Universitat de les Illes Balears

Departament de Ciències Matemàtiques i Informàtica

Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros

Tesis doctoral para optar al grado de Doctor en Informática por la Universitat de les Illes Balears presentada por

Antoni Lluís Mesquida Calafat

Realizada bajo la dirección de la Doctora

Antònia Mas Pichaco

Palma, Mayo de 2012

Esta investigación ha contado con el soporte y la financiación del proyecto coordinado **TIN2010-20057-C03-03 "Simulación aplicada a la gestión de equipos, procesos y servicios" Sim4Gest**, proyecto enmarcado dentro del Programa Nacional de Proyectos de Investigación Fundamental (2011-2013), otorgado por el Ministerio de Ciencia e Innovación.

Dra. Antònia Mas Pichaco

Professora Titular d'Universitat
Departament de Matemàtiques i Informàtica
Universitat de les Illes Balears

HACE CONSTAR:

Que la memoria titulada *Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros* presentada por Antoni Lluís Mesquida Calafat para optar a la obtención del grado de Doctor en Informática, ha sido realizada bajo su dirección en el Departament de Ciències Matemàtiques i Informàtica de la Universitat de les Illes Balears y reúne la suficiente materia original para ser considerada como tesis doctoral.

Dra. Antònia Mas Pichaco	Antoni Lluís Mesquida Calafat
Directora de la tesis	Doctorando

Palma, Mayo de 2012

Al meu pare

Agradecimientos

Me gustaría agradecer en este espacio a todas las personas que me aprecian y que se han preocupado por mí durante la realización de este trabajo.

En primer lloc vull donar les gràcies a tots els bons amics que he anat trobant durant la meva vida. Gràcies pel vostre constant interès en la meva feina i pels vostres ànims. Gràcies pel sincer suport que he rebut de part vostra quan més ho he necessitat.

Gràcies també a la meva família, i en especial, als meus padrins, tios i cosins, per haver-me fet sentir sempre valorat i estimat.

Gràcies als companys i amics del departament de Ciències Matemàtiques i Informàtica. Gràcies a tu Adelaida, per compartir moltes més coses que un despatx.

Gràcies a tu, Emi, per haver compartit l'experiència doctoral, per haver-me fet costat quan més falta m'ha fet i per haver duit a ca nostra alegria i bons sentiments.

Gràcies a tu Xema, per haver-te convertit en un gran aliat. Moltes gràcies pels teus ànims i interès i per obrir-me noves oportunitats de creixement professional i personal.

Gràcies a la meva amiga Antònia, per confiar en jo i per haver-me guiat tant en el món de la recerca com en la meva feina a la Universitat. Gràcies per contagiar-me la teva vitalitat i per motivar-me a emprendre nous projectes. Moltes gràcies per preocupar-te sempre per mi i per estar al meu costat.

Gràcies a tu, Maties, pels teus ànims i consells sempre assenyats i per obrir-me camí en la vida. Moltes gràcies per ser per a mi un gran exemple a seguir i un bon mirall on veure'm reflectit.

Gràcies als meus pares Magdalena i Toni, per ensenyar-me les coses més importants de la vida, per fer-me veure que els esforços sempre tenen recompensa i que la feina ben feta, sempre hi estarà. Moltes gràcies per inculcar-me els valors que m'han ajudat a ser com som. Vos estim.

Toni

Índice general

Índice de tablas

Índice de figuras

Lista de acrónimos

CMMI: *Capability Maturity Model Integration*

ITIL: *Information Technology Infrastructure Library*

ITSM: *Information Technology Service Management*. Gestión de Servicios de TI

ISO: *International Organization for Standardization*

SGC: Sistema de Gestión de Calidad

SGI: Sistema de Gestión Integrado

SGSI: Sistema de Gestión de Seguridad de la Información

SGSTI: Sistema de Gestión de Servicios de TI

SPI: *Software Process Improvement*, Mejora de Procesos de Software

TI: Tecnologías de la Información

Capítulo 1. Introducción

En este capítulo se exponen la motivación y los antecedentes que han impulsado esta investigación. También se describen los objetivos fijados al inicio de este trabajo.

Este capítulo presenta de forma breve una aproximación a la solución planteada y las aportaciones realizadas durante el desarrollo de la tesis doctoral. Detalla cómo se ha aplicado y validado la solución propuesta. Finalmente, se indica la estructura seguida en esta memoria.

1.1. Motivación

El creciente interés de las empresas de desarrollo de software en mejorar sus procesos internos ha impulsado diferentes iniciativas para el desarrollo de modelos de integración o aplicación simultánea de estándares de calidad de software. Entre las normas y estándares internacionales relacionados con la calidad del software más demandados por las empresas de este sector, destacan los modelos de calidad de procesos de software, los modelos de gestión de servicios de Tecnologías de la Información (TI) y los modelos de gestión de seguridad de la información.

La mayoría de los modelos anteriores estructuran sus recomendaciones, directrices, requisitos o mejores prácticas bajo un enfoque basado en procesos. Gracias a este mismo enfoque, existen una gran cantidad de relaciones entre los diferentes modelos, así como muchos elementos y aspectos en común. Así pues, se pueden aprovechar estas relaciones y elementos comunes a la hora de implantar diferentes estándares de calidad, evitando duplicidades y reduciendo los esfuerzos y recursos necesarios para su implantación.

1.2. Antecedentes

Desde el año 2000, uno de los principales intereses de nuestro grupo de investigación, MiProSoft, ha sido promover la Mejora de los Procesos de Software (SPI, del inglés *Software Process Improvement*) en las empresas de desarrollo de software de nuestro entorno. Con este objetivo, desde el año 2002, nuestro grupo ha liderado diferentes programas de SPI en pequeñas y medianas empresas de las Islas Baleares a través del proyecto QuaSAR (*Qualitat del Software baleAR*) (Amengual and Mas 2003; Amengual and Mas 2007; Mas and Amengual 2003; Mas and Amengual 2004, Mas and Amengual 2005).

Estos programas de SPI han posibilitado, por una parte, el análisis del sector de desarrollo de software en las Islas Baleares y, por otra parte, la provisión de unas directrices para estas empresas para la mejora de sus procesos de software.

El proyecto QuaSAR fue un proyecto pionero a nivel regional puesto que en el año 2002 todavía no había ninguna empresa de desarrollo de software en nuestra comunidad con una certificación de calidad ISO 9001, pero también a nivel nacional, pues supuso la primera experiencia de implantación simultánea de las normas ISO 9001 e ISO/IEC 15504. Las 8 organizaciones participantes en este proyecto, además de obtener la

certificación de calidad ISO 9001, iniciaron un programa de mejora de procesos según el estándar internacional ISO/IEC 15504 que en la actualidad todavía sigue vigente en alguna de ellas (Mas et al. 2009).

Dado que la tendencia actual en las organizaciones se dirige también hacia nuevos dominios de interés, como pueden ser la gestión de servicios de TI o la gestión de la seguridad de la información, se plantea la necesidad de crear un modelo integrado de los estándares de gestión de TI más demandados por las empresas del sector de desarrollo de software.

Así pues, continuando con el estándar ISO/IEC 15504 como marco de referencia para la evaluación y mejora de procesos, y teniendo en cuenta que la mayoría de las organizaciones de desarrollo de software involucradas en iniciativas de calidad ya disponen de un sistema de gestión de la calidad de acuerdo con la norma ISO 9001, al iniciar esta nueva investigación se plantearon las siguientes cuestiones:

- ¿Considera el estándar ISO/IEC 15504 mejores prácticas de otras disciplinas, como la gestión de servicios de TI o la gestión de la seguridad de la información?
- ¿Cuáles son los procesos del ciclo de vida del software que se relacionan con los procesos propios de la gestión de servicios de TI?
- ¿Qué controles de gestión de seguridad de la información son aplicables a los procesos del ciclo de vida de software?
- ¿Qué elementos tiene en común el sistema de gestión de calidad de la norma ISO 9001 con el sistema de gestión de servicios de TI que define la norma ISO/IEC 20000-1? ¿Y con el sistema de gestión de seguridad de la información que define la norma ISO/IEC 270001?
- ¿Pueden integrarse los requisitos de los tres sistemas de gestión anteriores en un único sistema de gestión integrado?

