audit Techniques) permite al auditor analizar de forma automática grandes cantidades de datos para buscar excepciones o anomalías, análisis de archivos log, realizar muestreos o probar el cumplimiento de controles y procedimientos. Del análisis de la información se desprenderán los hallazgos y las conclusiones de auditoría que posteriormente se detallarán en el informe.

3.3. Informe

Para finalizar el proceso, el auditor escribirá y remitirá al cliente un informe de auditoría que contenga todo lo mencionado anteriormente y los hallazgos y conclusiones alcanzadas. La mayoría de guías y metodologías diferencian entre hallazgos y conclusiones de auditoría. Los hallazgos corresponden directamente a los criterios de auditoría e indican el cumplimiento o no de dichos criterios. Las conclusiones son formuladas a partir de los hallazgos, la experiencia y el conocimiento del auditor mediante un proceso de razonamiento. Entre las conclusiones se pueden encontrar acciones correctivas propuestas a la organización, oportunidades recomendadas para alcanzar algún propósito interesante o recomendaciones para mitigar algún riesgo detectado. En el informe se suelen detallar las debilidades detectadas ya que suele ser lo más apreciado, aunque enfatizar los puntos fuertes de la organización también entra dentro del trabajo de auditoría. Al presentar los resultados es importante identificar el marco de referencia utilizado en la auditoría para evitar componentes de subjetividad en las conclusiones. Como escribe Antonio Minguillón no es lo mismo decir "La gestión de contraseñas no es adecuada" que "la gestión de contraseñas no es conforme con la norma ISO 27000 sobre seguridad de la información".

Normalmente los informes de auditoría incluyen información sensible y confidencial que la organización no desea que se haga transmita a terceros por lo que se debe tener especial cuidado en el tratamiento de estos documentos. Opcionalmente, a la entrega del informe final de auditoría se puede iniciar un trabajo de implantación y seguimiento de acciones correctivas a cargo del mismo equipo o de otros profesionales. La finalidad de esta tarea es mejorar los procesos de la organización y mitigar riesgos o amenazas detectadas.

4. Organizaciones y marcos de referencia

Ya se ha mencionado la multitud de dimensiones que una auditoría informática puede comprender y este hecho, junto con la complejidad y volumen de las empresas de hoy en día ha propiciado que numerosas entidades relacionadas con el tema aparezcan tanto a nivel nacional como internacional. No existe una aproximación a la auditoría que se considere la mejor o la más adecuada y que funcione perfectamente para todos los casos. Cada organización tiene que escoger de entre una amplia variedad la aproximación para la gestión y control de sus sistemas de información dependiendo de su naturaleza, madurez, sector y ámbito de actuación y siempre con la idea de alinear las tecnologías de la información con sus procesos de negocio.

Algunas empresas prefieren centrarse en un único marco de trabajo para la auditoría, mientras que otras consideran que para cada área un conjunto de protocolos u otros son los más indicados.

En el presente capítulo se presentan algunas de las metodologías de trabajo que influyen en la auditoría informática, junto con las organizaciones de origen.

Methodology/Framework	Source	Type	Focus
Generally Accepted Auditing Standards (GAAS)	AICPA	Auditing	External audits
International Standards on Auditing (ISA)	IFAC/IAASB	Auditing	External audit
Internal Control—Integrated Framework	COSO	Internal controls	Internal audit
International Professional Practices Framework (IPPF)	IIA	Auditing	Internal audit
ISO 19011	ISO	Auditing	Management systems
ISO/IEC 27007	ISO and IEC	Auditing	ISMS
Control Objectives for Business and Related Information Technology (COBIT)	ISACA	IT governance	Processes controls
Information Technology Infrastructure Library (ITIL)	Cabinet Office (UK)	IT service management	Service controls
ISO/IEC 38500	ISO and IEC	IT governance	Corporate governance
ISO/IEC 20000	ISO and IEC	Service management	Service processes
Federal Information System Controls Audit Manual (FISCAM)	GAO (US)	System auditing	Government organizations
Information System Security Review Methodology (ISSAI 5310)	ISSAI	System auditing	Government organizations
ISO/IEC 27001 and 27002	ISO and IEC	Security controls	ISMS
Special Publication 800-53A	NIST (US)	Security control assessment	Government organizations

Ilustración 2: Metodologías y marcos de trabajo. (Gantz, S., 2013)

4.1. COBIT 5

La auditoría informática juega un papel esencial de apoyo en el gobierno de las TI, ayudando a los equipos directivos de las empresas a asegurar que sus activos tecnológicos, procesos y servicios operan según las previsiones de acuerdo a los objetivos y metas establecidas por la organización. Aunque todas las organizaciones aplican algún método explícito o implícito para el gobierno de sus sistemas de información, no todas eligen adoptar un marco de trabajo formal que les ayude a estructurar y definir una política efectiva de gobierno y gestión de TI.

Control Objectives for Business and Related Information Technology (COBIT) fue originalmente desarrollado por ISACA en 1996 y ha sido ampliado y actualizado varias veces hasta el lanzamiento de la versión 5 en 2012. COBIT 5 tiene una perspectiva integradora ya que combina los principios clave de la versión 4.1 con otros marcos de trabajo específicos de ISACA como VAL IT (centrado en Inversiones de negocio de TI),

Risk IT (centrado en gestión del riesgo), ITAF (IT Assurance Framework) y BMIS (Business Model for Information Security), así como elementos de ITIL y de varias normas ISO.

Este modelo es uno de los más ampliamente utilizados para el gobierno de los sistemas de información, incluyendo la gestión de controles internos usados para satisfacer los requerimientos legales establecidos. Su jerarquía de principios, catalizadores y procesos provee una base sólida para la realización de auditorías informáticas en las organizaciones que lo implementan.

El marco COBIT 5 se construye sobre 5 principios básicos clave para el gobierno y la gestión de las TI empresariales:

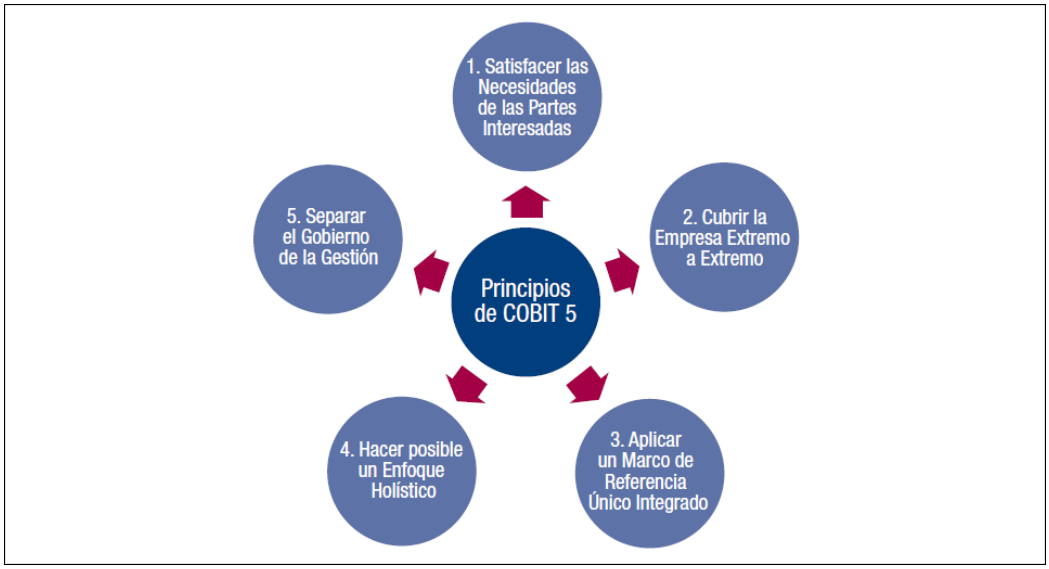

Ilustración 3: Principios de COBIT 5 (COBIT 5, 2012)

1. Satisfacer las necesidades de las partes interesadas

Todas las empresas tienen *stakeholders* (grupos de interés) a los que satisfacer y por tanto las empresas deben crear valor para todos ellos manteniendo un equilibrio entre beneficios, costes, riesgos y recursos. COBIT 5 provee procesos y catalizadores que permiten a las empresas a crear valor de negocio mediante el uso de TI.

2. Cubrir la empresa extremo a extremo

COBIT 5 integra el gobierno y la gestión de TI dentro del gobierno corporativo. La información y las tecnologías relacionadas son tratadas como cualquier otro activo de la empresa, por tanto se definen procesos a nivel de toda la empresa y no solo de la función de TI.

3. Aplica un marco de referencia único integrado

COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes permitiendo que pueda usarse como marco principal para el gobierno y gestión de las TI en la empresa.

4. Hacer posible un enfoque holístico

Para que el gobierno y la gestión de las TI en la empresa sea efectivo y eficiente se requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define siete categorías de catalizadores (*enablers*) que apoyan la implementación de un sistema de gobierno y gestión global para las TI de la empresa.

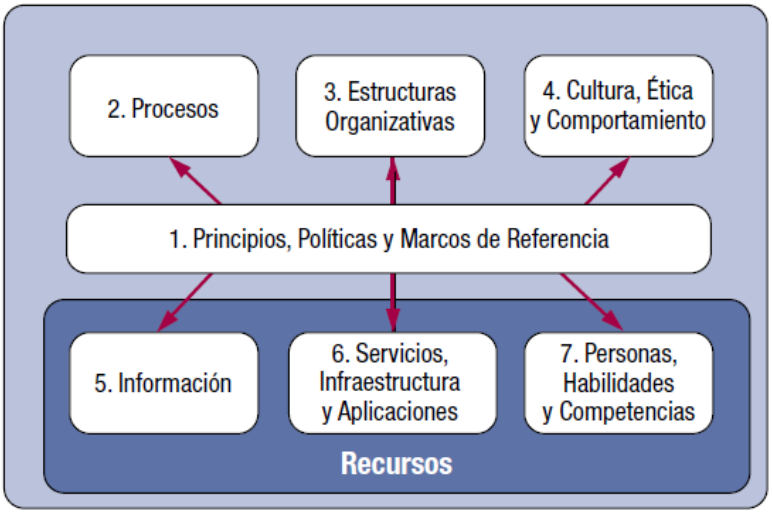

Ilustración 4: Catalizadores en COBIT 5 (COBIT 5, 2012)

5. Separar el gobierno de la gestión

En COBIT 5 se realiza una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren estructuras corporativas diferentes y sirven para diferentes propósitos.

El gobierno es la actividad que desempeña generalmente el consejo de administración de las empresas y que tiene como objetivos establecer los planes operativos de la empresa para que las metas corporativas se alcancen.

La gestión es la actividad encargada de planificar, ejecutar y controlar las actividades que se llevarán a cabo de forma alineada con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. La gestión suele ser responsabilidad de la dirección ejecutiva de la empresa.

COBIT 5 no se ha definido con carácter prescriptivo pero si defiende que las empresas implementen procesos tanto para el gobierno como para la gestión de forma que las áreas fundamentales queden cubiertas. El marco de trabajo propone un modelo de referencia de procesos que define y detalla varios procesos de gobierno y de gestión. En el modelo se encuentran todos los procesos que habitualmente se encuentran presentes en las empresas relacionados con las actividades de TI. Cada empresa puede hacer servir este modelo de procesos y adaptarlo a sus características particulares, implantando aquellos procesos que le resulten convenientes. Obviamente las empresas

grandes requerirán de un mayor número de procesos que las pequeñas y su complejidad también será mayor, pero todas ellas podrán utilizar COBIT 5 como guía.

El modelo de referencia de procesos de COBIT 5 divide los procesos en dos dominios principales:

- Gobierno: Contiene cinco procesos y dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión.
- Gestión: Contiene cuatro dominios en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Run and Monitor - PBRM). Estos dominios son una evolución de la estructura de procesos de COBIT 4.1. Los cuatro dominios son los siguientes:
  - Alinear, Planificar y Organizar (*Align, Plan and Organise, APO*)
  - Construir, Adquirir e Implementar (*Build, Acquire and Implement, BAI*)
  - Entregar, dar Servicio y Soporte (*Deliver, Service and Support, DSS*)
  - Supervisar, Evaluar y Valorar (*Monitor, Evaluate and Assess, MEA*)

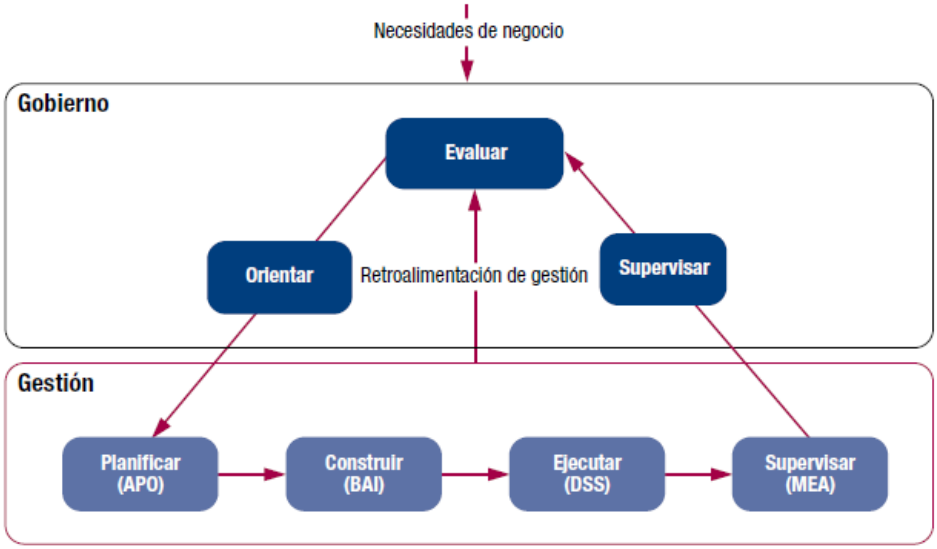

Ilustración 5: Áreas clave de Gobierno y Gestión en COBIT 5 (COBIT 5, 2012)

4.2. ISO 20.000-1:2011

La serie de normas ISO/IEC 20000 - Service Management es la familia de normas publicada por la International Organization for Standarization (ISO) para la gestión del servicio de TI y su primera edición se remonota a diciembre de 2005. La serie proviene del conjunto de normas BS 15000, desarrolladas por la entidad de normalización Británica (British Standards Institution) y se estructura en varias partes. Las principales son las siguientes:

- Parte 1: ISO/IEC 20000-1:2011 - Requisitos de los sistemas de gestión de servicios.
- Parte 2: ISO/IEC 20000-2:2012 - Guía de implementación de los sistemas de gestión de servicios.

- Parte 3: ISO/IEC TR 20000-3:2012 - Guía en la definición del alcance y la aplicabilidad.
- Parte 4: ISO/IEC DTR 20000-4:2010 - Modelo de referencia de procesos.
- Parte 5: ISO/IEC TR 20000-5:2013 – Plan de implementación para la 20000-1.

La parte 1 es la norma de referencia que establece los requisitos que los Sistemas de Gestión de Servicios de TI (SGS) deben alcanzar para lograr su alineación con las necesidades de negocio y con los requisitos de los clientes, asegurando una gestión óptima de los costes y la seguridad en la entrega del servicio.

La ISO 20000-1 se puede implantar en empresas de todo tipo de sector y tamaño, siempre que se realicen y exploten servicios de TI de forma externa o incluso de forma interna. La motivación de una empresa para adoptar las consideraciones de la norma puede venir por el deseo de ofrecer un servicio eficiente, consistente y fiable a la vez que rentable.

Al igual que sucede con otras normas de Gestión de Sistemas (Calidad, Medioambiental o Seguridad de la Información) la implantación de la norma requiere al prestador del servicio la definición y el modelado de sus procesos internos y la adopción de una cultura que promueva la mejora continua en la empresa

Como es habitual en muchas de las normas ISO, se emplaza a la organización a seguir la metodología conocida como Ciclo de Deming o Ciclo PDCA para todas las partes del SGS, así como para los servicios.

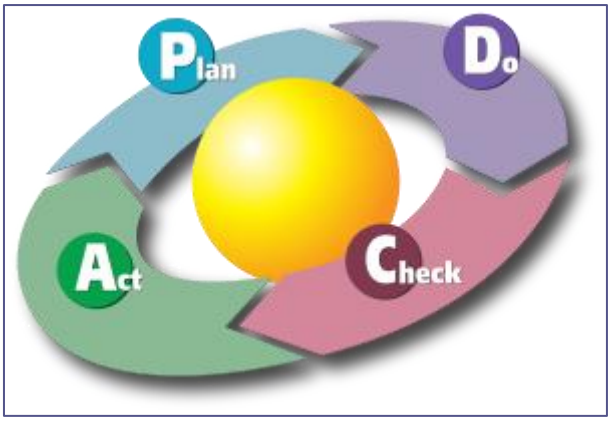

Ilustración 6: Ciclo PDCA

Esta metodología, de forma resumida, se compone de cuatro etapas (PLAN, DO, CHECK, ACT) y su significado es el siguiente:

- Planificar (PLAN): Establecer, documentar y acordar el Sistema de Gestión del Servicio.
- Hacer (DO): Implementar y operar el SGS para los procesos definidos.
- Verificar (CHECK): medir, monitorizar y revisar de forma formalizada el SGS contra las políticas y objetivos determinados por la empresa, así como informar de los resultados obtenidos.
- Actuar (ACT): Tomar las medidas que se estimen oportunas para mejorar de forma continua el comportamiento y la eficacia del SGS.