1.3. Objetivos de la investigación

El propósito de esta tesis doctoral es desarrollar un modelo integrado para facilitar la implantación de los estándares de gestión de TI que combine las mejores prácticas de todas estas disciplinas y facilite la implantación de las normas relacionadas con ellas, reduciendo esfuerzos y evitando duplicidades. Este modelo pretende facilitar a las empresas de desarrollo de software la implantación de diferentes estándares de calidad de software y reducir los esfuerzos necesarios para su implantación, aprovechando las lecciones aprendidas y las metas ya conseguidas en iniciativas de calidad emprendidas con anterioridad.

Para cumplir este propósito, al inicio de esta investigación se plantearon los siguientes objetivos específicos:

- **Objetivo 1**: Realizar un estudio del estado actual de los estándares y normas de calidad más demandadas por las empresas del sector del desarrollo de software. Analizar las acciones llevadas a cabo por los modelos de calidad de procesos de software para ampliar su alcance de aplicación más allá de los procesos del ciclo de vida del software, y contemplar aspectos propios de la gestión de servicios de TI y de la gestión de la seguridad de la información.
- **Objetivo 2**: Analizar cuales de los procesos y mejores prácticas de gestión de servicios de TI del estándar ISO/IEC 20000 y de los controles de seguridad de la información del estándar ISO/IEC 27000 están relacionados o contemplados, total o parcialmente, con alguno de los procesos del ciclo de vida del software de la norma ISO/IEC 15504.
- **Objetivo 3**: Identificar los requisitos comunes del sistema de gestión de calidad de la norma ISO 9001, del sistema de gestión de servicios de TI de la norma ISO/IEC 20000-1 y del sistema de gestión de seguridad de la información de la norma ISO/IEC 27001. Identificar las iniciativas existentes para la integración de estos tres sistemas de gestión.
- **Objetivo 4**: Elaborar un Modelo Integrado de Estándares de Gestión de TI, compuesto por:
  - un sistema de gestión integrado según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001, y
  - un mapa de procesos que toma como base los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5 y los amplía a partir de las relaciones detectadas con los procesos de la norma ISO/IEC 20000-4 y los controles de la norma ISO/IEC 27002.
- **Objetivo 5**: Validar el Modelo Integrado de Estándares de Gestión de TI aplicándolo en empresas desarrollo de software. Mejorarlo a partir de las lecciones aprendidas de su aplicación.

1.4. Aproximación a la solución

La solución que se plantea en esta tesis doctoral se basa en la definición de un Modelo Integrado de Estándares de Gestión de TI que pueda ser utilizado para:

- Facilitar la implantación de las normas ISO/IEC 20000 y/o ISO/IEC 27001 en organizaciones que ya hayan iniciado un programa de SPI según la norma ISO/IEC 15504 y que hayan obtenido la certificación ISO 9001.
- Implantar de manera integrada los procesos de la norma ISO/IEC 15504-5 de tal modo que estos procesos ya contemplen las buenas prácticas requeridas por los estándares ISO/IEC 20000-1 e ISO/IEC 27001.

El Modelo Integrado de Estándares de Gestión de TI desarrollado es el resultado de un proceso formado por tres fases:

- **Fase I: Relaciones entre las normas ISO/IEC 15504 e ISO/IEC 20000**. Durante la primera fase se llevó a cabo un estudio exhaustivo de todas las relaciones y elementos comunes entre los procesos del ciclo de vida del software que define la norma ISO/IEC 15504-5 y los procesos de gestión de servicios que define la norma ISO/IEC 20000-4.
- **Fase II: Relaciones entre las normas ISO/IEC 15504 e ISO/IEC 27000**. Utilizando el mismo método de investigación que el utilizado en la primera fase, en esta segunda fase se llevó a cabo un estudio exhaustivo de todas las relaciones y elementos comunes entre los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5 y los controles de seguridad de la información que define la norma ISO/IEC 27002.
- **Fase III: Definición de un Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001**. En esta última fase se construyó el núcleo del modelo integrado, esto es, un sistema de gestión integrado que aúna los requisitos de los sistemas de gestión de las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001.

La figura 1.1 presenta el Modelo Integrado de Estándares de Gestión de TI desarrollado en esta tesis doctoral. Este modelo está formado por:

- un Sistema de Gestión Integrado (SGI) según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001 y
- un mapa de procesos que toma como base los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5 y los amplía con:
  - los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y
  - los controles de seguridad de la información de la norma ISO/IEC 27002.

Las intersecciones entre los elementos de la figura son proporcionales a las relaciones detectadas entre los procesos de cada norma. Mediante esta representación se ha querido mostrar el esfuerzo aproximado que debería realizar una organización que ha iniciado un programa de mejora de procesos según la norma ISO/IEC 15504 para implantar la normas ISO/IEC 20000-1 e ISO/IEC 27001.

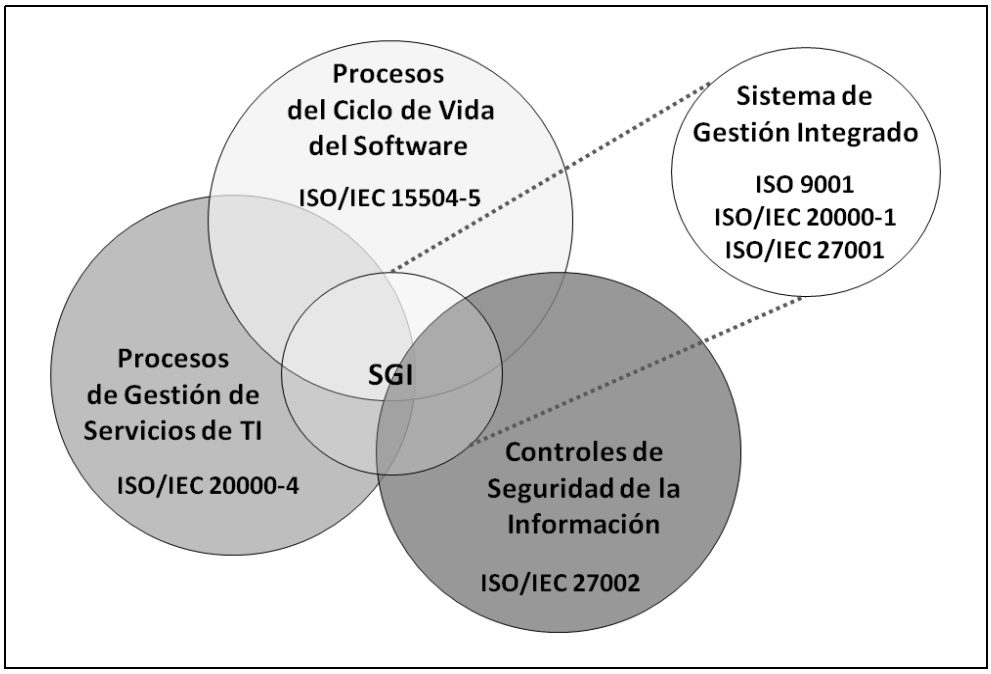

Figura 1.1. Modelo Integrado de Estándares de Gestión de TI

1.5. Aportaciones de la investigación

Las aportaciones a las organizaciones que podrán utilizar al aplicar la solución propuesta en esta tesis doctoral se describen a continuación:

- **Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5**. Este mapa de relaciones puede ser usado por:
  - organizaciones con un cierto nivel de madurez según ISO/IEC 15504 que estén interesadas en implantar uno o varios procesos del mapa de procesos de la norma ISO/IEC 20000-4, con el objetivo de conocer:
    - los esfuerzos de implantación que se puede ahorrar gracias a tener procesos de la norma ISO/IEC 15504-5 ya desplegados.

        - los esfuerzos adicionales necesarios para desplegar las buenas prácticas propias de la gestión de servicios de TI no cubiertas por los procesos del ciclo de vida del software ya implantados.
    - organizaciones que no han implantado las normas ISO/IEC 15504-5 e ISO/ISO 20000-4, pero que se plantean desplegar procesos de estas normas. Estas organizaciones podrán hacer uso de la comparativa para elegir de manera conjunta los procesos de ambas normas que desean implantar, y hacerlo de una manera integrada.

- ***ISO/IEC 15504 Security Extension***. Esta extensión de seguridad amplía el propósito y las prácticas básicas de los procesos de la norma ISO/IEC 15504-5 para que contemplen los objetivos y controles de seguridad de la norma ISO/IEC 27002. La *ISO/IEC 15504 Security Extension* puede ser usada por:
    - organizaciones con un cierto nivel de madurez según ISO/IEC 15504 que estén interesadas en implantar uno o varios controles de seguridad de la norma ISO/IEC 27002, con el objetivo de conocer los procesos de la norma ISO/IEC 15504-5 que pueden dar soporte a la implantación de cada control de seguridad de la norma ISO/IEC 27002.
    - organizaciones que no han implantado las normas ISO/IEC 15504-5 e ISO/ISO 27000, pero que se plantean hacerlo. Estas organizaciones podrán hacer uso de la extensión de seguridad para elegir de manera conjunta los procesos y controles de estas normas que desean implantar, y hacerlo de una manera integrada.

- **Guías para la implantación de sistemas de gestión integrados a partir de la norma ISO 9001**. Las dos guías desarrolladas definen directrices para facilitar a las organizaciones la implantación de sistemas de gestión integrados según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001.
    - La *Guía para la integración del Sistema de Gestión de Servicios de TI de la norma ISO/IEC 20000-1 con el Sistema de Gestión de Calidad de la norma ISO 9001* puede ser usada para facilitar la implantación del sistema de gestión de servicios de TI que propone la norma ISO/IEC 20000-1 de forma integrada con el sistema de gestión de calidad de la norma ISO 9001.

- La *Guía para la integración del Sistema de Gestión de Seguridad de la Información de la norma ISO/IEC 270001 con el Sistema de Gestión de Calidad de la norma ISO 9001* permite facilitar la implantación integrada del sistema de gestión de seguridad de la información de la norma ISO/IEC 27001 con el sistema de gestión de calidad de la norma ISO 9001.

- **Juego de mejora de procesos MiProJOC (www.miprojoc.com)**. Un juego de preguntas y respuestas que puede ser utilizado por los usuarios del nuevo modelo para repasar y consolidar los conceptos y aspectos teóricos de los estándares que integra.

1.6. Validez de la solución

Este trabajo se enmarca en el proyecto coordinado TIN2010-20057-C03-03 "Simulación aplicada a la gestión de equipos, procesos y servicios" Sim4Gest, proyecto enmarcado dentro del Programa Nacional de Proyectos de Investigación Fundamental (2011-2013), otorgado por el Ministerio de Ciencia e Innovación. La participación de los miembros del grupo de *Millora de Processos de Software (MiProSoft)* de la Universitat de les Illes Balears en este proyecto se centra en la definición de un modelo genérico de evaluación y mejora de los procesos de gestión de servicios TI.

Una vez concluida la elaboración de este modelo de gestión de servicios de TI, y atendiendo a la demanda de las organizaciones participantes en las diferentes ediciones del proyecto QuaSAR, se decidió ampliar este modelo para contemplar, además, los aspectos propios de la gestión de la seguridad de la información.

El Modelo Integrado de Estándares de Gestión de TI resultante de este trabajo de investigación ha sido aplicado a dos de las empresas participantes en la primera edición del proyecto QuaSAR.

Por otra parte, durante los últimos meses se ha iniciado la preparación de una nueva edición del proyecto QuaSAR 2012, formando un consorcio de seis empresas interesadas en conseguir una certificación según la norma ISO/IEC 20000-1. Sin embargo, el retraso de las convocatorias de ayudas públicas del Plan Avanza ha obligado a retrasar el inicio de esta nueva edición. Durante el desarrollo del proyecto QuaSAR 2012 se espera:

- Aplicar el Modelo Integrado de Estándares de Gestión de TI en las seis empresas participantes.

- Validar los productos desarrollados disponibles para las organizaciones. Estos productos son: el mapa de relaciones entre los procesos de las normas ISO/IEC 20000-4 e ISO/IEC 15504-5, la *ISO/IEC 15504 Security Extension,* las Guías para la implantación de sistemas de gestión integrados y el juego de mejora de procesos MiProJOC.
- Mejorar todos los resultados de esta tesis doctoral considerando las lecciones aprendidas en la aplicación en estas empresas de software.

1.7. Estructura de la tesis doctoral

Esta memoria se ha estructurado en ocho capítulos que se muestran a continuación.

Capítulo 1. Introducción: Es el capítulo actual, en el que se presenta el contexto de la investigación. Se define el problema en base a la situación actual y se recoge la motivación de la investigación. Además, se describen los objetivos de la investigación y se expone de forma breve una aproximación a la solución. También se detallan las aportaciones a la investigación y, por último, se describe cómo se ha aplicado la solución propuesta en este trabajo de investigación.

Capítulo 2. Estado del arte: Se estudia la situación actual de los estándares y modelos más demandados por las empresas de desarrollo de software. En primer lugar se ofrece una descripción de los estándares de calidad del software derivados de la norma ISO 9001. A continuación, se realiza una revisión de los modelos de calidad de procesos del ciclo de vida del software más utilizados en la actualidad, que son el modelo CMMI y el estándar internacional ISO/IEC 15504. Además, se presentan los modelos de gestión de servicios de TI más extendidos, como son ITIL y la norma ISO/IEC 20000. Finalmente, se introduce la serie ISO/IEC 27000 como familia de estándares de gestión de seguridad de la información.

Capítulo 3. Estudio de las relaciones entre los estándares ISO/IEC 20000 e ISO/IEC 15504: Se analizan las sinergias y elementos comunes entre los resultados de los procesos de gestión de servicios de TI definidos por la norma ISO/IEC 20000-4 y las prácticas básicas de los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5. Además, se presenta una revisión sistemática de la literatura que muestra iniciativas de mejora de procesos de gestión de servicios de TI basadas en el estándar internacional ISO/IEC 15504.

Capítulo 4. Estudio de las relaciones entre los estándares ISO/IEC 27000 e ISO/IEC 15504: Se analizan todas las relaciones existentes entre los controles de seguridad de la norma ISO/IEC 27002 y las prácticas básicas de la norma ISO/IEC

15504-5. Además, se presenta la *ISO/IEC 15504 Security Extension*, una extensión sobre los procesos de la norma ISO/IEC 15504-5 que detalla los cambios que son necesarios realizar para implantar los controles de seguridad relacionados.

Capítulo 5. Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001: Se describe un nuevo sistema de gestión integrado que amplía los requisitos del sistema de gestión de calidad de la norma ISO 9001 con los requisitos específicos del sistema de gestión de servicios de TI propuesto por la norma ISO/IEC 20000-1, y por los requisitos específicos del sistema de gestión de seguridad de la información propuesto por la norma ISO/IEC 27001. Además, se presentan las guías que se han elaborado para dar soporte a las organizaciones en la implantación del sistema de gestión integrado desarrollado.

Capítulo 6. Aplicación del Modelo Integrado de Estándares de Gestión de TI: Se describe la experiencia práctica y se exponen los resultados obtenidos de la aplicación del nuevo Modelo Integrado de Estándares de Gestión de TI en dos empresas de desarrollo de software reales.

Capítulo 7. Conclusiones y trabajo futuro: Se exponen las conclusiones de esta tesis doctoral y las posibles líneas futuras que se pueden abordar relacionadas con esta investigación. Se ofrece un resumen de las publicaciones relacionadas con esta investigación.

Capítulo 8. Referencias bibliográficas: Recoge las referencias a los trabajos consultados durante el desarrollo de este trabajo.

Finalmente, la memoria incluye unos anexos en los que se describe el protocolo utilizado para realizar revisiones sistemáticas de la literatura, y los productos de soporte para facilitar la utilización del modelo integrado desarrollado en esta investigación:

- Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5
- Mapa de relaciones entre los controles de seguridad de la norma ISO/IEC 27002 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5
- MiProJOC: el juego de mejora de procesos
- Guías para la implantación de sistemas de gestión integrados a partir de la norma ISO 9001

Capítulo 2. Estado del arte

En este capítulo se presenta la situación actual de los estándares basados en procesos más comúnmente demandados por las organizaciones de desarrollo de software.