La ISO 20000-1 es la norma de gestión del servicio de TI que se puede implantar y certificar, por lo que está sujeta también a auditorías de cumplimiento. Se ha considerado que la presente norma debía formar parte del presente trabajo ya que es auditable y un referente a nivel mundial en el área de la gestión de servicios de TI.

Cabe mencionar que la norma ISO 20000-1 está fuertemente alineada con otro de los marcos de trabajo muy populares en el mundo empresarial actual y que es ITIL. Ambas comparten el objetivo principal de implantar un SGS eficaz en la empresa para gestionar la provisión del servicio. La decisión de considerar para el presente trabajo uno respecto al otro se basa en el hecho de que ITIL no es una norma internacional certificable.

4.3. ISO 27:002:2013

La siguiente norma internacional seleccionada es la ISO 27002. Pertenece a la serie de normas ISO 27000, dedicadas a establecer un marco para la gestión de la seguridad de la información en organizaciones de cualquier tamaño y sector. Este conjunto de normativas ha sido desarrollado, a semejanza con la mencionada anteriormente, por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) y la primera versión fue publicada en el año 2005.

Los orígenes de la norma se remontan al año 1995 con la publicación por parte del BSI Británico de su norma Bs 7799 parte 1, que definía un código de buenas prácticas para la gestión de la seguridad de la información. En el año 1999 fue lanzada la segunda parte de la misma norma en la que se definió por primera vez los requisitos para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI, o ISMS en inglés).

La organización ISO adoptó la primera parte de la norma para la publicación de la ISO 17799 en el año 2000. Finalmente, tras sucesivas actualizaciones de las normas por parte de ambas entidades, ISO publicó la ISO 27001 en el año 2005 y poco después se cambió el nombre de la ISO 17799 para pasar a denominarse ISO 27002, con lo que nació la familia de normas dedicadas a la gestión de la seguridad de la información.

Desde entonces, el conjunto de normas de esta serie ha ido ampliándose progresivamente para cubrir los numerosos ámbitos de aplicación relacionados con la seguridad de la información. La evolución vertiginosa de las tecnologías de la información y la aparición de nuevos ámbitos donde la seguridad es un reto para las organizaciones ha motivado que esta sea una amplia familia normativa que debe ser continuamente revisada y a la que se incorporen nuevos miembros regularmente. A continuación se presentan algunas de las principales normas de la serie, sin pretender hacer un análisis extensivo de las mismas:

NORMA*	DESCRIPCIÓN
UNE-ISO 27000:2014	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.

NORMA*	DESCRIPCIÓN
UNE-ISO 27001:2014	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos.
UNE-ISO 27002:2009	Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información. Existe una versión más reciente publicada en 2013 que todavía no ha sido publicada en Español
ISO 27003:2010	Tecnología de la Información. Técnicas de seguridad. Guía de implementación para los sistemas de gestión de la seguridad de la información
ISO 27004:2009	Tecnología de la Información. Técnicas de seguridad. Guía para la medición de los sistemas de gestión de la seguridad de la información.
ISO 27005:2011	Tecnología de la Información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información.
ISO 27006:2011	Tecnología de la Información. Técnicas de seguridad. Requerimientos para entidades proveedoras de auditorías y la certificación de los sistemas de gestión de la seguridad de la información.
ISO 27007:2011	Tecnología de la Información. Técnicas de seguridad. Buenas prácticas para la auditoría de los sistemas de gestión de la seguridad de la información.
ISO 27013:2012	Tecnología de la Información. Técnicas de seguridad. Guía para la implementación integrada de las normas ISO 27001 e ISO 20000-1.

* Las versiones con el epígrafe UNE corresponden con las publicadas en España por AENOR. El resto no ha sido publicado en español. Fuentes (www.aenor.es, www.iso.org)

Adicionalmente, tanto ISO como IEC trabajan en la actualidad en el desarrollo de nuevas normativas dentro del área de la seguridad de la información para alinearse con las últimas tendencias tecnológicas existentes. Así, se están preparando textos que cubran áreas tan importantes hoy en día como los sistemas en la nube (27017), detección de intrusos y sistemas de protección (27039), seguridad en el almacenamiento digital (27040) o análisis e interpretación de evidencias digitales (27042).

Toda la familia normativa se apoya en dos de ellas como referencias principales, y son la ISO 27001 y la 27002. La primera corresponde con la norma que se implanta en las organizaciones y la que está sujeta a auditorías de cara a obtener y mantener la correspondiente certificación. En ella se definen los requisitos necesarios para implantar en cualquier organización un sistema de gestión de la seguridad de la información que ayude a preservar la confidencialidad, integridad y disponibilidad de

la información. La norma establece que las organizaciones deben definir unos objetivos de seguridad alineados con la estrategia corporativa y se debe llevar a cabo un proceso de apreciación y tratamiento de los riesgos.

Adicionalmente, la norma ISO 27002 establece un conjunto de controles de seguridad de la información que sirven como guía para la mitigación de los riesgos apreciados durante el análisis de riesgos. Así, en la última versión de la norma publicada en 2013 se definen un total de 114 controles agrupados en 14 bloques.

Para el presente trabajo se ha escogido la norma ISO 27002:2013 como norma, dado que dispone de controles mapeables.

4.4. PMBOK 5

PMBOK es una Guía de los Fundamentos para la Dirección de Proyectos y proporciona una completa colección de pautas o buenas prácticas para la dirección de proyectos. Este marco de trabajo es publicado y mantenido por el Project Management Institute (PMI). La primera versión fue publicada en el año 1996 y desde entonces, el estándar ha ido evolucionando hasta alcanzar la quinta edición en 2013.

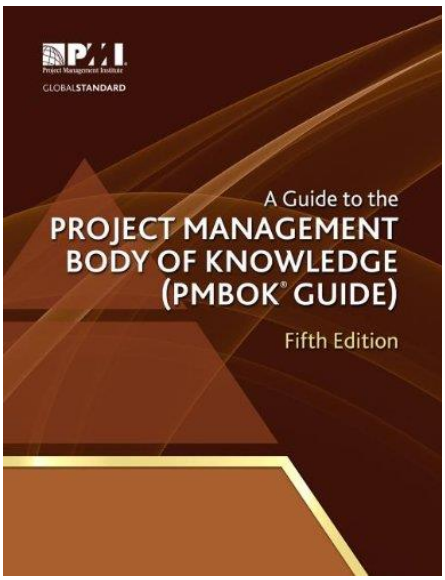

Ilustración 6: PMBOK5

Este documento contiene el estándar, reconocido internacionalmente por entidades como ANSI (www.ansi.org) o el IEEE (www.ieee.org), y en él se describen las normas, métodos, procesos y prácticas para ejercer la profesión de director de proyectos en organizaciones. Así pues, el PMI dispone de diversas certificaciones profesionales mundialmente reconocidas entre la que destaca PMP (Project Management Professional).

Según define PMI en la quinta edición de PMBOK, un proyecto se define como "un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único". Para un proyecto se deben definir unos objetivos a alcanzar dentro de un plazo

acotado temporalmente. En el ámbito de las tecnologías de la información, se utiliza el término de proyecto para gestionar, a modo de ejemplos, la implantación de normas o la auditoría de sistemas de información.

Cabe destacar que dentro de la nomenclatura utilizada por PMBOK se hace referencia a portafolios, programas y proyectos. Entender estos conceptos es importante para trabajar siguiendo las buenas prácticas definidas por el marco de trabajo. La imagen posterior trata de ilustrar estos conceptos:

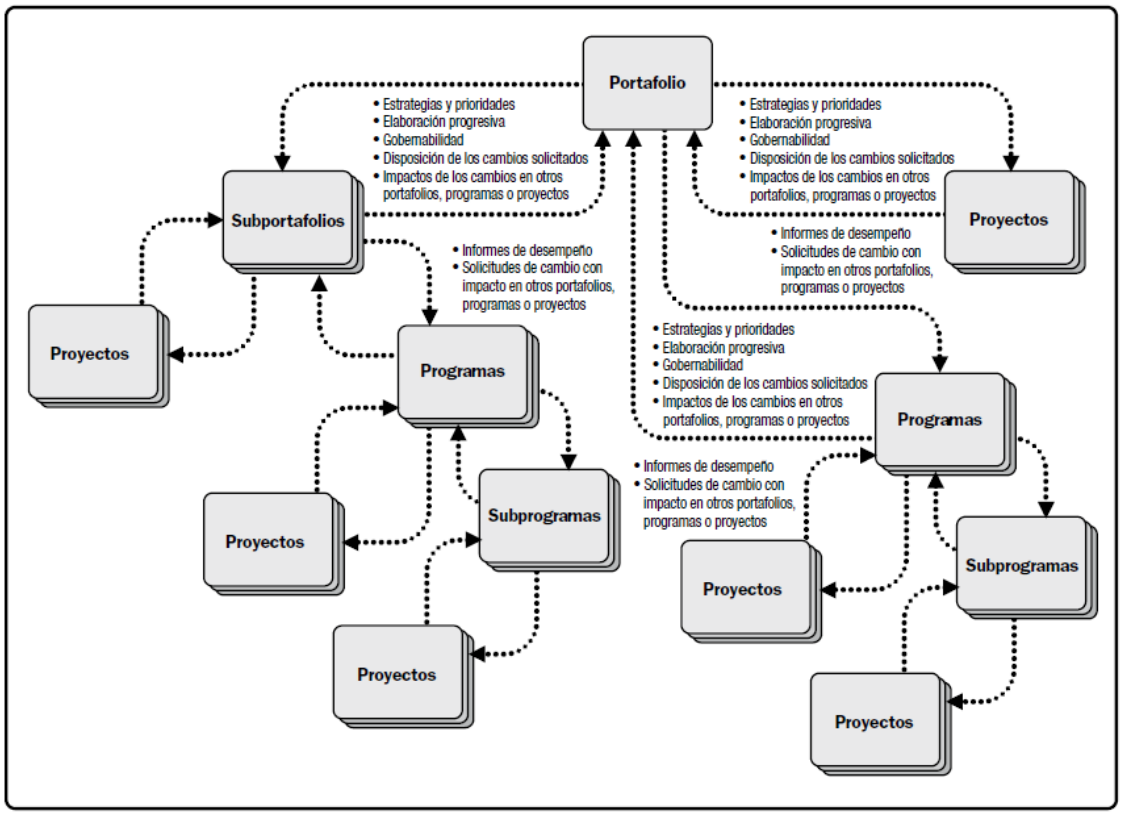

Ilustración 7: Portafolios, programas y proyectos según PMBOK (PMBOK5)

A grandes rasgos, un portafolio lo forman un conjunto de proyectos o programas que se gestionan en forma de grupo para alcanzar determinados objetivos estratégicos. Por el contrario, un programa se puede entender como una línea de trabajos dentro del ámbito de un portafolio y un proyecto es una unidad individual dentro de un programa o portafolio.

Así pues, la guía del PMBOK constituye el estándar para dirigir todo tipo de proyectos mediante la aplicación de un conjunto de buenas prácticas organizadas en diez áreas de conocimiento y cinco grupos de procesos. Dentro de cada área de conocimiento se definen hasta un total de 47 procesos.

Puesto que en el presente trabajo estamos tratando de establecer un marco de trabajo para la realización de auditorías integradas a sistemas de información, se ha considerado la necesidad de incluir los controles (o procesos) definidos en PMBOK para dotar a la herramienta de un componente enfocado a proyecto. Dada la magnitud que puede tener la aplicación de la herramienta, es necesario que la metodología utilizada esté alineada con las mejores prácticas en la gestión de proyectos.

4.5. CMMI-DEV 1.3

El modelo de integración de madurez de capacidades, más conocido por sus siglas en inglés CMMI (Capability maturity model integration) es un conjunto de buenas prácticas cuyo objetivo es ayudar a las organizaciones a mejorar sus procesos. El marco de trabajo es mantenido y publicado por el Software Engineering Institute (SEI) a través de equipos de trabajo provenientes de gobiernos y organizaciones privadas.

El modelo más conocido es el CMMI-DEV, aunque no se trata del único modelo publicado ya que también existen otros marcos de trabajos como CMMI para la adquisición y CMMI para los servicios. La evolución de las publicaciones, con sus diferentes versiones se muestra en la gráfica siguiente:

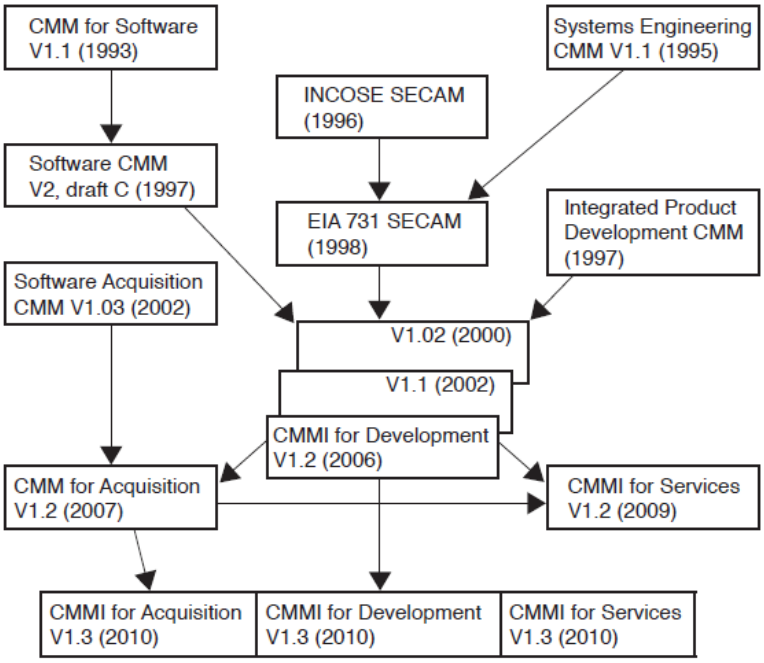

Ilustración 8: Historia de los CMM. (CMMI-DEV V1.3)

Sin duda, el modelo más conocido es el CMMI-DEV, cuyo propósito general es "proporcionar un conjunto completo e integrado de guías para desarrollar productos y servicios" según se indica en el propio documento oficial publicado. Según datos del SEI de septiembre de 2011, España es el país europeo con más empresas evaluadas según CMMI y en cuarta posición mundial, únicamente por detrás de China, Estados Unidos e India.

La motivación existente tras la publicación de este marco de trabajo es dar un enfoque sistemático ante los problemas a los que se enfrentan las empresas que desarrollan productos o servicios de TI. Según el propio modelo expone, otros marcos de trabajo cubren únicamente algunas partes específicas de las actividades de gestión de TI y dejan algunos huecos sin tratamiento, huecos que pretenden cubrir mediante buenas prácticas que tratan las actividades de desarrollo aplicadas a productos y servicios.

CMMI tiene un fuerte enfoque en los procesos y en la mejora de los mismos, y fruto de ello han definido tres dimensiones consideradas como críticas. Estas corresponden con las personas, los procesos y el equipamiento. De forma gráfica, estas tres dimensiones se representan de la siguiente manera:

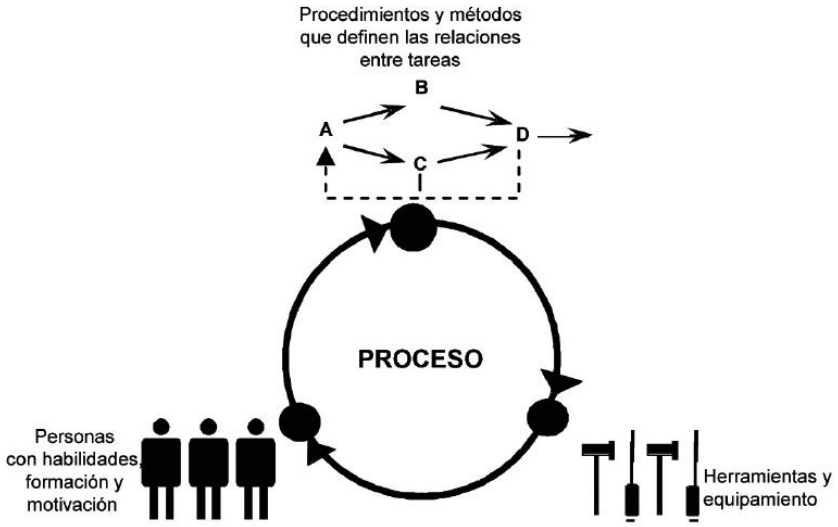

Ilustración 9: Las tres dimensiones críticas de CMMI. (CMMI-DEV V1.3)

El modelo CMM se centra en mejorar los procesos y para ello se definen los elementos considerados esenciales para mejorar la eficacia, así como un camino evolutivo que la entidad puede seguir para mejorar y alcanzar un alto grado de madurez en sus actividades, lo que le proporcionará calidad y eficacia mejorada. Entre las prácticas incluidas en el modelo, se incluyen consideraciones acerca de la gestión de proyectos, gestión de procesos, ingeniería de sistemas, hardware o software, así como otros procesos de soporte.