Estos estándares ofrecen modelos para diferentes áreas de conocimiento: modelos de gestión de la calidad, modelos de calidad de procesos de software, modelos de gestión de servicios de tecnologías de la información y modelos de gestión de seguridad de la información.

Los estándares que se describen en este capítulo han sido creados para satisfacer las necesidades de diferentes áreas de conocimiento dentro del campo de la Ingeniería del Software. Todos los modelos analizados tienen un enfoque basado en procesos y, por lo tanto, proporcionan marcos, metodologías y directrices específicas para gestionar la implantación de los procesos que definen y para optimizar las operaciones de la organización que los aplica.

Este capítulo se ha estructurado de la siguiente manera:

- En el apartado 2.1 se presentan una serie de estándares de calidad cuyos principios básicos han sido aplicados a los objetivos propuestos por esta investigación. Estos estándares son la norma ISO 9001, ISO/IEC 90003, ISO/IEC 90005 e ISO/IEC 90006.
- En el apartado 2.2 se analizan los dos modelos de evaluación y mejora de procesos de software más extensamente utilizados, el modelo CMMI (*Capability Maturity Model Integration*) y el estándar ISO/IEC 15504 (SPICE).
- En el apartado 2.3 se introducen las iniciativas que han surgido para contemplar los procesos relacionados con la gestión de servicios de TI. Así pues, se presentan los dos estándares de gestión de servicios de TI más conocidos y usados en la actualidad, ITIL (*Information Technology Service Management*) y la norma ISO/IEC 20000. Además, se muestran las acciones llevadas a cabo para que los modelos de evaluación y mejora de procesos de software CMMI e ISO/IEC 15504 cubrieran este tipo de procesos.
- En el apartado 2.4 se introduce la serie ISO/IEC 27000 como familia de estándares de gestión de la seguridad de la información, centrando la atención en el sistema de gestión propuesto por la parte ISO/IEC 27001 y los controles de seguridad que se detallan en la parte ISO/IEC 27002.

2.1. Modelos de calidad

En esta sección se presentan las normas ISO 9001, ISO/IEC 90003, ISO/IEC TR 90005 e ISO/IEC CD 90006.

La norma ISO 9001:2008 *Quality management systems - Requirements* (ISO9001 2008) promueve la adopción de un enfoque basado en procesos y especifica los requisitos para desarrollar, implementar y mejorar un Sistema de Gestión de Calidad (SGC). ISO 9001:2008 está estructurada en ocho cláusulas. Las tres primeras tratan el alcance, la aplicación de la norma y las definiciones. Las cinco cláusulas restantes están orientadas a procesos y definen los requisitos para la implementación de un SGC.

La figura 2.1 muestra el SGC propuesto por la norma ISO 9001. Este sistema de gestión sigue el ciclo Planificar-Hacer-Verificar-Actuar (PDCA, del inglés *Plan-Do-Check-Act*), también conocido como el ciclo de Deming. PDCA es un método iterativo de gestión en cuatro pasos utilizado para el control y la mejora continua de procesos y productos. El ciclo PDCA es el principio de funcionamiento de la mayoría de los sistemas de gestión de las normas ISO.

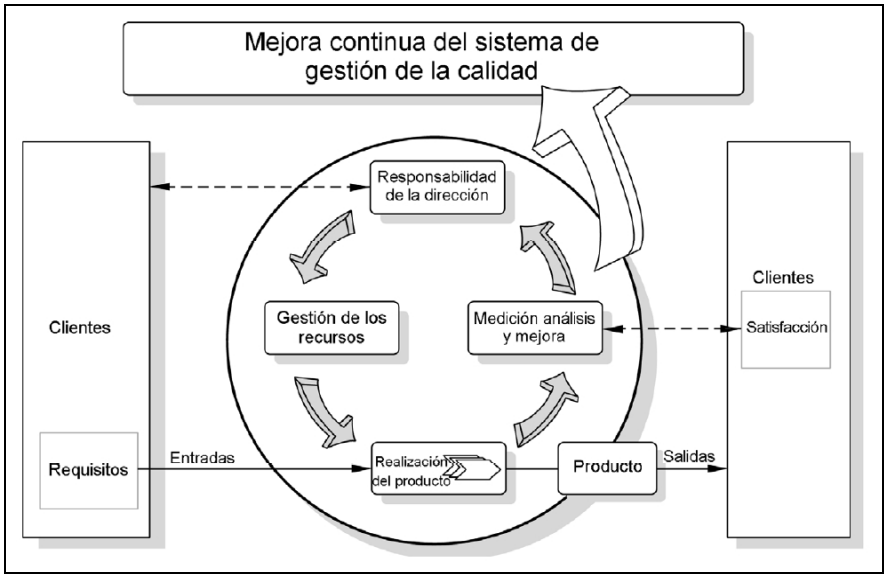

Figura 2.1. Sistema de gestión de calidad de la norma ISO 9001

La edición actual, ISO 9001:2008, sustituye a la tercera edición (ISO 9001:2000) que ha sido modificada para clarificar puntos en el texto y aumentar la compatibilidad con otras normas ISO. Esta norma permite a una organización integrar o alinear su SGC con los requisitos de otros sistemas de gestión.

Todos los requisitos de esta norma son genéricos y pretenden ser aplicables a cualquier tipo de organización, independientemente del tipo, tamaño y productos suministrados. Por este motivo, se han desarrollado normas específicas que constituyen una guía para la aplicación de esta norma en determinados dominios de interés. Para nuestra investigación se han considerado las guías ISO/IEC 90003, ISO/IEC 90005 e ISO/IEC 90006, puesto que todas ellas guardan relación con las áreas de la Ingeniería del Software y las Tecnologías de la Información.

- La norma ISO/IEC 90003:2004 *Software engineering - Guidelines for the application of ISO 9001:2000 to computer software* (ISO90003 2004) proporciona una guía para la aplicación de la norma ISO 9001 en la adquisición, suministro, desarrollo, operación y mantenimiento del software. Esta norma identifica todos

los aspectos que deben ser tratados independientemente de la tecnología, modelo de ciclo de vida, procesos de desarrollo, secuencia de actividades y estructura organizacional utilizados por la organización.

- La norma ISO/IEC TR 90005:2008 *Systems engineering - Guidelines for the application of ISO 9001 to system life cycle processes* (ISO90005 2008), publicada como informe técnico, proporciona una guía para la aplicación de la norma ISO 9001:2000 en la adquisición, suministro, desarrollo, operación y mantenimiento de sistemas y servicios de soporte relacionados.
- Con la intención de desarrollar una guía para la aplicación de la norma ISO 9001 a la gestión de servicios de TI, ISO inició en 2008 un nuevo proyecto denominado ISO/IEC CD 90006 *Information technology - Guidelines for the application of ISO 9001:2000 to IT service management*. Sin embargo, trascurridos dos años, el proyecto sigue todavía en desarrollo.

2.2. Modelos de calidad de procesos de software

Las iniciativas que han ido surgiendo en todo el mundo para la investigación en el área de la mejora de procesos han propiciado el desarrollo de diversos modelos que proponen diferentes métodos de evaluación de la capacidad de los procesos, diferentes maneras de representar las actividades necesarias para la mejora y diferentes maneras de guiar a la organización hacia la madurez.

Los modelos de evaluación y mejora de procesos de software permiten calcular la capacidad o madurez de todos los procesos que intervienen en el ciclo de vida del software, detectar los puntos fuertes y débiles de cada uno, y proponer un conjunto de actividades orientadas a guiar a la organización hacia la mejora continua de estos procesos. Cada uno de estos modelos proporciona un punto de partida para la homogeneización de los procesos, una terminología y un marco de actuación comunes, un campo de conocimiento derivado de su uso en toda una comunidad y una serie de directrices para priorizar las acciones de mejora surgidas a partir de una evaluación.

En los apartados 2.2.1 y 2.2.2 se analizan en detalle los dos grandes modelos de evaluación y mejora de procesos de software más utilizados actualmente, CMMI e ISO/IEC 15504 (SPICE). Aunque tradicionalmente estos dos modelos se han estado implantando en las empresas grandes, en los últimos años el interés por ellos en las pequeñas y medianas empresas ha ido creciendo considerablemente. Debido a que las características de estas empresas son, generalmente, muy diferentes a las de las grandes, se han creado modelos específicos para ellas, pero también se han realizado adaptaciones de los modelos CMMI y SPICE para facilitar su implantación en este tipo de empresas.

2.2.1. El modelo CMMI

El modelo CMMI surgió en el año 2000 como solución a todos los problemas de falta de integración y uso de múltiples modelos *Capability Maturity Model* (CMM).

El modelo CMM, también denominado CMM-SW, fue desarrollado por el *Software Engineering Institute* (SEI) junto con el centro de investigación gubernamental Mitre, como marco de referencia para la evaluación de la capacidad de los proveedores de software del gobierno de los Estados Unidos. En Septiembre de 1987 publicaron el primer resultado en forma de una breve descripción del proceso de madurez así como un cuestionario para detectar los puntos débiles de la empresa evaluada. Después de unos cuantos años de aplicación del primer modelo y refinamiento del mismo a partir de los resultados que se iban obteniendo en su aplicación en diferentes empresas, el SEI desarrolló y publicó la primera versión de CMM en 1991. Desde entonces, el modelo CMM se fue adaptando a múltiples disciplinas: Ingeniería de Sistemas, Ingeniería del Software, adquisición de software, desarrollo de procesos y de productos integrados, etc., derivando modelos diferentes.

Aunque se demostró la utilidad de estos modelos en numerosas organizaciones de sectores distintos, la utilización de múltiples modelos empezó a resultar problemática. Muchas empresas interesadas en aplicar sus iniciativas de mejora en diferentes secciones o departamentos de la organización, se encontraron con el problema de la utilización de modelos distintos, específicos para una disciplina concreta, con arquitecturas, contenidos y métodos de utilización distintos. Además, la aplicación de múltiples modelos no integrados resultaba demasiado costosa en términos de formación, evaluaciones y actividades de mejora. Con la intención de resolver toda esta problemática, el proyecto *CMM Integration* surgió con la intención de combinar tres modelos fuente:

- El *Capability Maturity Model for Software (SW-CMM) V2.0 draft C*
- El *Systems Engineering Capability Model (SECM)*
- El *Integrated Product Development Capability Maturity Model (IPD-CMM) V0.98*

Debido a la utilización del modelo CMMI en dominios de interés diferentes, el modelo fue agrupando sus mejores prácticas dando lugar al concepto de "constelaciones". Una constelación es una colección de componentes CMMI, entre los que se incluyen un modelo, materiales de formación y documentos relacionados con la evaluación, que proporcionan un marco de aplicación específico para un determinado dominio o área de interés. A partir de 2006, la arquitectura de los modelos CMMI fue mejorada para soportar múltiples

constelaciones y compartir las mejores prácticas entre constelaciones. Así pues, todos los modelos CMMI disponibles antes de 2006 fueron agrupados y considerados como parte de una primera constelación denominada *CMMI® for Development (CMMI-DEV)* (SEI 2010a)

Por otra parte, se empezaron a gestar dos constelaciones nuevas, una para servicios y otra para adquisiciones.

- *CMMI® for Services (CMMI-SVC)* (SEI 2010b)
- *CMMI® for Acquisition (CMMI-ACQ)* (SEI 2010c)

Con la publicación de CMMI V1.2, las tres constelaciones cobraron autonomía propia, dando lugar a tres modelos diferentes de CMMI. El día 1 de Noviembre de 2010 se publicó CMMI V1.3, que es la versión vigente en la actualidad. La figura 2.2 muestra las tres constelaciones o modelos CMMI V1.3.

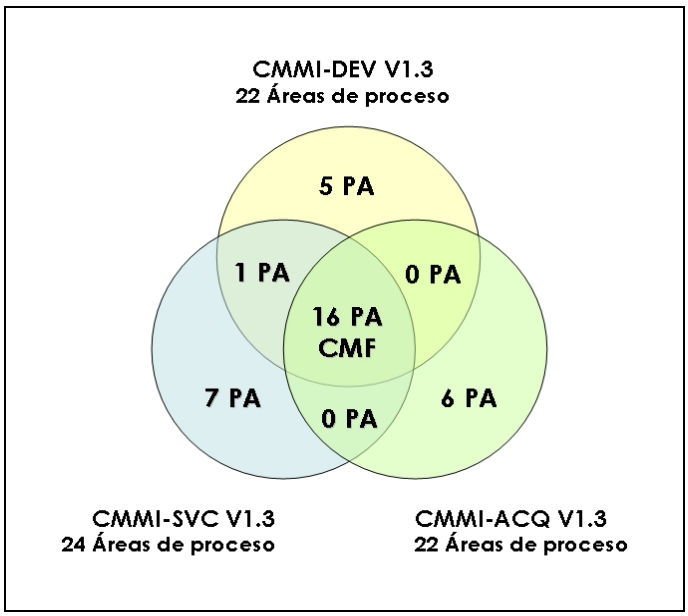

Figura 2.2. Constelaciones de CMMI V1.3

2.2.2. El estándar ISO/IEC 15504 (SPICE)

ISO/IEC 15504 *Information technology – Process assessment*, también denominado SPICE (*Software Process Improvement and Capability dEtermination*), es un estándar internacional que es aplicable a cualquier organización que quiera conocer y mejorar la capacidad de sus procesos, independientemente del tipo de organización. Su modelo bidimensional, caracterizado por una dimensión de procesos y una dimensión de capacidad, ofrece una base para la evaluación de la capacidad de los procesos y permite

reflejar los resultados obtenidos sobre una escala común, que puede usarse tanto para comprobar la evolución de una organización en el tiempo como para definir estrategias de mejora continua.

ISO/IEC 15504 no pretende fijar la manera de realizar los procesos en una organización, sino que valora su capacidad y ayuda a proponer medidas para aumentarla. Este estándar no indica en ningún momento en qué orden y de qué forma deben llevarse a cabo los procesos, se limita a definirlos y a caracterizarlos.

La primera versión del borrador apareció en Junio de 1995. Fue aplicado en numerosas empresas donde se fue revisando y refinando según el procedimiento habitual de desarrollo de estándares internacionales. Su primera publicación como informe técnico data del año 1998, y llevó por nombre ISO/IEC TR 15504. En base al conocimiento adquirido en la aplicación del Informe técnico en estas industrias, la comunidad internacional siguió con el proceso de revisión de la Norma, liberando entre los años 2003-06 las cinco primeras partes del nuevo estándar que se exponen a continuación.

- ISO/IEC 15504-1:2004. *Part 1: Concepts and vocabulary* (ISO15504 2004a). Es una parte informativa que constituye el punto de partida para la correcta utilización del estándar, proporcionando una guía de uso del mismo. Además, contiene un glosario de los términos y definiciones propios de la norma.
- ISO/IEC 15504-2:2003/Cor 1:2004. *Part 2: Performing an assessment* (ISO15504 2003). Es la única parte normativa en la que se definen los requisitos necesarios que deben cumplir tanto los modelos de procesos como los modelos de evaluación. Además, en esta parte, también se define un marco de medida para evaluar la capacidad de los procesos.
- ISO/IEC 15504-3:2004. *Part 3: Guidance on performing an assessment* (ISO15504 2004b). Establece una guía para el cumplimento de los requisitos que deben considerarse a la hora de llevar a cabo una evaluación y que se exponen en la parte normativa del estándar. Para ello, en esta parte se proporciona información acerca del proceso de evaluación, el marco de medida para la determinación de la capacidad de los procesos, el modelo de procesos y el modelo de evaluación de los mismos, herramientas para la evaluación y una guía sobre las competencias que deben poseer los evaluadores.
- ISO/IEC 15504-4:2004. *Part 4: Guidance on use for process improvement and process capability determination* (ISO15504 2004c). Proporciona una guía para determinar la capacidad de los procesos y realizar una evaluación con el propósito de mejorarlos. Para el caso específico de la mejora de procesos, los conceptos y principios expuestos en esta parte informativa de la norma resultan apropiados

para cualquier tipo y tamaño de organización, independientemente de sus objetivos de negocio y dominios de aplicación. En el caso de la determinación de la capacidad de los procesos, esta guía puede aplicarse en el marco de cualquier relación cliente-proveedor.