La arquitectura del modelo está basada en la definición de áreas de proceso. En total existen 22 áreas de proceso y para cada una de las cuales se incluyen prácticas, que pueden ser genéricas o específicas. Las prácticas genéricas se encuentran en todas las áreas de proceso, mientras que las específicas como su nombre indica solo se definen para un área concreta.

Para la evaluación de una organización contra el presente modelo se definen varias etapas o niveles, organizadas en dos grupos. Mientras los niveles de capacidad se refieren a la consecución de la mejora de los procesos en áreas de proceso individuales, los niveles de madurez son un medio para mejorar los procesos mediante la implantación de un conjunto de áreas de proceso. En la gráfica posterior se muestran los 4 niveles de capacidad y los 5 niveles de madurez.

Nivel	*Representación continua* *Niveles de capacidad*	*Representación por etapas* *Niveles de madurez*
Nivel 0	Incompleto	
Nivel 1	Realizado	Inicial
Nivel 2	Gestionado	Gestionado
Nivel 3	Definido	Definido
Nivel 4		Gestionado cuantitativamente
Nivel 5		En optimización

Ilustración 10: Niveles de madurez. (CMMI-DEV V1.3)

El nivel de madurez es lo que comúnmente se utiliza para medir el grado de implantación del modelo en una organización y por tanto está sujeto a auditorías. Un nivel de madurez se alcanza cuando se demuestra cumplimiento satisfactorio en un grupo de áreas de proceso determinado. Las reglas siguientes son, de modo resumido, las que determinan el nivel de una organización según el modelo CMMI-DEV V1.3:

- Para lograr el nivel de madurez 2, todas las áreas de proceso asignadas al nivel de madurez 2 deben lograr el nivel de capacidad 2 o 3.
- Para lograr el nivel de madurez 3, todas las áreas de proceso asignadas a los niveles de madurez 2 y 3 deben lograr el nivel de capacidad 3.
- Para lograr el nivel de madurez 4, todas las áreas de proceso asignadas a los niveles de madurez 2, 3 y 4 deben lograr el nivel de capacidad 3.
- Para lograr el nivel de madurez 5, todas las áreas de proceso deben lograr el nivel de capacidad 3.

Dado que este marco es ampliamente conocido en el sector de las tecnologías de la información y que, de algún modo se complementa con los demás presentados anteriormente, se ha considerado su inclusión en el presente trabajo.

5. Mapeo de controles

5.1. Referencias anteriores

Una de las principales motivaciones que han habilitado la consecución del presente trabajo, imponiéndose esta idea sobre otras igualmente válidas, ha sido el no encontrar publicaciones o estudios especializados que aborden el mapeo de controles entre los referentes normativos en materia tecnológica.

Obviamente, la idea subyacente al presente trabajo y la problemática de la realización de auditorías integradas no es propia, por lo que existen publicaciones anteriores que tratan el tema. No obstante, estas publicaciones se encuentran desfasadas, haciendo referencia a versiones antiguas de los marcos de trabajo o normativas por lo que no resultan válidas en la actualidad como metodología de trabajo, siendo necesaria su actualización.

Este trabajo pretende cubrir, desde la humildad del autor, el vacío motivado por las sucesivas actualizaciones de las normas de referencia, pero antes de presentar el trabajo realizado se estima conveniente hacer referencia los trabajos previos que se encuentran a disposición de todo aquel que lo necesite.

La organización ISACA dispone dentro de su amplio catálogo de publicaciones de varios libros dedicados al mapeo de COBIT, su marco de trabajo para el gobierno y la gestión de TI, con respecto a otros estándares y normas internacionales. Estas publicaciones están disponibles a través del *knowledge Center* de su página web (www.isaca.org). Varios de estos trabajos previos han servido como base documental y como inspiración para el desarrollo del presente Trabajo Final de Grado.

El primero de ellos es el libro titulado “Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit”, publicado en el año 2008 por el IT Government Institute. Este instituto fue impulsado en 1998 por ISACA y su principal objetivo es ayudar a las organizaciones a generar valor a través de una gestión y de un gobierno eficaz de los sistemas de información.

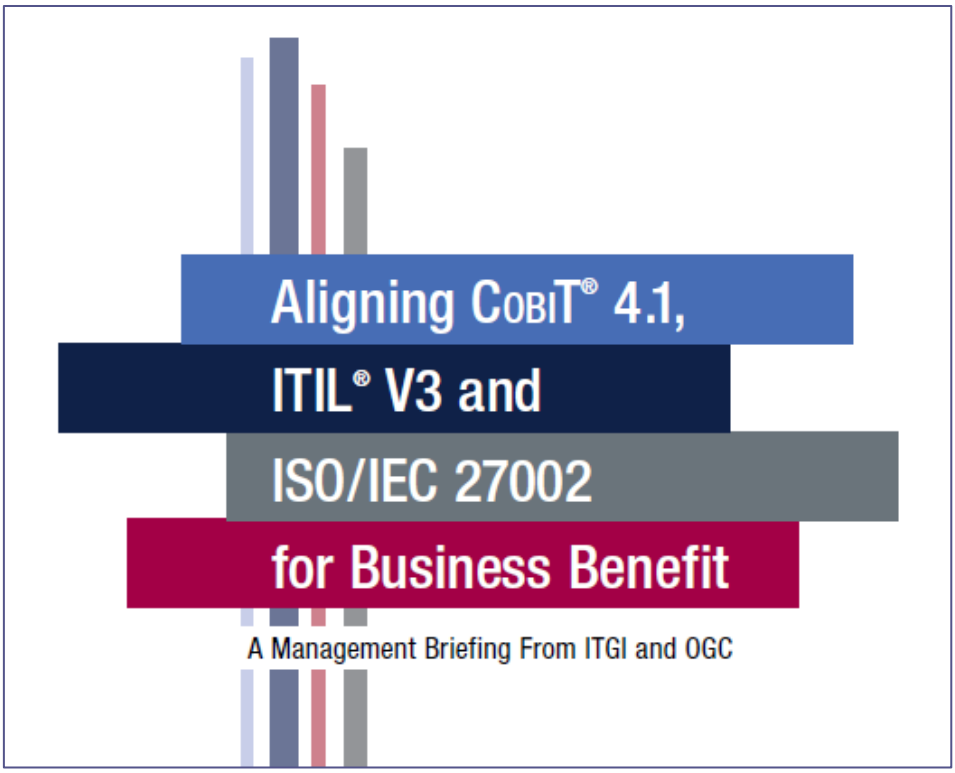

Ilustración 11: Mapeo previo de COBIT5

El objetivo perseguido por la publicación es alinear las mejores prácticas contenidas tanto en COBIT 4.1, la versión antecesora a la actual, con ITIL v3 y la ISO 27002:2005 que como ya se ha comentado en secciones previas ha sido desplazada por la versión del 2013.

El mapeo de controles que propone el libro está enfocado a alto nivel, sin entrar en detalles de la exactitud de la correspondencia y puede constituir una herramienta útil no para la realización de una auditoría sino más bien para la implantación conjunta de las normas.

En este caso, la única distinción que se realiza para diferenciar el tipo de mapeo se basa en dos casos:

a. Para cada control, si el texto se muestra en negrita se debe entender que ese marco provee la cobertura más amplia para el área de control. A continuación se muestra un ejemplo:

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO8 Manage Quality *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO8.3 Development and acquisition standards	• Life cycle standards for deliverables	• *SS 6.5 Sourcing strategy* • *SD 3.5 Design activities* • *SD 3.6 Design aspects* • *SD 3.9 Service-oriented architecture* • *SD 3.11 Service design models* • *SD 5.3 Application management* • *SD 7 Technology considerations* • *ST 3.2.3 Adopt a common framework and standards* • *ST 4.1.4 Policies, principles and basic concepts* • *ST 4.1.5.1 Transition strategy*	• **6.1.5 Confidentiality agreements** • **6.2.3 Addressing security in third-party agreements** • **12.5.5 Outsourced software development**

Ilustración 12: Ejemplo de mapeo cobertura amplia.

b. Para cada control, si el texto se muestra en cursiva se debe entender que proporciona alguna cobertura, sin llegar a ser extensiva. Se reproduce un ejemplo a continuación:

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO2 Define the Information Architecture *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO2.2 Enterprise data dictionary and data syntax rules	• Corporate data dictionary • Common data understanding	• *SD 5.2 Data and information management* • *SD 7 Technology considerations*	• *7.1.1.1 Inventory of assets* • *11.1.1 Access control policy*
PO2.3 Data classification scheme	• Information classes • Ownership • Retention • Access rules • Security levels for each information class	• *SD 5.2 Data and information management*	• *7.2.1 Classification guidelines* • *10.7.1 Management of removable data* • *10.8.1 Information exchange policies and procedures* • *10.8.2 Exchange agreements* • *11.1.1 Access control policy*

Ilustración 13: Ejemplo de mapeo cobertura menor.

Cabe mencionar que se ha mapeado toda buena práctica o control que hace alguna referencia, por leve que esta sea. Esta estrategia es útil dependiendo de los resultados que se pretendan alcanzar. Para el caso concreto de una auditoría de sistemas de información, la inclusión de tantas referencias resultaría en una herramienta de trabajo demasiado compleja y costosa de revisar, por lo que no resulta un mapeo eficaz para el propósito perseguido en el presente trabajo, más aún cuando las versiones de COBIT y de ISO 27002 no son las actualmente vigentes.

La segunda de las publicaciones es el libro análogo al anterior titulado “COBIT® Mapping: Mapping of ISO/IEC 20000 With COBIT® 4.1” y publicado en el año 2011 por ISACA. El libro propone un mapeo de controles entre COBIT 4.1 y la versión de 2005 de la norma ISO 20.000. Desgraciadamente para ISACA y para los muchos contribuyentes que colaboraron en su redacción, la norma ISO 20000 fue revisada y actualizada en el mismo año de publicación del libro, por lo que su periodo de vigencia se vio reducido a unos pocos meses.

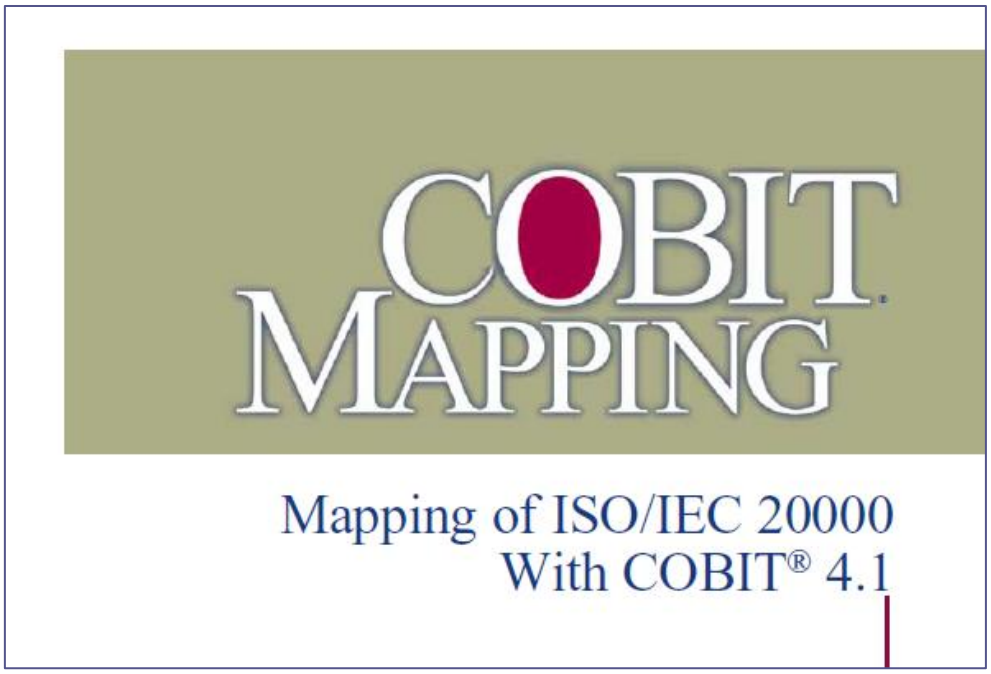

Ilustración 14: Mapeo previo COBIT-ISO2000

En este caso el mapeo se presenta en dos niveles. El primero de ellos es una correspondencia a alto nivel, comparando los objetivos que se desprenden de la ISO 20000 con los controles de COBIT y el segundo es un mapeo mucho más detallado.

A modo de resumen, en el libro se presenta el gráfico posterior en el que se puede observar el grado de intensidad de las correspondencias entre las normas.

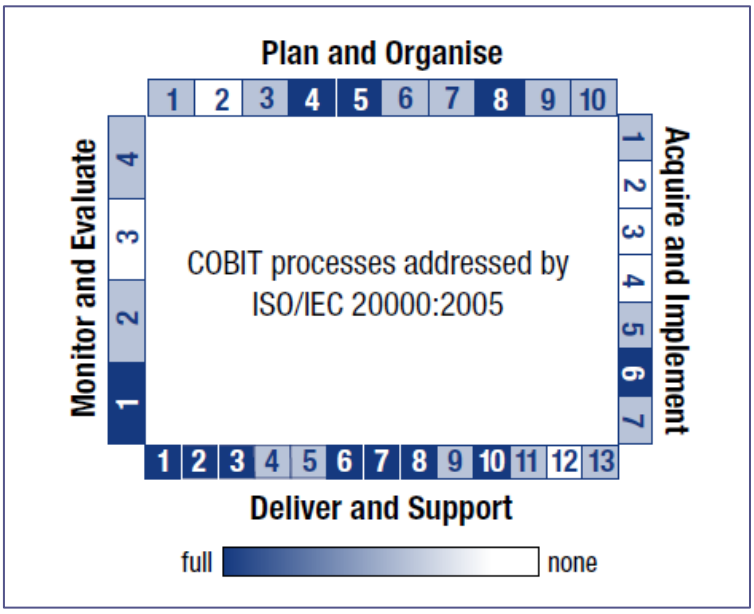

Ilustración 15: Intensidad del mapeo COBIT-ISO20000

Posteriormente, para el mapeo detallado se utiliza una escala que se ha considerado óptima, por lo que se ha adaptado para el desarrollo del presente trabajo, tal y como se detalla en el apartado 5.3 de este documento. En este caso distinguen 3 niveles de

mapeo que se corresponden con las siglas E (Exceed), A (Addressed) y C (Covered). Posteriormente se explicará con más detalle el significado de los términos.

El resultado del mapeo que se presenta en el libro es una completa tabla con todos los puntos de la norma y sus correspondencias con COBIT. Esta herramienta propuesta sí que resultaría válida para la realización de una auditoría de sistemas de información, salvando el hecho de que las dos normas referidas han evolucionado a versiones más actuales.

Seguidamente, la tercera de las publicaciones de referencia para el presente trabajo corresponde con el libro titulado "COBIT® Mapping: Mapping of CMMI® for Development, V1.2, With COBIT® 4.1" publicado en 2011 por ISACA. Este libro, al igual que el anterior, pertenece a una serie de publicaciones con mapeos de COBIT con algunos marcos de trabajo relevantes. En este caso concreto, se mapea COBIT 4.1 con CMMI para el desarrollo en su versión 1.2.

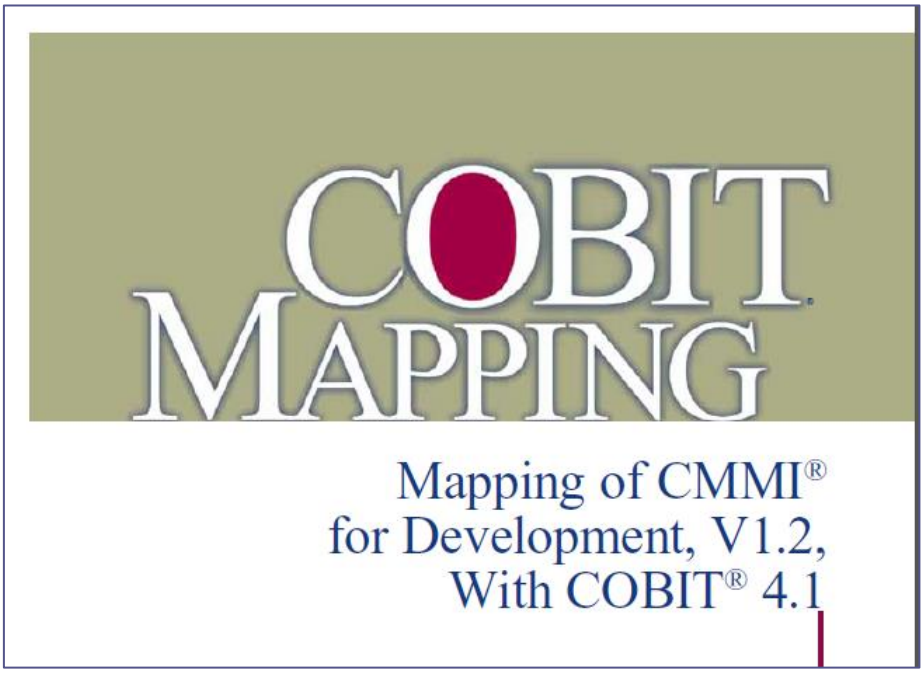

Ilustración 16: Mapeo previo COBIT-CMMI

De forma similar a la descrita para el caso anterior, en este caso también se presenta un mapeo a alto nivel de ambos marcos de trabajo para posteriormente desarrollar un mapeo detallado de controles.

La metodología utilizada para el mapeo es la misma que se presentó en el caso anterior, y que como ya se ha comentado, se utilizará para el desarrollo de los mapeos contenidos en este estudio.

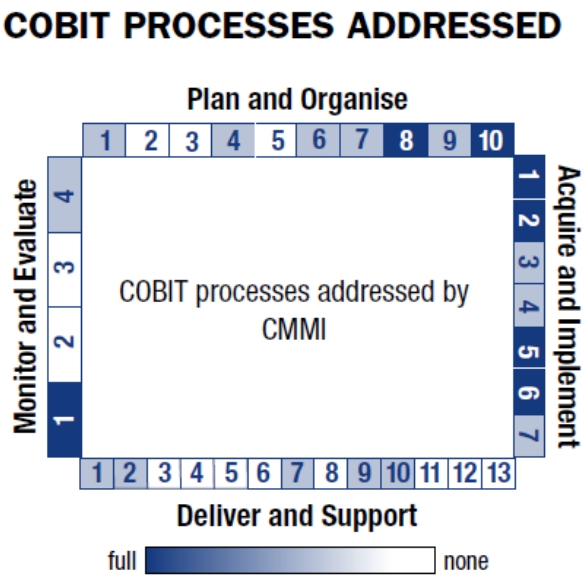

Ilustración 17: Intensidad del mapeo COBIT-CMMI

Por tanto, estamos ante otro caso en el que la herramienta propuesta cumple con los requisitos para poder ser utilizado en el transcurso de una auditoría de sistemas de información, si no fuera por el hecho de que ambos marcos de trabajo utilizados no corresponden con las versiones actuales.

El último caso es el del libro titulado "COBIT MAPPING: MAPPING OF PMBOK WITH COBIT 4.0" y su fecha de publicación fue en el año 2006 dentro de la misma línea de publicaciones mostradas anteriormente.

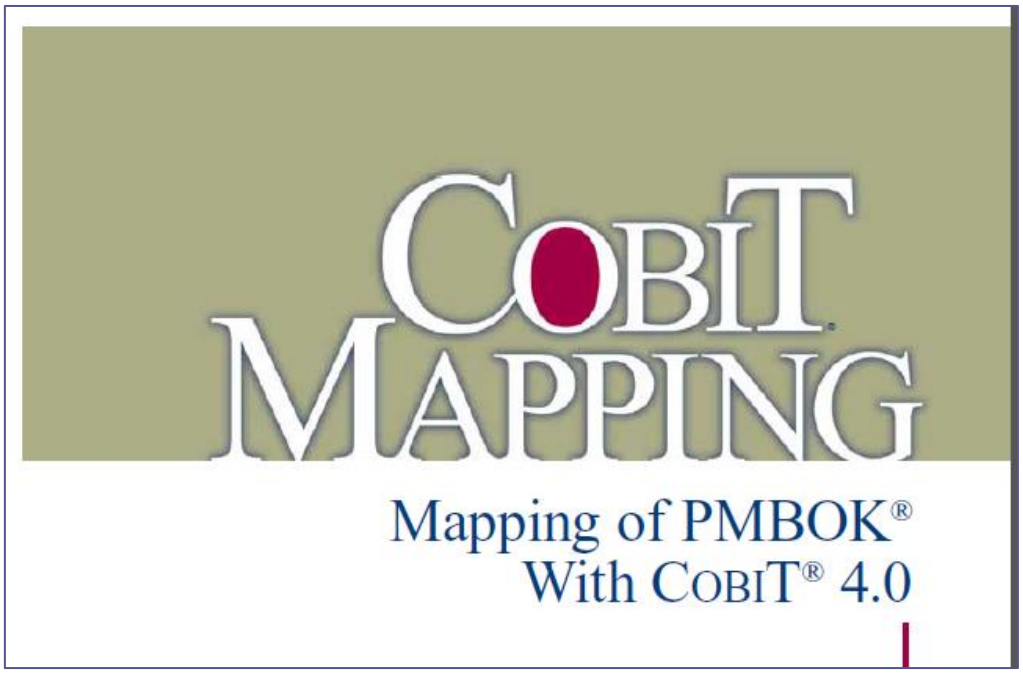

Ilustración 18: Mapeo previo COBIT-PMBOK

Igualmente, se presenta un mapeo a alto nivel y otro detallado, siguiendo para el segundo caso la misma metodología presentada previamente. En este caso, al ser más antigua la publicación se observa como las versiones de los marcos de trabajo no son los antecesores de los actuales (en el caso de COBIT) sino una versión incluso anterior por lo que su uso en la actualidad presenta demasiadas limitaciones.

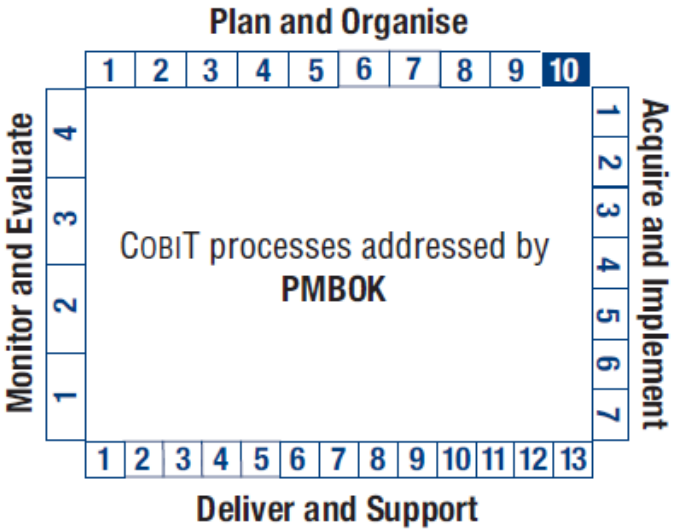

Ilustración 18: Intensidad del mapeo COBIT-PMBOK

Adicionalmente, desde ISACA se ha completado la serie de publicaciones mencionada en este apartado con otras no menos interesantes, pero que quedan fuera del alcance al no referirse a normas incluidas en el mapeo, pero que perfectamente podrían incorporarse en trabajos futuros o actualizaciones. La lista completa de publicaciones es la siguiente:

- COBIT® Mapping: Mapping of FFIEC Framework With COBIT® 4.1
- COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT® 4.0, 2nd Edition
- COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0
- COBIT® Mapping: Mapping of ISO/IEC 20000:2005 With COBIT® 4.1
- COBIT® Mapping: Mapping of ITIL V3 With COBIT® 4.1
- COBIT® Mapping: Mapping of NIST SP 800-53 With COBIT® 4.1
- COBIT® Mapping: Mapping of PMBOK® With COBIT® 4.0
- COBIT® Mapping: Mapping of SEI's CMM® for Software With COBIT® 4.0
- COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0

5.2. Selección de controles

En secciones anteriores ya se han presentado las normas y marcos de trabajo con los que se trabajará en el desarrollo del TFG. Los documentos que describen las normativas y los *frameworks* son heterogéneos entre ellos, ya que están desarrollados por entidades distintas y para finalidades igualmente diferentes, aunque en cierta parte solapadas. Esta diferenciación se hace evidente al estudiar los textos publicado para los diferentes casos.

En esta línea es fácil observar como en las normas publicadas por ISO/IEC los textos son más bien breves, presentándose al lector únicamente los conceptos principales o los controles pero sin entrar en detalles de implementación o de buenas prácticas relacionadas. Por el contrario, se evidencia que en los marcos de trabajos publicados por entidades o asociaciones de carácter privado, los textos son mucho más detallados y extensos, proporcionando mucha más información al lector. Este hecho provoca que el trabajo de alinear los controles de las diferentes normativas sea complejo y deba tratar de delimitarse que se va a mapear y hasta que nivel de cada una de las normas se va a llegar.

A continuación se detalla, para cada uno de los marcos propuestos la selección de controles y el nivel de detalle que se ha escogido, atendiendo siempre a criterios de homogeneidad y de granularidad. Como ejemplo, se puede decir que se ha tratado de evitar mapear controles específicos de una norma con apartados generales de otra, ya que no produciría resultados válidos según los objetivos definidos.

COBIT5 se ha definido con una arquitectura multinivel dado que pretende cubrir gran cantidad de áreas relacionadas con las tecnologías de la información. Concretamente, la estructura de COBIT5 se basa en los siguientes niveles, relacionados en orden de magnitud, es decir, de mayor a menor nivel:

- Área: Es el concepto de mayor nivel que proporciona COBIT5. Se definen dos áreas que son la Gestión y Gobierno. Dentro de las áreas se encuadran los dominios. La imagen posterior capturada del libro “COBIT5-Enabling Processes” ilustra el concepto de área.

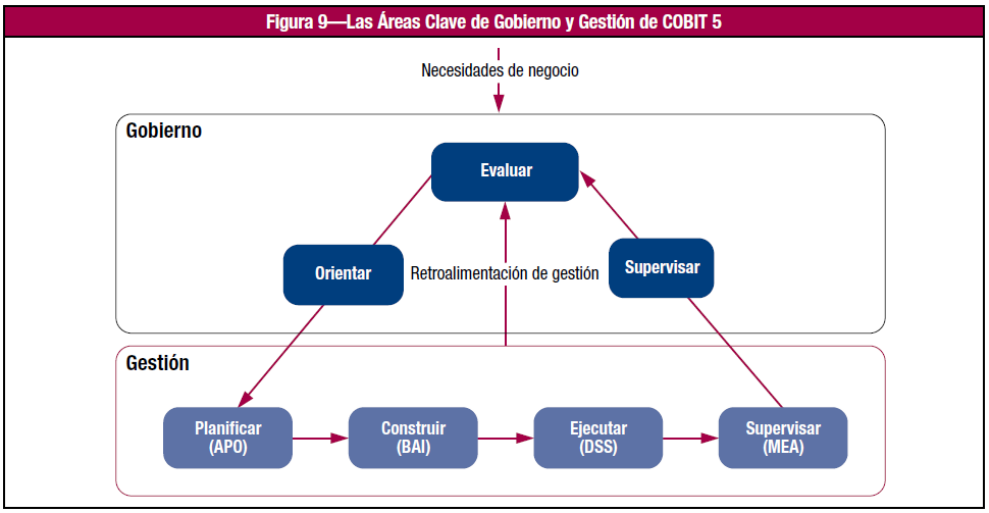

Ilustración 19: Áreas definidas en COBIT5

- Dominio: Corresponde con el segundo nivel. En COBIT5 se amplía el número de dominios respecto a su precedente y se definen 5 dominios. Los dominios se identifican por sus siglas EDM (Evaluar, Orientar y Supervisar), APO (Alinear, Planificar y Organizar), BAI (Construir, Adquirir e Implementar), DSS (Entregar, Dar Servicio y Soporte) y MEA (Supervisar, Evaluar y Valorar).
- Proceso: Dentro de cada dominio se identifican un número variable de procesos que comprenden el ciclo de vida completo del proceso particular. En total se definen hasta 37 procesos.
- Práctica: Igualmente, el nivel inferior corresponde con las buenas prácticas. En COBIT5 existen un total de 202 prácticas. Estas prácticas son los objetivos de control de COBIT, por lo que es el nivel de granularidad idóneo para ser mapeado. Para el desarrollo del mapeo detallado se han considerado todas las prácticas definidas en COBIT5.
- Actividad: Adicionalmente, existe un nivel de granularidad más fino y que corresponde con las actividades. Dentro de cada práctica se detallan un número variable de actividades que permiten al auditor o implantador identificar tareas concretas para cumplir con las prácticas. La captura posterior se muestra una práctica con sus actividades relacionadas, a modo de ejemplo, para ilustrar la estructura de práctica/actividades que incluye COBIT5.

EDM03 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gobierno	**Entradas**		**Salidas**	
EDM03.01 Evaluar la gestión de riesgos. Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.	**De**	**Descripción**	**Descripción**	**A**
	APO12.01	Factores y problemas de riesgos emergentes	Guías de apetito de riesgo	APO12.03
			Niveles de tolerancia de riesgo aprobados	APO12.03
	Fuera del Ámbito de COBIT	Principios de la gestión de riesgos de la empresa	Evaluación de las actividades de gestión de riesgo	APO12.01
Actividades				
1. Determinar el nivel de riesgos relacionados con las TI que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo).				
2. Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.				
3. Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.				
4. Evaluar proactivamente los factores de riesgo TI con anterioridad a las decisiones estratégicas de la empresa pendientes y asegurar que las decisiones de la empresa se toman conscientes de los riesgos.				
5. Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.				
6. Evaluar las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las perdidas relacionadas con TI y la tolerancia de los líderes a los mismos.				

Ilustración 20: Práctica EDM03.01 (COBIT5)

Para la selección de controles de la norma ISO 20000-1:2011 se han escogido los 13 procesos de control que deben aplicarse a los servicios de TI que se prestan. La relación de los 13 procesos se muestra a continuación:

Procesos ISO 20000 de Provisión del Servicio

- Gestión de Nivel de Servicio
- Generación de Informes del Servicio
- Gestión de la Continuidad y Disponibilidad del Servicio
- Elaboración de Presupuesto y Contabilidad de los Servicios
- Gestión de la Capacidad
- Gestión de la Seguridad de la Información

Procesos ISO 20000 de Relación

- Gestión de las Relaciones con el Negocio
- Gestión de Suministradores

Procesos ISO 20000 de Resolución

- Gestión de Incidencias y peticiones de servicio
- Gestión de Problemas

Procesos ISO 20000 de Control

- Gestión de la Configuración
- Gestión de Cambios
- Gestión de la entrega y despliegue

Respecto a la norma ISO 27002:2013 se han escogido los 114 controles incluidos en la norma. El motivo de elegir la ISO 27002 sobre la ISO 27001 es precisamente que incluye los controles que las empresas deben considerar para mitigar los riesgos que se detecten mediante el proceso de apreciación y tratamiento de riesgos.

La arquitectura de CMMI-DEV 1.3 permite múltiples opciones a la hora de escoger que controles o prácticas se desean mapear. En función del nivel de madurez que se pretenda alcanzar, será obligatoria la implantación de un grupo de áreas de proceso. Los paquetes de áreas de proceso se acumulan por lo que si se pretende lograr un nivel de madurez 3, se deberán implantar las correspondientes al nivel 3 y a los inferiores.

Para el desarrollo del presente trabajo se ha considerado adecuado mapear las áreas de trabajo correspondientes al nivel 3 de madurez ya que es probablemente el nivel al que la mayoría de empresas optan. En posteriores evoluciones del mapeo se planteará ampliar la herramienta con las cuatro áreas de proceso que se incluyen en los niveles 4 y 5.

Adicionalmente, dentro de cada área de proceso se definen metas genéricas (GG), que son comunes a todas las áreas de proceso y específicas (SG) que como su nombre indica, son exclusivas para cada área de proceso. Asimismo, dentro de cada una de las metas se incluyen una serie de prácticas (genéricas y específicas según el caso), y que corresponde con actividades o controles que se deberán tomar en consideración si se desea alcanzar el cumplimiento con un área de proceso.

Javier Garzás en su libro titulado "Guía Práctica de Supervivencia en una Auditoría CMMI" ilustra la estructura de las áreas de proceso de CMMI con el siguiente esquema.