- ISO/IEC 15504-5:2006. *Part 5: An exemplar Process Assessment Model* (ISO15504 2006). Proporciona un modelo para la realización de una evaluación basada en el modelo de procesos ISO/IEC 12207:1995 Amd 1:2002 (ISO12207 2002) y Amd 2:2004 (ISO12207 2004) que define los procesos del ciclo de vida del software. El modelo de evaluación que se detalla en esta parte incluye un conjunto de indicadores para determinar la capacidad de los procesos. En Enero de 2012 se publicó una nueva versión de esta parte, llamada ISO/IEC 15504-5:2012 *Part 5: An exemplar software life cycle process assessment model* (ISO15504 2012), con el objetivo de alinearse al modelo de procesos de la nueva versión de la norma ISO/IEC 12207:2008 (ISO12207 2008).

Después de la publicación de estas cinco partes del estándar, la comunidad internacional inició el desarrollo de cinco partes más. Cuatro de ellas, las partes 6, 7, 9 y 10, han sido publicadas como informes técnicos (TR) o especificaciones técnicas (TS). La parte 8 se encuentra actualmente en fase de borrador de especificación técnica.

- ISO/IEC TR 15504-6:2008. *Part 6: An exemplar system life cycle process assessment model* (ISO15504 2008a). Proporciona un ejemplo de un modelo de evaluación para los proceso del ciclo de vida del sistema recogidos en la norma ISO/IEC 15288.
- ISO/IEC TR 15504-7:2008. *Part 7: Assessment of organizational maturity* (ISO15504 2008b). Esta parte del estándar amplía la evaluación de la capacidad de los procesos definiendo los requisitos para la madurez de una organización y proporciona un marco para la definición de modelos de madurez.
- ISO/IEC DTS 15504-8. *Part 8: An exemplar process assessment model for IT service management*. Se espera que esta parte defina un modelo de evaluación de los procesos de gestión de servicios de TI que recoge la norma ISO/IEC 20000-4.
- ISO/IEC TS 15504-9:2011. *Part 9: Target process profiles* (ISO15504 2011a). Proporciona directrices para establecer perfiles de procesos objetivo para determinar la capacidad y mejorar los procesos de la organización.
- ISO/IEC TS 15504-10:2011. *Part 10: Safety extension* (ISO15504 2011b). Proporciona las ampliaciones de seguridad y las posibles acciones de mejora de los procesos cuando el software/sistema en desarrollo está relacionado con la seguridad.

Según la información aparecida en el SPICE User Group (SPICEUG 2009), en la reunión de la ISO celebrada el 29 de Mayo de 2009 en Hyderabad (India) se produjo la aprobación por parte de la ISO de una nueva generación de estándares, denominada serie ISO 33001-99 *Process Assessment*, que reemplazará a las diferentes partes del estándar ISO/IEC 15504 y que incluirá algunas partes nuevas. Está nueva numeración dará lugar a los nuevos estándares que se muestran en la tabla 2.1.

Grupo	**Parte**		**Relación con ISO/IEC 15504**
Core Elements	33001	*Concepts & Terminology*	15504-1
	33002	*Requirements for Process Assessment*	15504-2
	33003	*Requirements for Process Measurement Frameworks*	
	33004	*Requirements for Process Reference, Process Assessment and Organizational Maturity Models*	
Guidance	33010	*Guide for performing assessments*	15504-3
	33011	*Guide for defining a documented assessment process*	
	33012	*Guide for constructing process measurement frameworks*	15504-4
	33013	*Guide for constructing process reference models, process assessment models and organisational maturity models for assessments*	15504-4
	33014	*Guide for process improvement*	
	33015	*Guide for process capability determination*	
	33016	*Body of Knowledge for Process Assessment*	
	33017	*Body of Knowledge for Process Improvement*	
Measurement Frameworks	33020	*Measurement Framework for assessment of process capability and organizational maturity*	15504-7
Documented Assessment Processes	33030	*Exemplar documented assessment process*	
Process Reference Models	33040	*Safety Extension*	15504-10
	33041	*High Maturity Extension*	
Process Assessment Models	33060	*Process Assessment Model for Software Life Cycle Processes*	15504-5
	33061	*Process Assessment Model for System Life Cycle Processes*	15504-6
	33062	*Process Assessment Model for IT Service Management Processes*	15504-8

Grupo	Parte		Relación con ISO/IEC 15504
	33063	*Process Assessment Model for Software Testing Processes*	
	33064	*Safety Extension*	
	33065	*High Maturity Extension*	
Organizational Maturity Models	33080	*Organizational Maturity Model for Software Engineering*	
	33081	*An Integrated Organizational Maturity Model for Software and Systems Engineering*	

Tabla 2.1. Partes de la serie ISO/IEC 33001-99

2.2.2.1. La dimensión de procesos. La norma ISO/IEC 12207

En el estándar ISO/IEC 15504, la dimensión de procesos viene representada por un Modelo de Referencia de Procesos (PRM, *Process Reference Model*) externo que define un conjunto de procesos caracterizados según su propósito y las salidas que generan. Para realizar una evaluación de procesos conforme con la norma ISO/IEC 15504-2 (parte normativa), se debe definir un Modelo de Evaluación de Procesos (PAM, *Process Assessment Model*) basado en un determinado PRM, que satisfaga los requisitos definidos en esta parte.

Nuestra investigación se ha centrado en los procesos del ciclo de vida del software. Para el caso particular de una evaluación de este tipo de procesos, en la parte ISO/IEC 15004-5 se detalla un PAM basado en el PRM proporcionado por la norma ISO/IEC 12207:1995/Amd 1:2002 & Amd 2:2004 *Information technology - Software life cycle processes* (ISO12207 2002; ISO12207 2004) que cumple con los requisitos normativos de la parte ISO/IEC 15504-2.

Asimismo, actualmente existen, o se encuentran en desarrollo, otras iniciativas para la evaluación de procesos definidos en PRM específicos para los sectores que se detallan a continuación:

- Procesos del ciclo de vida del sistema. Estudio a través de la norma ISO/IEC 15288.
- Software embebido para la automoción. A través de una iniciativa de *AutomotiveSPICE*.
- Software para dispositivos médicos. A través de una iniciativa denominada *MediSPICE*.

- Procesos de gestión de servicios de Tecnologías de la Información. A través de una iniciativa del *SPICE User Group*.
- Procesos de sistemas de gestión de calidad. A través de la iniciativa *SPICE for 9000 (S9K)*.
- *Human Centered Lifecycle Process*. Estudio a través de la norma ISO/IEC 18529.
- Procesos de desarrollo basado en componentes. Estudio a través del proyecto *OOSPICE* (*Object Oriented SPICE*).

La norma ISO/IEC 12207 define 48 procesos del ciclo de vida del software, agrupados en nueve grupos de procesos. La figura 2.3 muestra los procesos considerados por la norma ISO/IEC 12207, y que son los que utiliza la norma ISO/IEC 15504-5.

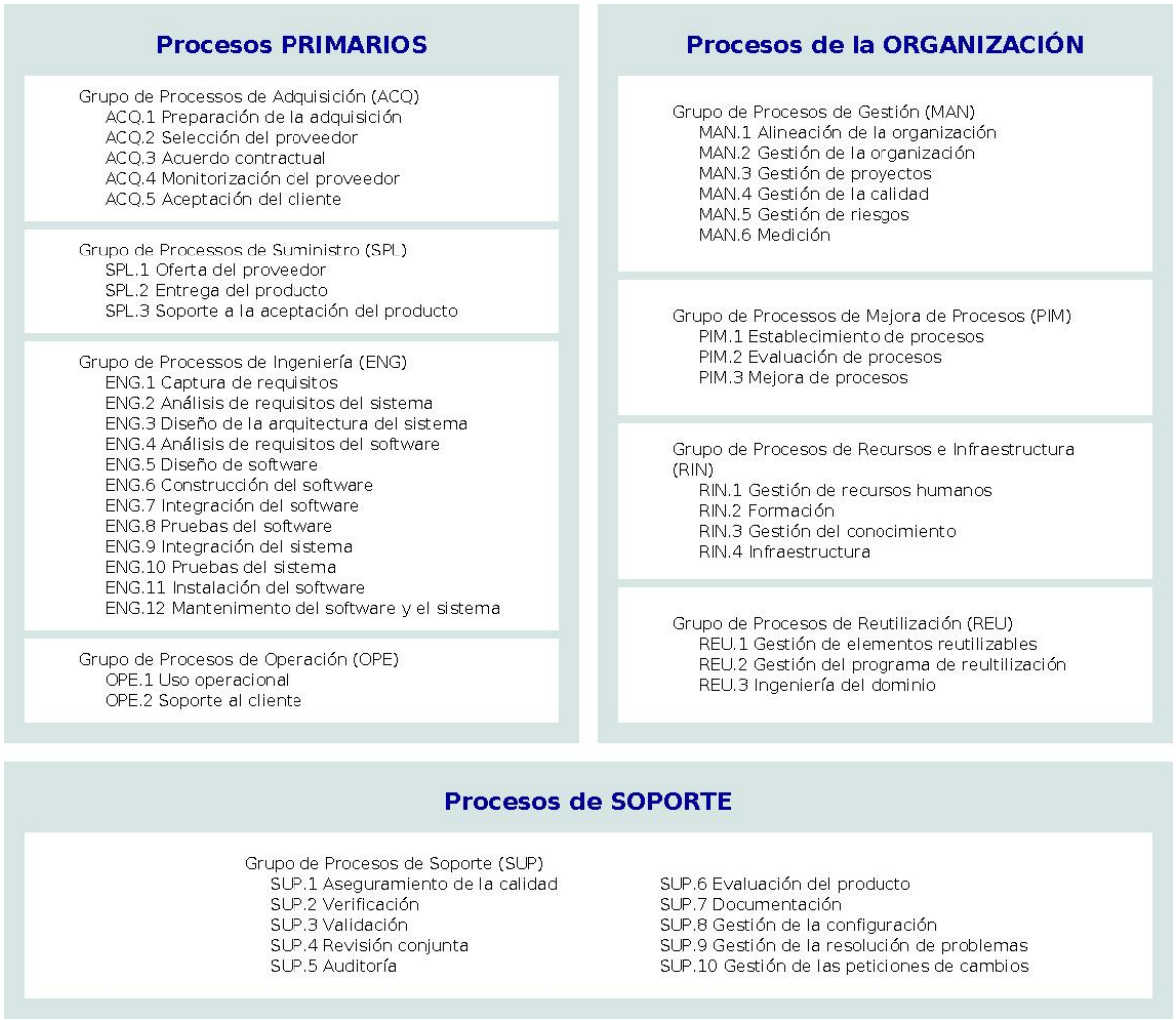

Figura 2.3. Categorías y grupos de procesos contemplados en ISO/IEC 12207

Este modelo de procesos agrupa los procesos que se realizan durante el ciclo de vida del software en tres categorías que, a su vez, están compuestas por grupos de procesos tal y como se describe a continuación:

- **Categoría de procesos primarios**. Contiene los siguientes grupos de procesos:
  - Adquisición (ACQ). Son los procesos que realiza el cliente para la adquisición de un producto o servicio.
  - Suministro (SPL). Abarca los procesos realizados por el proveedor tanto en la propuesta como en la entrega de un producto o servicio.
  - Ingeniería (ENG). Agrupa a los procesos que directamente especifican, implementan o mantienen el producto software, su relación con el sistema y la documentación del cliente.
  - Operación (OPE). Describe los procesos directamente relacionados con la transición del producto o servicio al cliente, y se ocupan del correcto uso y operación del mismo.
- **Categoría de procesos de soporte**. Formada por un único grupo de procesos:
  - Soporte (SUP). Contiene los procesos que pueden ser utilizados por cualquiera de los otros procesos incluyendo a la vez otros procesos de soporte, en determinadas partes o aspectos del ciclo de vida del software.
- **Categoría de procesos de la organización**. Agrupa los siguientes grupos de procesos:
  - Gestión (MAN). Está formada por los procesos que contienen prácticas que pueden ser utilizadas por cualquiera que gestione cualquier tipo de proyecto o de proceso del ciclo de vida del software.
  - Mejora del proceso (PIM). Está formada por los procesos que establecen, definen, despliegan e implantan, evalúan y mejoran los procesos que se realizan en la organización.
  - Recursos e Infraestructura (RIN). Describe los procesos que se realizan para dotar a la organización tanto de los recursos humanos, como de la infraestructura necesaria para que los otros procesos puedan realizarse de manera apropiada.
  - Reutilización (REU). Contiene los procesos directamente relacionados con la realización de acciones destinadas a explotar las oportunidades de reutilización.

La norma ISO/IEC 15504-5 etiqueta cada proceso con un identificador estándar. Este identificador se compone de una abreviatura de tres letras, correspondientes a las iniciales en inglés del grupo de procesos, y un número, que indica la posición del proceso dentro del grupo al que pertenece. Por ejemplo, ENG.5 identifica al proceso de diseño del software, que es un proceso del grupo de procesos de ingeniería.

La tabla 2.2 muestra el número de procesos y prácticas básicas de cada uno de los grupos de procesos que contiene la norma ISO/IEC 15504-5.

Grupos de procesos de la norma ISO/IEC 15504-5	Procesos	Prácticas básicas
Adquisición (ACQ)	5	23
Suministro (SPL)	3	25
Ingeniería (ENG)	12	66
Operación (OPE)	2	11
Gestión (MAN)	6	52
Mejora del Proceso (PIM)	3	23
Recursos e Infraestructura (RIN)	4	29
Reutilización (REU)	3	26
Soporte (SUP)	10	73
	48	**328**

Tabla 2.2. Procesos y prácticas básicas de la norma ISO/IEC 15504-5.

2.2.2.2. La dimensión de capacidad

La dimensión de capacidad define una escala de valoración para medir la capacidad de los procesos que consta de seis niveles, desde el nivel 0 hasta el nivel 5, y que se muestran en la tabla 2.3.

Escala	Descripción
Nivel 0 Incompleto	El proceso no existe o no se consigue su propósito. No pueden identificarse los productos o salidas del proceso.
Nivel 1 Realizado	Se alcanza el propósito del proceso en términos generales. El personal de la organización reconoce que el proceso se realiza cuando es necesario, pero no se hace de una forma planificada ni se realiza ningún seguimiento. Las salidas del proceso se identifican fácilmente y este hecho confirma que el proceso se realiza.

Escala	Descripción
Nivel 2 Gestionado	Se obtienen los productos del proceso, pero esta vez, de acuerdo con una planificación y realizándose un seguimiento. Estos productos se ajustan a unos estándares y a unas especificaciones de requisitos prefijadas. También se tienen definidos plazos y recursos. La principal diferencia con un proceso de nivel 1 es que, en este caso, se generan productos que cumplen completamente con los requisitos de calidad y lo hacen dentro de los plazos de tiempo y con los recursos establecidos.
Nivel 3 Establecido	El proceso se realiza y se gestiona utilizando procedimientos definidos según los principios de la Ingeniería del Software. Cada implementación de un proceso se hace utilizando procedimientos creados según un estándar y debidamente documentados. Además, se dispone de los recursos necesarios para alcanzar los propósitos establecidos. La principal diferencia con el nivel 2 es que se utiliza un proceso definido y con capacidad para alcanzar los resultados esperados.
Nivel 4 Predecible	La realización del proceso se gestiona de forma cuantitativa, es decir, se recogen medidas detalladas del nivel de realización del proceso y se analizan. Ésto permite mantener el proceso dentro de unos límites predefinidos, así como disponer de una mejor posición para poder cuantificar la capacidad del proceso y predecir su comportamiento. La principal diferencia con el nivel 3 es que ahora el proceso se lleva a término de manera consistente dentro de unos límites predefinidos.
Nivel 5 En optimización	La realización de un proceso se optimiza de forma continuada para que contribuya a alcanzar los objetivos de negocio de la organización. Se establecen objetivos cuantitativos de eficacia y eficiencia en la realización de los procesos, basados en los objetivos de negocio de la organización. Se lleva a cabo una supervisión continua de los procesos y se analizan los datos obtenidos. Ésto permite que los procesos estándares definidos dentro de la organización cambien dinámicamente, para adaptarse de forma efectiva a los actuales y futuros objetivos de la empresa. La principal diferencia con el nivel 4, es que ahora los procesos, definidos y estandarizados, cambian de manera dinámica, y se adaptan para satisfacer con eficacia los objetivos actuales y futuros del negocio.