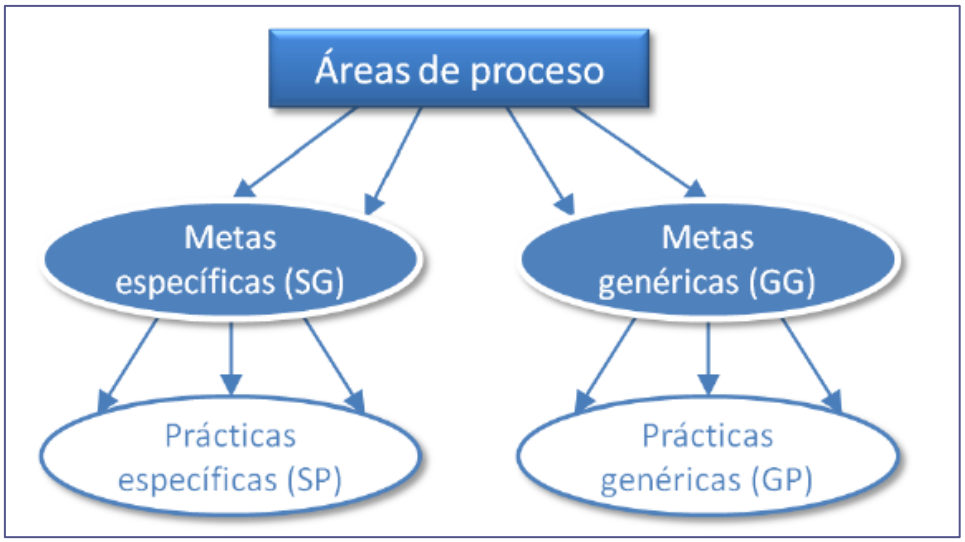

Ilustración 21: Estructura CMMI. (Garzás, Javier, 2011)

Por tanto, el proceso de selección de controles para el mapeo efectivo de CMMI concluye con la elección de todas las prácticas específicas dentro de las áreas de proceso que se deben implantar para alcanzar un nivel de madurez 3. En total se han incluido 18 de las 22 áreas de proceso definidas, que corresponden con las siguientes:

Áreas de proceso para un nivel 2 de madurez.

- Gestión de requerimientos (REQM)
- Planificación de proyecto (PP)

- Monitorización y control del proyecto (PMC)
- Gestión de acuerdos con proveedores (SAM)
- Gestión de configuración (CM)
- Aseguramiento de la calidad de proceso y producto (PPQA)
- Medición y Análisis (MA)

Áreas de proceso para un nivel 3 de madurez.

- Desarrollo de requerimientos (RD)
- Solución técnica (TS)
- Integración de producto (PI)
- Verificación (VER)
- Validación (VAL)
- Definición de procesos de la organización (OPD)
- Enfoque de procesos de la organización (OPF)
- Formación organizativa (OT)
- Gestión integrada de proyecto (IPM)
- Gestión de riesgos (RSKM)
- Análisis de decisiones y resolución (DAR)

Finalmente, PMBOK5 se estructura en torno a 13 áreas de proceso, dentro de las cuales se incluyen un total de 47 prácticas. Para el desarrollo del mapeo se han incluido todas las prácticas definidas. Las 13 áreas de proceso (con su código numérico asignado por el propio PMBOK5) son las siguientes:

- Gestión de la integración del proyecto (4)
- Gestión del alcance del proyecto (5)
- Gestión del tiempo del proyecto (6)
- Gestión de los costes del proyecto (7)
- Gestión de la calidad del proyecto (8)
- Gestión de los recursos humanos del proyecto (9)
- Gestión de los recursos humanos del proyecto (9)
- Gestión de las comunicaciones del proyecto (10)
- Gestión de los riesgos del proyecto (11)
- Gestión de las adquisiciones del proyecto (12)
- Gestión de los interesados del proyecto (13)

5.3. Metodología de mapeo

En esta sección se definirán los criterios generales utilizados para la realización del mapeo de todos los controles seleccionados en el apartado previo. Dada la heterogeneidad de los marcos de trabajo y de las normas incluidas en el trabajo y el alto número de controles presentes en los mismos, es una tarea de vital importancia definir de qué modo se considerará que un control tiene relación con otro.

La importancia de detallar esta metodología radica en que lo que realmente se pretende con el producto que surja de aplicar estos criterios es que sea una herramienta eficiente y eficaz para la realización de auditorías integradas de sistemas de información.

Como ya se ha mencionado anteriormente, la metodología se ha adaptado a partir de la propuesta por ISACA en los libros anteriormente presentados. Tras sopesar varias opciones finalmente se ha optado por definir tres diferentes criterios de mapeo que son los siguientes:

- Parcial (P): El conjunto de actividades comprendidas dentro de la práctica de COBIT5 es más amplia que el/los controles especificados. Significa a efectos de la auditoría que si se ha evidenciado un nivel de cumplimiento satisfactorio con la práctica de COBIT5, se entenderá por cubierto el control en la otra norma de referencia y por consiguiente podría evitarse su reevaluación.

  Cabe destacar que no la relación no es simétrica, por consiguiente no se puede decir lo mismo en sentido contrario. En este caso no se puede considerar cubierta una práctica en COBIT5 si se dispone de evidencia de cumplimiento para un control de las otras normas de referencia.

- Completo (C): El conjunto de actividades comprendidas dentro de la práctica de COBIT5 es semejante y puede considerarse, a efectos de la auditoría, que el cumplimiento se ha logrado para los controles de la norma indicada. El mapeo completo se ha utilizado cuando los controles son muy semejantes, teniendo en cuenta que discernir entre una u otra modalidad no es un proceso matemático y por tanto puede estar sujeto a interpretaciones.

  En este caso si puede entenderse la relación como bidireccional, por lo que si se demuestra el cumplimiento en uno de los lados del mapeo, se podrá entender que el otro lado también está cubierto.

- Excede (E): El conjunto de actividades comprendidas dentro de la práctica de COBIT5 es menos amplia que el conjunto de controles especificados. Esto es, si se ve desde la otra perspectiva, que el conjunto de controles de la norma de referencia tiene un alcance mayor que las actividades definidas por COBIT5.

  En este caso, a efectos de una auditoría no se puede dar por cubierto un control si se ha catalogado el mapeo como “Excede”. En dirección opuesta sí que se puede dar por cubierta una práctica de COBIT5 si se dispone de evidencia de cumplimiento para los controles indicados en el mapeo.

Cabe mencionar aunque resulte evidente que no todos los controles tienen correspondencia por lo que necesariamente existirán controles vacíos en las tablas de mapeo detallado del ANEXO I.

Destacar también que la metodología de mapeo tiene una orientación clara hacia la eficacia de la herramienta de auditoría integrada que se pretende construir, por lo que no se han considerado ligados controles con una conexión remota en cuanto a alcance o conceptos, mostrando en el resultado final únicamente aquellos para los cuales la

correspondencia es concisa. De otra forma la herramienta resultante perdería eficacia y disminuiría su nivel de aplicabilidad.

Con el objetivo de ilustrar la metodología de mapeo mostrada en el presente apartado, se incluyen diversos ejemplos representativos de cada caso, extraídos del mapeo detallado presente en el ANEXO I.

- Mapeo Parcial. El primer ejemplo corresponde con un mapeo parcial. Se puede observar mediante la captura posterior que la práctica o control de COBIT corresponde con el código APO10.03 y trata de la relación con los proveedores y sus contratos. COBIT5 define ocho actividades o buenas prácticas para la implantación del control.

APO10.03 Gestionar contratos y relaciones con proveedores. Formalizar y gestionar las relaciones con cada proveedor. Gestionar, mantener y supervisar los contratos y la entrega de servicios. Asegurar que los nuevos contratos o los cambios son conformes a las normas de la empresa, las leyes y las regulaciones. Gestionar los conflictos contractuales.	**De**	**Descripción**	**Descripción**	**A**
	BAI03.04	Planes de adquisiciones aprobados	Roles y responsabilidades de los proveedores	Interno
			Procesos de revisión y comunicación	Interno
			Resultados y sugerencias de mejora	Interno
Actividades				
1. Asignar propietarios de la relaciones para cada proveedor y hacerles responsables de la calidad del servicio proporcionado.				
2. Especificar un proceso de comunicación formal y de revisión, que incluyan las interacciones con el proveedor y la planificación.				
3. Acordar, gestionar, mantener y renovar los contratos con los proveedores. Asegurar que los contratos son conformes con las normas corporativas y con los requisitos legales y regulatorios.				
4. Incluir en los contratos con los proveedores de servicios clave disposiciones para revisar los lugares de trabajo y las prácticas y controles de la dirección o de terceras partes.				
5. Evaluar la eficiencia de la relación con los proveedores e identificar las mejoras necesarias.				
6. Definir, comunicar y acordar las maneras de implementar las mejoras requeridas en las relaciones.				
7. Hacer uso de los procedimientos establecidos para tratar los conflictos contractuales haciendo uso primero, siempre que sea posible, de relaciones y mecanismos de comunicación eficaces que permitan superar los problemas de servicio.				
8. Definir y formalizar los roles y responsabilidades de cada proveedor. Cuando varios proveedores se combinan para proporcionar un servicio, considerar asignar un rol de proveedor líder a uno de los proveedores para que asuma la responsabilidad global del contrato.				

Ilustración 22: Práctica APO10.03

Seguidamente, observamos el resultado del mapeo. Para este caso el control APO10.03 mapea con controles de todas las normas y marcos de trabajo usados pero para ilustrar el ejemplo únicamente se han incluidos dos casos. Para una relación completa se incita al lector a consultar el mapeo completo en el ANEXO I.

COBIT 5	**CMMI-DEV V1.3**		**PMBOK 5**	
Práctica	**C**	**Control**	**C**	**Control**
APO10.03: Gestionar contratos y relaciones con proveedores.	P	SAM-SP 1.3. Establecer acuerdos con proveedores. SAM-SP 2.2. Aceptar el producto adquirido.	P	12.2 Efectuar las Adquisiciones

En base a los resultados obtenidos en el mapeo, para este control de COBIT5 podremos considerar que las prácticas específicas de CMMI SAM-SP 1.3 y SAM-SP 2.2, así como el apartado 12.2 de PMBOK5 están cubiertas si se evidencia el cumplimiento completo de la práctica APO10.03.

- Mapeo Completo: Para este ejemplo de mapeo completo el control elegido es APO01.06 relativo a la propiedad de los activos (datos y sistemas) de la organización. En este caso COBIT5 incluye cuatro actividades para esta práctica, que son las que se muestran en la imagen posterior.

APO01.06 Definir la propiedad de la información (datos) y del sistema. Definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación.	**De**	**Descripción**	**Descripción**	**A**
			Directrices para la clasificación de datos	APO03.02 BAI02.01 DSS05.02 DSS06.01
			Directrices para el control y seguridad de datos	BAI02.01
			Procedimientos de integridad de datos	BAI02.01 DSS06.01
Actividades				
1. Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en toda la empresa.				
2. Definir, mantener y proporcionar herramientas adecuadas, técnicas y directrices para garantizar la seguridad y control efectivo sobre la información y los sistemas en colaboración con el propietario.				
3. Crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones. Incluir los sistemas subcontratados y aquellos cuya propiedad debe permanecer dentro de la empresa.				
4. Definir e implementar procedimientos para asegurar la integridad y consistencia de toda la información almacenada en formato electrónico, tales como bases de datos, almacenes de datos (*data warehouses*) y archivos de datos.				

Ilustración 23: Práctica APO01.06

En este caso el mapeo es con la norma ISO27002:2013, concretamente con algunos controles del bloque "A.8: Gestión de activos". En este caso se ha definido el mapeo como completo ya que se estima que el cumplimiento en uno de los lados podría corresponderse con el cumplimiento en la otra parte.

COBIT 5	**ISO27002:2013**	
Práctica	**C**	**Control**
APO01.06: Definir la propiedad de la información (datos) y del sistema.	C	A.8.1.1: Inventario de activos A.8.1.2: Propiedad de los activos A.8.2.1: Clasificación de la información

- Mapeo Excede: Finalmente, para mostrar un ejemplo de mapeo tipificado como Excede se ha escogido la práctica DSS05.05 relativo a la gestión del acceso físico a los activos. En COBIT se definen siete actividades tal y como muestra la siguiente captura.

DSS05.05 Gestionar el acceso físico a los activos de TI. Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.	**De**	**Descripción**	**Descripción**	**A**
			Peticiones de acceso aprobadas	Interno
			Registros de acceso	DSS06.03
Actividades				
1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.				
2. Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.				
3. Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.				
4. Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.				
5. Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.				
6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alama en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.				
7. Realizar regularmente formación de concienciación de seguridad física.				

Ilustración 24: Práctica APO01.06

En este caso el mapeo es con un numeroso grupo de controles de la norma ISO 27002:2013 ya que la misma dispone de un bloque de controles especialmente dedicado a controles de acceso físico.

COBIT 5	**ISO27002:2013**	
Práctica	**C**	**Control**
DSS05.05: Gestionar el acceso físico a los activos de TI.	E	A.11.1.1: Perímetro de seguridad física A.11.1.2: Controles físicos de entrada A.11.1.3: Seguridad de oficinas, despachos y recursos A.11.1.5: El trabajo en áreas seguras A.11.1.6: Áreas de carga y descarga A.11.2.1: Emplazamiento y protección de equipos A.11.2.6: Seguridad de los equipos fuera de las instalaciones

Para este caso se podría asumir que el cumplimiento de DSS05.05 en COBIT5 no garantiza un cumplimiento de los controles relacionados, pero si a la inversa. Si se dispone de evidencia de cumplimiento de todos los controles identificados se podría afirmar que se ha alcanzado el cumplimiento para la práctica DSS05.05.

A continuación se muestra un nuevo ejemplo en el que se combinan varias modalidades de mapeo. En este caso se observa como la práctica BIA 07.01 de COBIT mapea de forma Parcial con la ISO 27002 y con CMMI, pero de forma completa con el punto 9.3 de la ISO 20000.

COBIT 5		ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3	
Práctica	**C**	**Proceso**	**C**	**Control**	**C**	**Control**	
BIA07.01: Establecer un plan de implementación.	E	9.3	P	A.14.2.5	P	PI-SP 1.1. Establecer una estrategia de integración. PI-SP 3.1. Confirmar la disponibilidad de los componentes de producto para la integración.	

La práctica de COBIT5 se muestra a continuación.

BAI07.01 Establecer un plan de implementación. Establecer un plan de implementación que cubra la conversión de datos y sistemas, criterios de aceptación de las pruebas, comunicación, formación, preparación del lanzamiento, paso a producción, soporte inicial en producción, plan de marcha atrás o de contingencia y una revisión post-implantación. Obtener la aprobación de las partes relevantes.	**De**	**Descripción**	**Descripción**	**A**
	BAI01.09	Plan de gestión de la calidad	Plan de implantación aprobado	Interno
	BAI06.01	• Plan y cronograma de cambio • Peticiones de cambio aprobadas	Proceso de marcha atrás de la implantación o de recuperación	Interno
Actividades				
1. Crear un plan de implantación que refleje la estrategia global de implantación, la secuencia de acciones de implantación, recursos necesarios, interdependencias, criterios para la aceptación por parte de la Dirección de la implantación en producción, requisitos para verificar la instalación, estrategia de transición para el soporte en producción, y la actualización de los planes de continuidad de negocio (BCPs).				
2. Confirmar que todos los planes de implantación son aprobados por las partes interesadas tanto de ámbito técnico como de negocio, y revisados por auditoría interna, si es apropiado.				
3. Obtener el compromiso de los proveedores externos de soluciones a participar en cada paso de la implantación.				
4. Identificar y documentar el proceso de marcha atrás y recuperación.				
5. Revisar formalmente los riesgos técnicos y de negocio asociados a la implantación y asegurar que el riesgo clave es considerado y tratado en el proceso de planificación.				

Ilustración 25: Práctica APO01.06

5.4. Mapeo de controles

Después de haber expuesto la metodología usada para el mapeo, en esta sección se ofrece al lector el mapeo final de controles que se ha desarrollado como proceso de trabajo central en el presente TFG. En el ANEXO I se encuentra el resultado completo del mapeo realizado, con la totalidad de las prácticas definidas en COBIT5 (202) y su correspondencia con los diferentes controles identificados en secciones previas.

El trabajo se ha desarrollado de forma iterativa, esto es, mapeando de forma individual cada norma o marco de trabajo con los controles de COBIT5. Para establecer un mapeo, siguiendo la metodología expuesta, se han considerado todas las actividades incluidas en cada práctica de COBIT5. Una vez mapeada una norma se ha revisado el resultado en su conjunto y se ha proseguido con la siguiente de forma análoga. Finalmente, se ha realizado una profunda revisión a nivel global, tratando de detectar puntos incoherentes y para corregir o retocar alguna correspondencia.

Dado el carácter de memoria del presente documento, se ha presentado el mapeo detallado en formato de tablas, siendo la herramienta generada una hoja de cálculo editable. Esta primera versión de la herramienta permite mayor flexibilidad que una tabla de texto y es la que usaría en caso de aplicarla a una auditoría real. Además, por

economía documental, en el mapeo detallado se ha incluido la referencia al control, identificando cada control mediante su código o numeración sin incluir el texto completo. Se asume que un auditor que maneje con soltura las normativas dispone de los textos completos para consulta, restando facilidad de manejo la inclusión de todos los textos de los controles.

Para presentar los resultados obtenidos en esta sección se ha optado por incluir un resumen del mapeo a nivel de dominio de COBIT5, para entendimiento rápido del grado de alineamiento que tiene cada uno de los cinco dominios COBIT con las diferentes normas. Este mapeo resumido, o a nivel ejecutivo, tiene la única finalidad de ser una representación para entendimiento del lector, constituyendo el mapeo completo la finalidad del presente trabajo.

- Evaluar, Orientar y Supervisar (EDM). El primer dominio de COBIT5 es el correspondiente con la parte de Gobierno, por lo que los procesos y las prácticas incluidas son de nivel estratégico y organizativo. Como era de suponer previamente, este dominio es el que menor alineamiento tiene respecto a las normativas y marcos de trabajo relacionados. COBIT5 es mucho más detallado en cuanto a los procesos de Gobierno de TI, lo que redunda en que todas las correspondencias definidas para este dominio sean de tipo "Parcial". A efectos prácticos en una auditoría de sistemas de información, el cumplimiento de este dominio en COBIT redundaría en el cumplimiento de algunos puntos de la ISO20000, CMMI y PMBOK, siendo su incidencia respecto a la ISO27002 residual.

- Alinear, Planificar y Organizar (APO): Este dominio (al igual que los siguientes) entra dentro del área de Gestión, por lo que su incidencia es mayor respecto a las normas. Dada la amplitud del dominio (13 procesos) su correspondencia con los controles mapeados es mucho mayor, siendo la mayoría de ellas de tipo "Parcial". Destacan los procesos APO09, APO10 y APO13, con numerosas correspondencias respecto a las ISO 20000 y 27002 y APO06, APO11 y APO12 donde el alineamiento es mayor respecto a CMMI y PMBOK.

- Construir, Adquirir e Implementar (BAI): El siguiente dominio COBIT también entra dentro del área de Gestión y su nivel de alineamiento también es destacable respecto a las demás referencias. Destaca por encima de los demás su alta correspondencia con los controles de CMMI, lo que cabía esperarse dado que el enfoque de CMMI es el desarrollo de sistemas de información. Además, procesos como BAI03, BAI04 y BAI10 también están bien alineados respecto a las normas ISO 20000 y 27002.

- Entregar, dar Servicio y Soporte (DSS): Este dominio, orientado a la gestión de la entrega y del soporte de los servicios de TI tiene como principal correspondencia a la norma ISO 20000 que se basa en principios similares. No obstante, destaca también su buen alineamiento con los controles de la ISO 27002. Por el contrario, su correspondencia con PMBOK o CMMI es prácticamente nula.

- Supervisar, Evaluar y Valorar (MEA): El último de los dominios de COBIT5 engloba aquellos procesos destinados a la monitorización y control de las actividades y eventos de la organización como método para la mejora continua. En general, todos los marcos de trabajo disponen de sus controles destinados a estas finalidades, lo que se evidencia mediante numerosos mapeos. Destaca sobre los demás el mapeo entre MEA01 y el área de proceso MA de CMMI. En este caso, muchas de las correspondencias se han tipificado como "Excede", siendo en general más amplio el tratamiento en CMMI que en COBIT para esta área concreta.

Tal y como se ha mencionado anteriormente, el producto final resultante es una herramienta en forma de hoja de cálculo. Se define el siguiente caso de uso principal para la herramienta:

1. Realizar una auditoría completa de COBIT5 en la organización. Mediante este primer paso se obtiene evidencia del cumplimiento o incumplimiento de los procesos de la organización respecto al marco de trabajo más amplio de los considerados en el presente trabajo.

2. Mediante la herramienta, identificar y filtrar todos los controles mapeados de tipo "Parcial" o "Completo" y considerar su cumplimiento como satisfactorio de forma automática.

3. Mediante la herramienta, identificar y filtrar los controles mapeados de tipo "Excede" y considerar si se deben recabar evidencias adicionales que permitan dar por cubierto el control.

4. Para aquellos controles que no tienen correspondencia con COBIT5, realizar las pruebas necesarias para determinar su grado de cumplimiento.

5. Preparar el informe final de cumplimiento de las normas o marcos de referencia que se hayan incluido en el alcance de la auditoría.

6. Conclusiones

Como punto final al presente Trabajo Final de Grado, al revisar y analizar el trabajo desarrollado se puede concluir que se ha alcanzado el objetivo planteado inicialmente de presentar una metodología de trabajo novedosa para el desarrollo de auditorías integradas de sistemas de información.

La metodología propuesta se basa en la realización de auditorías respecto a COBIT 5 para posteriormente (o paralelamente) hacer uso de la herramienta desarrollada para inferir los controles de las demás referencias que ya se han cubierto y para los que no haría falta solicitar evidencias adicionales.

La base para el éxito de la herramienta propuesta es el conocimiento de que para demostrar el grado de cumplimiento en diferentes normas o estándares, es habitual que se soliciten las mismas evidencias, resultando redundante el trabajo desarrollado por los auditores. Mediante la herramienta propuesta, se tiene el convencimiento de que se puede llevar a cabo un trabajo optimizado de auditoría integrada, aportando valor para la organización auditada, optimizando el proceso de auditoría y reduciendo costes para la entidad prestadora del servicio.

Esta reducción de costes puede ser el factor determinante que permita a una empresa ofertar a sus clientes potenciales un producto atractivo económicamente y competitivo, logrando la tan ansiada diferenciación en el mercado actual.

A lo largo de los capítulos que componen el presente documento se han ido desarrollando las diversas metas intermedias que se habían definido en el apartado de objetivos. Así pues, se han escogido cuatro normas y marcos de trabajo de relevancia internacional, seguidamente se han analizado para seleccionar la granularidad y los controles a mapear. Paralelamente, se ha definido una metodología para el mapeo de controles, basándose en los trabajos previos desarrollados por la Organización ISACA.

Finalmente, como actividad central se ha aplicado la metodología de mapeo a las diferentes normas de forma iterativa hasta lograr la herramienta de auditoría integrada que supone el activo principal consecuencia del presente trabajo. El desarrollo de esta parte del trabajo ha supuesto aproximadamente un 60% del volumen total de tiempo invertido en el TFG.

Respecto a la herramienta generada, la cual se presenta en formato de tabla resumida posteriormente, pues concluirse que su uso supone una mejora en los procesos de auditoría integrada ya que permite al auditor eliminar duplicidades en su trabajo y mejora el proceso de revisión del cumplimiento permitiendo que mediante la presentación de evidencias para un control determinado de COBIT 5 se puedan inferir que controles de las demás normas también quedan cubiertos o si por el contrario se debe solicitar alguna evidencia adicional.

6.1. Líneas de trabajo abiertas

Dado el carácter acotado de un Trabajo Final de Grado y la gran amplitud del área de estudio, se han identificado una serie de mejoras y de tareas futuras que permitirían evolucionar y mejorar la herramienta y como consecuencia, el proceso de auditoría integrada de sistemas de información.

- Considerar la inclusión de más normativas o marcos de trabajo. Actualmente, en el mercado coexisten gran cantidad de estándares en dura pugna entre sí para convertirse en la referencia para las empresas. En ampliaciones futuras de la herramienta se contempla la posibilidad de añadir los controles relacionados con la legislación vigente en España, siendo la Ley Orgánica de Protección de datos y principalmente el Real Decreto que la desarrolla (1720/2007) un claro candidato.

  Adicionalmente y siguiendo la misma línea, se podrían definir mapeos sectoriales, incluyendo normativas de aplicación a ciertos tipos de organizaciones. A modo de ejemplo, el Esquema Nacional de Seguridad se podría mapear para su uso en administraciones públicas, mientras que los controles de PCI-DSS se podrían mapear para su uso en entidades que traten datos relativos a las tarjetas de crédito.

- Obviamente, otra línea de evolución abierta para la herramienta sería realizar un proceso de refinado del mapeo, una vez que el mismo haya sido testado en un entorno real.

- Adicionalmente, sería deseo del autor de este trabajo implementar una herramienta software, que de forma guiada y automatizada pudiera generar informes y resultados de auditorías integradas.

6.2. Agradecimientos.

Aunque el que escribe figure como autor del presente trabajo, el mismo no habría podido desarrollarse sin el soporte de muchas personas.

Empezando por mis padres, cuya infinita paciencia, apoyo recibido e insistencia han hecho posible en gran medida que actualmente esté redactando estas líneas. A ellos solo me cabe agradecerles hasta la saciedad que no dejaran en el olvido algo que se ha dilatado en el tiempo más de lo que cabría esperar.

A mi querida Lauren, por su esfuerzo y su apoyo incondicional que me han permitido disponer del tiempo y de los recursos para poder finalmente dedicarme a lo que realmente me motiva.

Finalmente, y no por ello de menor importancia, a mis tutores y mentores. A Ignacio Gil por sus consejos y sus discursos inspiradores y a todo el equipo de Auren, encabezado por José Miguel Cardona y Josep Cuñat por acogerme y darme la oportunidad de desarrollar mi carrera profesional en un área como la auditoría, la consultoría y el peritaje informático.

ANEXO I: Mapeo detallado de controles

1. Evaluar, Orientar y Supervisar

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Proceso**	**C**	**Control**	**C**	**Control**	**C**	**Control**
EDM01.01: Evaluar el sistema de gobierno.	-	-	-	-	-	-	-	-
EDM01.02: Orientar el sistema de gobierno.	-	-	-	-	-	-	-	-
EDM01.03: Supervisar el sistema de gobierno.	-	-	-	-	-	-	-	-
EDM02.01: Evaluar la optimización de valor.	-	-	-	-	-	-	-	-
EDM02.02: Orientar la optimización del valor.	-	-	-	-	-	-	-	-
EDM02.03: Supervisar la optimización de valor.	-	-	-	-	-	-	-	-
EDM03.01: Evaluar la gestión de riesgos.	-	-	-	-	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Proceso**	**C**	**Control**	**C**	**Control**	**C**	**Control**
EDM03.02: Orientar la gestión de riesgos.	P	6.6.1.	-	-	P	RSKM-SP 1.3. RSKM-SP 2.2.	-	-
EDM03.03: Supervisar la gestión de riesgos.	-	-	-	-	-	-	P	11.6: Controlar los riesgos
EDM04.01: Evaluar la gestión de recursos.	-	-	-	-	-	-	-	-
EDm04.02: Orientar la gestión de recursos.	-	-	-	-	-	-	-	-
EDM04.03: Supervisar la gestión de recursos.	-	-	-	-	-	-	-	-
EDM05.01: Evaluar los requisitos de elaboración de informes de las partes interesadas.	-	-	-	-	-	-	P	10.1: Planificar la Gestión de las Comunicaciones 13.2: Planificar la Gestión de los Interesados
EDM05.02: Orientar la comunicación con las partes interesadas y la elaboración de informes.	-	-	-	-	-	-	P	10.2 Gestionar las Comunicaciones 13.3 Gestionar la Participación de los Interesados
EDM05.03: Supervisar la comunicación con las partes interesadas.	-	-	-	-	-	-	P	10.3 Controlar las Comunicaciones 13.4 Controlar la Participación de los Interesados

2. Alinear, Planificar y Organizar

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
APO01.01: Definir la estructura organizativa.	-	-	-	-	-	-	-	-
APO01.02: Establecer roles y responsabilidades.	-	-	P	A.6.1.1 A.6.1.2 A.7.2.1 A.8.1.3 A.16.1.1	-	-	-	-
APO01.03: Mantener los elementos catalizadores del sistema de gestión.	-	-	-	-	-	-	-	-
APO01.04: Comunicar los objetivos y la dirección de gestión.	-	-	-	-	-	-	-	-
APO01.05: Optimizar la ubicación de la función de TI.	-	-	-	-	-	-	-	-
APO01.06: Definir la propiedad de la información (datos) y del sistema.	-	-	C	A.8.1.1 A.8.1.2 A.8.2.1	-	-	-	-
APO01.07: Gestionar la mejora continua de los procesos.	-	-	-	-	-	-	-	-
APO01.08: Mantener el cumplimiento con las políticas y procedimientos.	-	-	-	-	P	OPF-SP 1.1	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
APO02.01: Comprender la dirección de la empresa.	P	7.1	-	-	-	-	-	-
APO02.02: Evaluar el entorno, capacidades y rendimiento actuales.	P	6.5	-	-	-	-	-	-
APO02.03: Definir el objetivo de las capacidades de TI.	C	6.5	-	-	-	-	-	-
APO02.04: Realizar un análisis de diferencias.	-	-	-	-	-	-	-	-
APO02.05: Definir el plan estratégico y la hoja de ruta.	-	-	-	-	-	-	-	-
APO02.06: Comunicar la estrategia y la dirección de TI.	-	-	-	-	-	-	-	-
APO03.01: Desarrollar la visión de la arquitectura de empresa.	-	-	-	-	-	-	-	-
APO03.02: Definir la arquitectura de referencia.	-	-	P	A.8.1.1 A.8.1.3 A.8.2.1 A.8.2.2 A.8.2.3	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
APO03.03: Seleccionar las oportunidades y las soluciones.	-	-	-	-	-	-	-	-
APO03.04: Definir la implementación de la arquitectura.	-	-	-	-	-	-	-	-
APO03.05: Proveer los servicios de arquitectura empresarial.	-	-	-	-	-	-	-	-
APO04.01: Crear un entorno favorable para la innovación.	-	-	-	-	-	-	-	-
APO04.02: Mantener un entendimiento del entorno de la empresa.	-	-	-	-	-	-	-	-
APO04.03: Supervisar y explorar el entorno tecnológico.	P	6.5	-	-	-	-	-	-
APO04.04: Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.	-	-	-	-	-	-	-	-
APO04.05: Recomendar iniciativas apropiadas adicionales.	-	-	-	-	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
APO04.06: Supervisar la implementación y el uso de la innovación.	-	-	-	-	-	-	-	-
APO05.01: Establecer la mezcla del objetivo de inversión.	-	-	-	-	-	-	-	-
APO05.02: Determinar la disponibilidad y las fuentes de fondos.	-	-	-	-	-	-	-	-
APO05.03: Evaluar y seleccionar los programas a financiar.	-	-	-	-	-	-	-	-
APO05.04: Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	-	-	-	-	-	-	-	-
APO05.05: Mantener los portafolios.	-	-	-	-	-	-	-	-
APO05.06: Gestionar la consecución de beneficios.	-	-	-	-	-	-	-	-
APO06.01: Gestionar las finanzas y la contabilidad	P	6.4	-	-	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
APO06.02: Priorizar la asignación de recursos.	-	-	-	-	-	-	-	-
APO06.03: Crear y mantener presupuestos.	P	6.4	-	-	-	-	-	-
APO06.04: Modelar y asignar costes.	P	6.4	-	-	-	-	-	-
APO06.05: Gestionar costes.	P	6.4	-	-	-	-	-	-
APO07.01: Mantener la dotación de personal suficiente y adecuada.	-	-	P	A.7.1.1 A.7.1.2	-	-	P	9.1 Planificar la Gestión de los Recursos Humanos
APO07.02: Identificar personal clave de TI.	-	-	P	A.7.3.1 A.8.1.4.	-	-	P	9.2 Adquirir el Equipo del Proyecto
APO07.03: Mantener las habilidades y competencias del personal.	-	-	-	-	E	OT-SP 1.1. Establecer las necesidades estratégicas de formación. OT-SP 1.2. Determinar qué necesidades de formación son responsabilidad de la organización. OT-SP 1.3. Establecer un	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
						plan táctico de formación en la organización. OT-SP 1.4. Establecer una capacidad de formación. OT-SP 2.1. Impartir la formación. OT-SP 2.2. Establecer los - registros de formación. OT-SP 2.3. Evaluar la eficacia de la formación.		
APO07.04: Evaluar el desempeño laboral de los empleados.	-	-	P	A.7.2.3 A.8.1.3	-	-	-	-
APO07.05: Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	-	-	-	-	-	-	P	9.1 Planificar la Gestión de los Recursos Humanos
APO07.06: Gestionar el personal contratado	C	7.2	-	-	-	-	-	-
APO08.01: Entender las expectativas del negocio.	-	-	-	-	-	-	-	-
APO08.02: Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.	-	-	-	-	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
APO08.03: Gestionar las relaciones con el negocio.	C	7.1						
APO08.04: Coordinar y comunicar.	-	-	-	-	-	-	-	-
APO08.05: Proveer datos de entrada para la mejora continua de los servicios.	-	-	-	-	-	-	-	-
APO09.01: Identificar servicios TI.	P	6.1	-	-	-	-	-	-
APO09.02: Catalogar servicios basados en TI.	E	6.1	-	-	-	-	-	-
APO09.03: Definir y preparar acuerdos de servicio.	E	6.1	-	-	P	SAM-SP 1.3. Establecer acuerdos con proveedores.	-	-
APO09.04: Supervisar e informar de los niveles de servicio.	E	6.2	-	-	P	SAM-SP 2.2. Ejecutar el acuerdo con el proveedor.	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
APO09.05: Identificar y evaluar las relaciones y contratos con proveedores.	E	6.1 7.1	-	-	-	-	-	-
APO10.01: Identificar y evaluar las relaciones y contratos con proveedores.	P	7.2	P	A.15.1.1 A.15.1.2	-	-	P	12.1 Planificar la Gestión de las Adquisiciones
APO10.02: Seleccionar proveedores.	-	-	-	-	C	SAM-SP 1.2. Seleccionar a los proveedores. SAM-SP 1.1. Determinar el tipo de adquisición.		
APO10.03: Gestionar contratos y relaciones con proveedores.	C	7.2	P	A.13.2.2 A.13.2.4 A.15.1.3	P	SAM-SP 1.3. Establecer acuerdos con proveedores. SAM-SP 2.2. Aceptar el producto adquirido.	P	12.2 Efectuar las Adquisiciones
APO10.04: Gestionar el riesgo en el suministro.	-	-	P	A.15.2.2	-	-	-	-
APO10.05: Supervisar el cumplimiento y el rendimiento del proveedor.	C	7.2	P	A.14.2.7 A.15.2.1	-	-	P	12.3 Controlar las Adquisiciones 12.4 Cerrar las Adquisiciones

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
APO11.01: Establecer un sistema de gestión de la calidad (SGC).	-	-	-	-	P	OPD-SP 1.1. Establecer los procesos estándar.	P	8.1 Planificar la Gestión de la Calidad
APO11.02: Definir y gestionar estándares, procesos y prácticas de calidad.	-	-	-	-	E	OPD-SP 1.1. Establecer los procesos estándar. OPD-SP 1.3. Establecer los criterios y las guías de adaptación. OPD-SP 1.5. Establecer la biblioteca de activos de proceso de la organización. OPD-SP 1.6. Establecer los estándares del entorno de trabajo. OPD-SP 1.7. Establecer las reglas y guías para los equipos. OPF-SP 1.1. Establecer las necesidades de proceso de la organización.	P	8.2 Realizar el Aseguramiento de Calidad
APO11.03: Enfocar la gestión de la calidad en los clientes.	P	7.1	-	-	-	-	-	-
APO11.04: Supervisar y hacer controles y revisiones de la calidad.	-	-	-	-	E	OPF-SP 1.2. Evaluar los procesos de la organización OPF-SP 1.3. Identificar las mejoras de proceso de la organización	P	8.3 Controlar la Calidad

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
APO11.05: Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	-	-	-	-	E	DAR-SP 1.1. Establecer y mantener guías para determinar qué cuestiones están sujetas a un proceso de evaluación formal. DAR-SP 1.2. Establecer y mantener los criterios para evaluar las alternativas y la clasificación relativa de estos criterios. DAR-SP 1.4. Seleccionar métodos de evaluación.	P	8.2 Realizar el Aseguramiento de Calidad
APO11.06: Mantener una mejora continua.	-	-	-	-	E	OPF-SP 1.3. Identificar las mejoras de proceso de la organización. OPF-SP 2.1. Establecer los planes de acción de proceso. OPF-SP 2.2. Implementar los planes de acción de proceso.	P	8.2 Realizar el Aseguramiento de Calidad
APO12.01: Recopilar datos.	-	-	P	A.16.1.2	E	RSKM-SP 1.1. Determinar las fuentes y las categorías de riesgos. RSKM-SP 2.1. Identificar los riesgos.	P	11.2 Identificar los Riesgos
APO12.02: Analizar el riesgo.	-	-	-	-	E	RSKM-SP 1.2. Definir los parámetros de riesgos. RSKM-SP 2.1. Identificar los riesgos. RSKM-SP 2.2. Evaluar, clasificar y priorizar los riesgos.	E	11.3 Realizar el Análisis Cualitativo de Riesgos 11.4 Realizar el Análisis Cuantitativo de Riesgos

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
APO12.03: Mantener un perfil de riesgo.	-	-	-	-	E	RSKM-SP 2.2. Evaluar, clasificar y priorizar los riesgos.	-	-
APO12.04: Expresar el riesgo.	-	-	-	-	-	-	-	-
APO12.05: Definir un portafolio de acciones para la gestión de riesgos.	-	-	-	-	P	RSKM-SP 1.3. Establecer una estrategia de gestión de riesgos.	C	11.5 Planificar la Respuesta a los Riesgos
APO12.06: Responder al riesgo.	-	-	-	-	C	RSKM-SP 3.1. Desarrollar los planes de mitigación de riesgos. RSKM-SP 3.2. Implementar los planes de mitigación de riesgos.	C	11.5 Planificar la Respuesta a los Riesgos
APO13.01: Establecer y mantener un SGSI.	P	6.6.1	P	A.5.1.1 A.6.1.1	-	-	-	-
APO13.02: Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	P	6.6.1	P	A.7.2.2 A.12.1.1 A.16.1.5	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
APO13.03: Supervisar y revisar el SGSI.	P	6.6.1	C	A.5.1.2 A.18.2.1	-	-	-	-

3. Construir, Adquirir e Implementar

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
BIA01.01: Mantener un enfoque estándar para la gestión de programas y proyectos.	-	-	-	-	E	IPM-SP 1.1. Establecer y mantener el proceso definido del proyecto desde su arranque y a lo largo de la vida del proyecto.	-	-
BIA 01.02: Iniciar un programa.	-	-	-	-	P	OPF-SP 3.1. Desplegar los activos de proceso de la organización. OPF-SP 3.2. Desplegar los procesos estándar.	-	-
BIA01.03: Gestionar el compromiso de las partes interesadas.	-	-	-	-	E	IPM-SP 2.1. Gestionar la involucración en el proyecto de las partes interesadas relevantes. IPM-SP 2.2. Participar con las partes interesadas relevantes para identificar, negociar y seguir las dependencias críticas. PP-SP 2.6. Planificar la involucración de las partes interesadas. PP-SP 3.3. Obtener el compromiso con el plan.	E	13.1 Identificar a los Interesados 13.2 Planificar la Gestión de los Interesados 13.3 Gestionar la Participación de los Interesados 13.4 Controlar la Participación de los Interesados

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
BIA01.04: Desarrollar y mantener el plan de programa.	-	-	-	-	P	IPM-SP 1.4. Integrar el plan del proyecto y otros planes que afecten al proyecto para describir el proceso definido del proyecto. IPM-SP 1.6. Establecer y mantener equipos. OPD-SP 1.2. Establecer las descripciones de los modelos de ciclo de vida.	-	-
BIA01.05: Lanzar y ejecutar el programa.	-	-	-	-	-	-	-	-
BIA01.06: Supervisar, controlar e informar de los resultados del programa.	-	-	-	-	E	IPM-SP 2.3. Resolver las cuestiones con las partes interesadas relevantes. MA-SP 1.1. Establecer y mantener los objetivos de medición derivados de las necesidades de información y de los objetivos identificados. OPF-SP 3.3. Monitorizar la implementación.	-	-
BIA01.07: Lanzar e iniciar proyectos dentro de un programa.	-	-	-	-	P	IPM-SP 1.5. Gestionar el proyecto utilizando el plan de proyecto, otros planes que afecten al proyecto y el proceso definido del proyecto.	E	4.1 Desarrollar el Acta de Constitución del Proyecto 5.1 Planificar la Gestión del Alcance 5.3 Definir el Alcance 7.1 Planificar la Gestión de los Costos

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
BIA01.08: Planificar proyectos.	-	-	-	-	E	IPM-SP 1.1. Establecer y mantener el proceso definido del proyecto desde su arranque y a lo largo de la vida del proyecto. IPM-SP 1.2. Utilizar los activos de proceso de la organización y el repositorio de mediciones para estimar y planificar las actividades del proyecto. PP-SP 1.1. Estimar el alcance del proyecto. PP-SP 1.2. Establecer las estimaciones de los atributos de los productos de trabajo y de las tareas. PP-SP 1.3. Definir las fases del ciclo de vida del proyecto. PP-SP 1.4. Estimar el esfuerzo y el coste. PP-SP 2.1. Establecer el presupuesto y el calendario. PP-SP 2.2. Identificar los riesgos del proyecto. PP-SP 2.3. Planificar la gestión de los datos. PP-SP 2.4. Planificar los recursos del proyecto. PP-SP 2.5. Planificar el conocimiento y las habilidades necesarias. PP-SP 2.6. Planificar la involucración de las partes	E	4.2 Desarrollar el Plan para la Dirección del Proyecto 5.2 Recopilar Requisitos 5.4 Crear la EDT/WBS 6.1 Planificar la Gestión del Cronograma 6.2 Definir las Actividades 6.3 Secuenciar las Actividades 6.4 Estimar los Recursos de las Actividades 6.5 Estimar la Duración de las Actividades 6.6 Desarrollar el Cronograma 9.1 Planificar la Gestión de los Recursos Humanos 10.1 Planificar la Gestión de las Comunicaciones 12.1 Planificar la Gestión de las Adquisiciones

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
						interesadas. PP-SP 2.7. Establecer el plan de proyecto.		
BIA01.09: Gestionar la calidad de los programas y proyectos.	-	-	-	-	-	-	E	8.1 Planificar la Gestión de la Calidad 8.2 Realizar el Aseguramiento de Calidad 8.3 Controlar la Calidad
BIA01.10: Gestionar el riesgo de los programas y proyectos.	-	-	P	A.6.1.5	P	PMC-SP 1.3. Monitorizar los riesgos del proyecto. PP-SP 3.1. Revisar los planes que afectan al proyecto.	E	11.1 Planificar la Gestión de los Riesgos 11.2 Identificar los Riesgos 11.4 Realizar el Análisis Cuantitativo de Riesgos 11.5 Planificar la Respuesta a los Riesgos

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
BIA01.11: Supervisar y controlar proyectos.	-	-	-	-	E	PMC-SP 1.1. Monitorizar los parámetros de planificación del proyecto. PMC-SP 1.2. Monitorizar los compromisos. PMC-SP 1.3. Monitorizar los riesgos del proyecto. PMC-SP 1.4. Monitorizar la gestión de los datos. PMC-SP 1.5. Monitorizar la involucración de las partes interesadas. PMC-SP 1.6. Llevar a cabo las revisiones del progreso. PMC-SP 1.7. Llevar a cabo las revisiones de hitos. PMC-SP 2.1. Analizar las cuestiones. PMC-SP 2.2. Llevar a cabo las acciones correctivas. PMC-SP 2.3. Gestionar las acciones correctivas.	E	4.3 Dirigir y Gestionar el Trabajo del Proyecto 4.4 Monitorear y Controlar el Trabajo del Proyecto 4.5 Realizar el Control Integrado de Cambios 5.5 Validar el Alcance 5.6 Controlar el Alcance 7.4 Controlar los Costos 10.3 Controlar las Comunicaciones 11.6 Controlar los Riesgos 12.3 Controlar las Adquisiciones

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
BIA01.12: Gestionar los recursos y los paquetes de trabajo del proyecto.	-	-	-	-	E	IPM-SP 1.3. Establecer y mantener el entorno de trabajo del proyecto en base a los estándares de entorno de trabajo de la organización. PP-SP 2.4. Planificar los recursos del proyecto. PP-SP 3.2. Conciliar los niveles de trabajo y de recursos.	E	4.3 Dirigir y Gestionar el Trabajo del Proyecto 6.4 Estimar los Recursos de las Actividades 6.5 Estimar la Duración de las Actividades 9.1 Planificar la Gestión de los Recursos Humanos 12.1 Planificar la Gestión de las Adquisiciones
BIA01.13: Cerrar un proyecto o iteración.	-	-	-	-	P	IPM-SP 1.7. Contribuir con experiencias relativas al proceso a los activos de proceso de la organización. OPF-SP 3.4. Incorporar las experiencias en los activos de proceso de la organización.	C	4.6 Cerrar el Proyecto o Fase 12.4 Cerrar las Adquisiciones
BIA01.14: Cerrar un programa.	-	-	-	-	-	-	-	-
BIA02.01: Definir y mantener los requerimientos técnicos y funcionales de negocio.	-	-	-	-	E	RD-SP 1.1. Educir las necesidades. RD-SP 1.2. Trasformar las necesidades de las partes interesadas en requisitos del cliente. RD-SP 2.1. Establecer los requisitos de producto y de	C	5.2 Recopilar Requisitos

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
						componente de producto. RD-SP 2.2. Asignar los requisitos de componente de producto. RD-SP 2.3. Identificar los requisitos de interfaz. RD-SP 3.1. Establecer los conceptos y los escenarios de operación. RD-SP 3.2. Establecer una definición de la funcionalidad y de los atributos de calidad requeridos. RD-SP 3.3. Analizar los requisitos. RD-SP 3.4. Analizar los requisitos para conseguir un equilibrio. REQM- SP 1.1. Comprender los requisitos. REQM-SP 1.3. Gestionar los cambios a los requisitos. REQM-SP 1.4. Mantener la trazabilidad bidireccional de los requisitos. REQM-SP 1.5. Asegurar el alineamiento entre el trabajo del proyecto y los requisitos.		

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
BIA02.02: Realizar un estudio de viabilidad y proponer soluciones alternativas.	-	-	-	-	E	DAR-SP 1.3. Identificar soluciones alternativas para tratar las cuestiones. DAR-SP 1.5. Evaluar las soluciones alternativas utilizando criterios y métodos establecidos. DAR-SP 1.6. Seleccionar las soluciones a partir de alternativas en base a criterios de evaluación. SAM-SP 1.1. Determinar el tipo de adquisición. TS-SP 1.1. Desarrollar soluciones alternativas y los criterios de selección. TS-SP 1.2. Seleccionar las soluciones de componentes de producto. TS-SP 2.3. Realizar los análisis sobre si hacer, comprar o reutilizar.	-	-
BIA02.03: Gestionar los riesgos de los requerimientos.	-	-	-	-	-	-	-	-
BIA02.04: Obtener la aprobación de los requerimientos y soluciones.	-	-	-	-	P	RD-SP 3.5. Validar los requisitos. REQM-SP 1.2. Obtener el compromiso sobre los requisitos.	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
BIA03.01: Diseñar soluciones de alto nivel.	-	-	P	A14.2.1	P	TS-SP 1.1. Desarrollar soluciones alternativas y los criterios de selección.	-	-
BIA03.02: Diseñar los componentes detallados de la solución.	-	-	-	-	P	TS-SP 2.1. Diseñar el producto o los componentes de producto.	-	-
BIA03.03: Desarrollar los componentes de la solución.	-	-	P	A.14.2.6	P	TS-SP 2.2. Establecer un paquete de datos técnicos. TS-SP 3.1. Implementar el diseño. TS-SP 3.2. Desarrollar la documentación de soporte del producto.	-	-
BIA03.04: Obtener los componentes de la solución.	-	-	-	-	C	SAM-SP 1.1. Determinar el tipo de adquisición. SAM-SP 2.2. Aceptar el producto adquirido.	P	12.2 Efectuar las Adquisiciones 12.3 Controlar las Adquisiciones
BIA03.05: Construir soluciones.	P	6.1	P	A.12.4.1 A.14.2.1 A.14.2.6	P	SAM-SP 2.3. Asegurar la transición de los productos. TS-SP 3.1. Implementar el diseño. TS-SP 3.2. Desarrollar la documentación de soporte del producto.	-	-
BIA03.06: Realizar controles de calidad.	-	-	P	A.14.1.2 A.14.1.3	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
BIA03.07: Preparar pruebas de la solución.	-	-	-	-	-	-	-	-
BIA03.08: Ejecutar pruebas de la solución.	-	-	P	A.14.2.8 A.14.2.9	-	-	-	-
BIA03.09: Gestionar cambios a los requerimientos.	-	-	P	A.14.2.2	-	-	-	-
BIA03.10: Mantener soluciones.	-	-	P	A.12.6.1	-	-	-	-
BIA03.11: Definir los servicios TI y mantener el catálogo de servicios	P	6.1	-	-	-	-	-	-
BIA04.01: Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.	E	6.3.1 6.3.2 6.5	P	A.12.1.3 A.17.2.1	-	-	-	-
BIA04.02: Evaluar el impacto en el negocio.	P	6.3.1	P	A.17.1.1	-	-	-	-
BIA04.03: Planificar requisitos de servicios nuevos o modificados.	C	6.5	-	-	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
BIA04.04: Supervisar y revisar la disponibilidad y la capacidad.	C	6.2 6.3.2 6.5	-	-	-	-	-	-
BIA04.05: Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.	C	6.3.3 6.5	-	-	-	-	-	-
BIA05.01: Establecer el deseo de cambiar.	-	-	-	-	-	-	-	-
BIA05.02: Formar un equipo de implementación efectivo.	-	-	-	-	-	-	-	-
BIA05.03: Comunicar la visión deseada.	-	-	-	-	-	-	-	-
BIA05.04: Facultar a los que juegan algún e identificar ganancias en el corto plazo.	-	-	-	-	-	-	-	-
BIA05.05: Facilitar la operación y el uso.	-	-	-	-	-	-	-	-
BIA05.06: Integrar nuevos enfoques.	-	-	-	-	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
BIA05.07: Mantener los cambios.	-	-	-	-	-	-	-	-
BIA06.01: Evaluar, priorizar y autorizar peticiones de cambio.	C	9.2	P	A.12.1.2 A.14.2.2 A.14.2.4	-	-	P	4.5 Realizar el Control Integrado de Cambios
BIA06.02: Gestionar cambios de emergencia.	C	9.2	-	-	-	-	-	-
BIA06.03: Hacer seguimiento e informar de cambios de estado.	P	9.2	-	-	-	-	-	-
BIA06.04: Cerrar y documentar los cambios.	P	9.2	-	-	-	-	-	-
BIA07.01: Establecer un plan de implementación.	E	9.3	P	A.14.2.5	P	PI-SP 1.1. Establecer una estrategia de integración. PI-SP 3.1. Confirmar la disponibilidad de los componentes de producto para la integración.	-	-
BIA07.02: Planificar la conversión de procesos de negocio, sistemas y datos.	-	-	-	-	P	PI-SP 2.2. Gestionar las interfaces. SAM-SP 2.3. Asegurar la transición de los productos.	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
BIA07.03: Planificar pruebas de aceptación.	-	-	-	-	P	PI-SP 1.3. Establecer los procedimientos y los criterios de integración del producto.	-	-
BIA07.04: Establecer un entorno de pruebas.	P	9.3	P	A.12.1.4 A.14.3.1	P	PI-SP 1.2. Establecer el entorno de integración del producto.	-	-
BIA07.05: Ejecutar pruebas de aceptación.	P	9.3	P	A.14.2.3 A.14.2.8 A.14.2.9	P	PI-SP 2.1. Revisar la completitud de las descripciones de las interfaces.	-	-
BIA07.06: Pasar a producción y gestionar los lanzamientos.	P	9.2 9.3	-	-	P	PI-SP 3.2. Ensamblar los componentes de producto. PI-SP 3.4. Empaquetar y entregar el producto o componente de producto.	-	-
BIA07.07: Proporcionar soporte en producción desde el primer momento.	-	-	-	-	-	-	-	-
BIA07.08: Ejecutar una revisión post-implantación.	C	9.2 9.3	-	-	P	PI-SP 3.3. Evaluar los componentes de producto ensamblados.	-	-
BIA08.01: Cultivar y facilitar una cultura de intercambio de conocimientos.	-	-	-	-	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
BIA08.02: Identificar y clasificar las fuentes de información.	-	-	P	A.6.1.4	-	-	-	-
BIA08.03: Organizar y contextualizar la información, transformándola en conocimiento.	-	-	-	-	-	-	-	-
BIA08.04: Utilizar y compartir el conocimiento.	-	-	-	-	-	-	-	-
BIA08.05: Evaluar y retirar la información.	-	-	-	-	-	-	-	-
BIA09.01: Identificar y registrar los activos actuales.	-	-	P	A.8.1.1 A.8.1.2	-	-	-	-
BIA09.02: Gestionar Activos Críticos.	-	-	-	-	-	-	-	-
BIA09.03: Gestionar el ciclo de vida de los activos.	-	-	P	A.8.1.3 A.8.1.4 A.8.2.2 A.8.3.2 A.11.2.7	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
BIA09.04: Optimizar el coste de los activos.	-	-	-	-	-	-	-	-
BIA09.05: Administrar Licencias.	-	-	P	A.18.1.2	-	-	-	-
BIA10.01: Establecer y mantener un modelo de configuración.	E	9.1	-	-	E	CM-SP 1.2. Establecer y mantener un sistema de gestión de configuración y de gestión de cambios para controlar los productos de trabajo.	-	-
BIA10.02: Establecer y mantener un repositorio de configuración y una base de referencia.	E	9.1	-	-	E	CM-SP 1.1. Identificar los elementos de configuración, los componentes, y los productos de trabajo relacionados que serán puestos bajo gestión de configuración. CM-SP 1.3. Crear o liberar las líneas base para uso interno y para la entrega al cliente.	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
BIA10.03: Mantener y controlar los elementos de configuración.	E	9.1	-	-	E	CM-SP 1.2. Establecer y mantener un sistema de gestión de configuración y de gestión de cambios para controlar los productos de trabajo. CM-SP 2.1. Seguir las peticiones de cambio a los elementos de configuración. CM-SP 2.2. Controlar los cambios a los elementos de configuración.	-	-
BIA10.04: Generar informes de estado y configuración.	-	-	-	-	E	CM-SP 3.1. Establecer y mantener los registros que describen los elementos de configuración.	-	-
BIA10.05: Verificar y revisar la integridad del repositorio de configuración.	E	9.1	-	-	E	CM-SP 3.1. Establecer y mantener los registros que describen los elementos de configuración.	-	-

4. Entregar, dar Servicio y Soporte

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
DSS01.01: Ejecutar procedimientos operativos.	-	-	E	A.12.1.1				
DSS01.02: Gestionar servicios externalizados de TI.	-	-	P	A.15.1.2 A.15.2.1				
DSS01.03: Supervisar la infraestructura de TI.	-	-	P	A.16.1.2	-	-	-	-
DSS01.04: Gestionar el entorno.	-	-	P	A.6.1.3 A.6.2.1 A.11.1.4 A.11.1.5 A.11.2.1 A.11.2.6	-	-	-	-
DSS01.05: Gestionar las instalaciones.	-	-	P	A.11.1.6 A.11.2.2 A.11.2.3 A.11.2.4	-	-	-	-
DSS02.01: Definir esquemas de clasificación de incidentes y peticiones de servicio.	E	8.1	P	A.16.1.2 A.16.1.4	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
DSS02.02: Registrar, clasificar y priorizar peticiones e incidentes.	E	8.1	P	A.16.1.3	-	-	-	-
DSS02.03: Verificar, aprobar y resolver peticiones de servicio.	P	8.1	-	-	-	-	-	-
DSS02.04: Investigar, diagnosticar y localizar incidentes.	P	8.1	P	A.16.1.1 A.16.1.7	-	-	-	-
DSS02.05: Resolver y recuperarse ante incidentes.	-	-	P	A.16.1.1 A.16.1.7	-	-	-	-
DSS02.06: Cerrar peticiones de servicio e incidentes.	-	-	-	-	-	-	-	-
DSS02.07: Seguir el estado y emitir de informes.	P	6.2	-	-	-	-	-	-
DSS03.01: Identificar y clasificar problemas.	P	8.2	-	-	-	-	-	-
DSS03.02: Investigar y diagnosticar problemas.	P	8.2						

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
DSS03.03: Levantar errores conocidos.	P	8.2	-	-	-	-	-	-
DSS03.04: Resolver y cerrar problemas.	P	8.2	-	-	-	-	-	-
DSS03.05: Realizar una gestión de problemas proactiva.	-	-	-	-	-	-	-	-
DSS04.01: Definir la política de continuidad de negocio, objetivos y alcance.	-	-	P	A.17.1.1	-	-	-	-
DSS04.02: Mantener una estrategia de continuidad.	-	-	P	A.17.1.1	-	-	-	-
DSS04.03: Desarrollar e implementar una respuesta a la continuidad del negocio.	C	6.3.1 6.3.2	P	A.17.1.2	-	-	-	-
DSS04.04: Ejercitar, probar y revisar el BCP.	C	6.3.3	P	A.17.1.3	-	-	-	-
DSS04.05: Revisar, mantener y mejorar el plan de continuidad.	P	6.3.3	P	A.17.1.3	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
DSS04.06: Proporcionar formación en el plan de continuidad.	-	-	-	-	-	-	-	-
DSS04.07: Gestionar acuerdos de respaldo.	-	-	P	A.12.3.1 A.17.2.1	-	-	-	-
DSS04.08: Ejecutar revisiones post-reanudación.	P	6.3.3	-	-	-	-	-	-
DSS05.01: Proteger contra software malicioso (malware).	-	-	E	A.6.1.4 A.8.1.3 A.12.2.1 A.12.5.1	-	-	-	-
DSS05.02: Gestionar la seguridad de la red y las conexiones.	P	6.6.2	E	A.9.1.2 A.12.4.4 A.13.1.1 A.13.1.2 A.13.1.3 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3	-	-	-	-
DSS05.03: Gestionar la seguridad de los puestos de usuario final.	-	-	E	A.6.2.1 A.9.4.4 A.10.1.1 A.10.1.2 A.11.2.8 A.11.2.9 A.12.6.2	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
DSS05.04: Gestionar la identidad del usuario y el acceso lógico.	-	-	E	A.6.2.2 A.9.1.1 A.9.1.2 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.5 A.9.2.6 A.9.3.1 A.9.4.1 A.9.4.2 A.9.4.3 A.9.4.5 A.12.4.1 A.12.4.3	-	-	-	-
DSS05.05: Gestionar el acceso físico a los activos de TI.	-	-	E	A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.6	-	-	-	-
DSS05.06: Gestionar documentos sensibles y dispositivos de salida.	-	-	E	A.8.3.1 A.8.3.2 A.8.3.3 A.11.2.5 A.11.2.7	-	-	-	-
DSS05.07: Supervisar la infraestructura para detectar eventos relacionados con la	P	6.6.2 6.6.3	E	A.12.4.1 A.12.4.2 A.12.6.1 A.12.7.1	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
seguridad.								
DSS06.01: Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos.	-	-	-	-	-	-	-	-
DSS06.02: Controlar el procesamiento de la información.	-	-	-	-	-	-	-	-
DSS06.03: Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	-	-	P	A.6.1.1 A.6.1.2	-	-	-	-
DSS06.04: Gestionar errores y excepciones.	-	-	-	-	-	-	-	-
DSS06.05: Asegurar la trazabilidad de los eventos y responsabilidades y de información.	-	-	P	A.12.4.1	-	-	-	-
DSS06.06: Asegurar los activos de información.	-	-	P	A.8.1.3 A.8.2.1	-	-	-	-

5. Supervisar, Evaluar y Valorar

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
MEA01.01: Establecer un enfoque de la supervisión.	P	6.1 6.2	-	-	E	MA-SP 1.1. Establecer y mantener los objetivos de medición derivados de las necesidades de información y de los objetivos identificados VAL-SP 1.1. Seleccionar los productos para la validación. VAL-SP 1.2. Establecer el entorno de validación. VAL-SP 1.3. Establecer los procedimientos y los criterios de validación. VER-SP 1.2. Establecer el entorno de verificación. VER-SP 1.3. Establecer los procedimientos y los criterios de verificación.	-	-
MEA01.02: Establecer los objetivos de cumplimiento y rendimiento.	P	6.1	-	-	E	MA-SP 1.2. Especificar las medidas para tratar los objetivos de medición MA-SP 1.3. Especificar los procedimientos de recogida y de almacenamiento de datos OPD-SP 1.4. Establecer el repositorio de mediciones de la organización. VAL-SP 1.1. Seleccionar los productos para la validación.		

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	C	Control	C	Control	C	Control	C	Control
						VER-SP 1.1. Seleccionar los productos de trabajo para la verificación.		
MEA01.03: Recopilar y procesar los datos de cumplimiento y rendimiento.	P	6.1	-	-	E	MA-SP 1.4. Especificar los procedimientos de análisis MA-SP 2.1. Obtener los datos de la medición MA-SP 2.2. Analizar los datos de la medición MA-SP 2.3. Almacenar los datos y los resultados PPQA-SP 1.1. Evaluar objetivamente los procesos. PPQA-SP 1.2. Evaluar objetivamente los productos de trabajo. VAL-SP 2.1. Realizar la validación. VER-SP 2.1. Preparar las revisiones entre pares. VER-SP 2.2. Realizar las revisiones entre pares. VER-SP 3.1. Realizar la verificación.	E	4.4 Monitorear y Controlar el Trabajo del Proyecto 5.5 Validar el Alcance 5.6 Controlar el Alcance 6.7 Controlar el Cronograma

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
MEA01.04: Analizar e informar sobre el rendimiento.	P	6.2	-	-	E	MA-SP 2.2. Analizar los datos de la medición MA-SP 2.4. Comunicar los resultados. PPQA-SP 2.2. Establecer los registros. VAL-SP 2.2. Analizar los resultados de la validación. VER-SP 2.3. Analizar los datos de las revisiones entre pares. VER-SP 3.2. Analizar los resultados de la verificación.	E	4.4 Monitorear y Controlar el Trabajo del Proyecto
MEA01.05: Asegurar la implantación de medidas correctivas.	P	6.2	-	-	P	PPQA-SP 2.1. Comunicar y resolver las no conformidades.	-	-
MEA02.01: Supervisar el control interno.	-	-	P	A.18.2.2	-	-	-	-
MEA02.02: Revisar la efectividad de los controles sobre los procesos de negocio.	-	-	P	A.18.2.1	-	-	-	-
MEA02.03: Realizar autoevaluaciones de control.	-	-	P	A.18.2.3	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
MEA02.04: Identificar y comunicar las deficiencias de control.	-	-	-	-	-	-	-	-
MEA02.05: Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	-	-	P	A.18.2.1	-	-	-	-
MEA02.06: Planificar iniciativas de aseguramiento.	-	-	-	-	-	-	-	-
MEA02.07: Estudiar las iniciativas de aseguramiento.	-	-	-	-	-	-	-	-
MEA02.08: Ejecutar las iniciativas de aseguramiento.	-	-	-	-	-	-	-	-
MEA03.01: Identificar requisitos externos de cumplimiento.	-	-	P	A.18.1.1	-	-	-	-
MEA03.02: Optimizar la respuesta a requisitos externos.	-	-	P	A.18.1.2 A.18.1.3	-	-	-	-

COBIT 5	ISO20000-1:2011		ISO27002:2013		CMMI-DEV V1.3		PMBOK 5	
Práctica	**C**	**Control**	**C**	**Control**	**C**	**Control**	**C**	**Control**
MEA03.03: Confirmar el cumplimiento de requisitos externos.	-	-	P	A.18.1.4 A.18.1.5	-	-	-	-
MEA03.04: Obtener garantía del cumplimiento de requisitos externos.	-	-	P	A.18.1.4 A.18.1.5				

ANEXO II: Bibliografía

ISACA (2012). COBIT5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la empresa.

ISACA (2012). COBIT5, Procesos Catalizadores.

ISACA (2013). COBIT5, Información Catalizadora.

AENOR (2011). UNE-ISO/IEC 20000-1. Tecnología de la Información. Gestión del Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio (SGS).

ISO, IEC (2013). ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.

AENOR (2014). UNE-ISO/IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos.

Software Engineering Institute (2010). CMMI para Desarrollo, Versión 1.3. Mejora de los procesos para el desarrollo de mejores productos y servicios.

Project Management Institute (2013). GUÍA DE LOS FUNDAMENTOS PARA LA DIRECCIÓN DE PROYECTOS, Quinta edición.

Minguillón, Antonio (2010). La auditoría de sistemas de información integrada en la auditoría financiera. La perspectiva del sector público. Sindicatura de Comptes de la Comunitat Valenciana.

Gantz, Stephen (2014). The Basics of IT Audit. Purposes, Processes, and Practical Information. Elsevier Inc.

Piattini, Mario et Al (2001). Auditoría Informática, un enfoque práctico. Segunda edición. Alfaomega Grupo Editor S.A.

Senft, Sandra et Al (2009). Information Technology Control and Audit. Third Edition. AUERBACH PUBLICATIONS.

Garzás, Javier et Al (2011). Guía práctica de supervivencia en una auditoría CMMI®. Segunda Edición. Boletín de la Escuela Técnica Superior de Ingeniería Informática – Universidad Rey Juan Carlos.

IT Governance Institute (2008). Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business.

IT Governance Institute (2006). COBIT MAPPING: MAPPING OF PMBOK WITH COBIT 4.0.

IT Governance Institute (2008). COBIT® MAPPING: MAPPING OF ITIL® V3 WITH COBIT® 4.1.

ISACA (2011). COBIT® Mapping: Mapping of CMMI® for Development, V1.2, With COBIT® 4.1.

ISACA (2011). COBIT® Mapping: Mapping of ISO/IEC 20000 With COBIT® 4.1.

ISACA (2011). COBIT Mapping: Overview of International IT Guidance, 3rd Edition.