Tabla 2.3. Dimensión de capacidad de ISO/IEC 15504

Cada nivel dentro de esta escala está caracterizado por unos atributos de proceso (PA, *Process Attribute*), cada uno de los cuales valora un aspecto particular de la capacidad del proceso. Dependiendo de los valores de estos atributos alcanzados por un proceso, éste se encontrará en una u otra posición de la escala. La tabla 2.4 muestra los nueve atributos considerados por el estándar. Estos atributos vienen identificados por las siglas PA seguidas de dos números que indican el nivel de capacidad y el número de atributo dentro de un mismo nivel, respectivamente.

Nivel	Atributo (PA)	Descripción
0	No hay atributos en este nivel	
1	Realización del proceso (PA.1.1)	Representa la medida de cuánto se alcanza el propósito de un proceso, transformando los productos de entrada en productos de salida.
2	Gestión de la realización (PA.2.1)	Representa el grado de gestión de la realización del proceso, para que se obtengan productos que cumplan los objetivos definidos.
	Gestión de los productos resultantes (PA.2.2)	Representa el grado de gestión de los productos resultantes producidos por los procesos.
3	Definición del proceso (PA.3.1)	Representa el nivel de realización del proceso, según el cual, el proceso utiliza una definición de proceso basada en un proceso estándar para conseguir sus objetivos.
	Implantación del proceso (PA.3.2)	Representa el nivel de adecuación de la implantación o despliegue efectivo del proceso estándar.
4	Medida del proceso (PA.4.1)	Representa el nivel en el que las medidas y los objetivos de los productos y de los procesos son utilizados para asegurar que la realización del proceso soporte el alcance de los objetivos definidos como apoyo a los objetivos de negocio.
	Control del proceso (PA.4.2)	Representa el nivel de control del proceso a través de la recopilación, análisis y uso de medidas de proceso y de producto, para corregir, en caso necesario, el rendimiento del proceso para conseguir los objetivos de proceso y de producto definidos.
5	Innovación del proceso (PA.5.1)	Representa el nivel de control de los cambios en la definición, gestión y realización del proceso, con el fin de alcanzar los objetivos de negocio fijados en la organización.
	Optimización del proceso (PA.5.2)	Representa el nivel bajo el cual se identifican e implantan los cambios en los procesos, para conseguir una mejora continua en el cumplimiento de los objetivos de negocio de la organización.

Tabla 2.4. Atributos de proceso asociados a los niveles de capacidad de ISO/IEC 15504

Para determinar si un proceso cumple un determinado nivel de capacidad es necesario calcular el porcentaje de cumplimiento de los atributos que identifican el nivel considerado. La escala de valoración de los atributos se compone de cuatro valores tal y como se muestra en la tabla 2.5. El estándar obliga a evaluar empezando desde el nivel 1 y, solamente en el caso de que los atributos de un determinado nivel sean ampliamente o completamente alcanzados, se permite la evaluación de un nivel superior.

Valores posibles del atributo		Grado de cumplimiento	Situación para determinar el grado de alcance del atributo
N	No alcanzado	0% - 15%	Indica una poca o nula evidencia de que se ha alcanzado este atributo en el proceso evaluado.
P	Parcialmente alcanzado	16% - 50%	Se evidencia una aproximación sistemática del alcance del atributo, pero algunas de sus características no se dan.
L	Ampliamente alcanzado	51% - 85%	Hay bastantes evidencias de que se alcanza el atributo, pero la realización del proceso diverge en alguna área.
F	Completamente alcanzado	86% - 100%	Hay evidencia de que el atributo se alcanza plenamente y de manera sistemática en el proceso evaluado y no hay debilidades importantes en la unidad organizacional en la que se ubica el proceso.

Tabla 2.5. Escala de valoración de los atributos de proceso según ISO/IEC 15504

2.3. Modelos de gestión de servicios de TI

Actualmente las organizaciones proveedoras de servicios de Tecnologías de la Información necesitan disponer de una gestión de servicios efectiva para cumplir las demandas de sus clientes. Para estas organizaciones ya no es suficiente apostar por la mejor tecnología, una orientación a procesos en el desarrollo de sus productos y en su propia organización interna, sino que también deben considerar la calidad de los servicios que proporcionan a sus clientes. El interés que la calidad de los servicios ofrecidos ha despertado en las organizaciones ha propiciado el nacimiento de una nueva disciplina, la Gestión de Servicios de Tecnologías de la Información (o ITSM del inglés *Information Technology Service Management*), que se centra en la perspectiva del cliente como principal aportación al negocio.

La gestión de servicios de TI es una disciplina orientada a procesos que combina la gestión de procesos y las mejores prácticas de la industria en una aproximación estandarizada con el objetivo de optimizar los servicios de TI. También se puede definir como el conjunto de capacidades organizacionales especializadas en proporcionar valor a los clientes en forma de servicios. Para proveer y gestionar de forma eficaz los servicios ofrecidos a lo largo de todo su ciclo de vida, resulta imprescindible definir y adoptar un conjunto de buenas prácticas. Si estas prácticas se agrupan y estructuran en procesos, este conjunto de procesos del área de provisión y gestión de servicios, puede utilizarse para ampliar el concepto de ciclo de vida de procesos de software hacia un ciclo de vida de producto completo, que abarque también todos los aspectos relacionados con la provisión y gestión de los servicios.

Con el objetivo de crear un marco único que agrupara todos los procesos relacionados con la gestión de los servicios han ido surgiendo diferentes iniciativas que se analizan en esta sección. Estas iniciativas se pueden clasificar en dos categorías bien distintas:

- Por una parte, algunas de estas iniciativas se han centrado en la creación y desarrollo de nuevos modelos, normas o estándares específicos de calidad de servicios. Dentro de este grupo, las más destacadas son ITIL (*Information Technology Infrastructure Library*) e ISO/IEC 20000, que se exponen en los apartados 2.3.1 y 2.3.2 de este capítulo, respectivamente.
- Por otra parte, dada la orientación a procesos en la gestión de servicios de TI, otros proyectos se han basado en la ampliación de los modelos de evaluación y mejora de procesos, como CMMI e ISO/IEC 15504 (SPICE), para cubrir los procesos de gestión de servicios. Estas actuaciones se describen en el apartado 2.3.3 de este capítulo.

Finalmente, en el apartado 2.3.4 se ofrece, a modo de resumen, una comparativa de todas estas iniciativas, mostrando las principales características de cada una de ellas.

2.3.1. ITIL (*Information Technology Infrastructure Library*)

ITIL es un conjunto de buenas prácticas de gestión de servicios, desarrollado por la *Office of Government Commerce* del Reino Unido y aceptado en todo el mundo como estándar de facto. ITIL se centra en la medida continua y en la mejora de la calidad de los servicios ofrecidos, tanto desde la perspectiva del negocio, como desde la perspectiva del cliente.

La versión inicial de ITIL, publicada entre 1989 y 1995, estaba compuesta por 31 libros que cubrían todos los aspectos de la gestión de servicios. Esta versión inicial fue revisada y reemplazada, entre 2000 y 2004 por ITIL V2, formada por sólo siete libros. En junio de 2007, ITIL V2 fue sustituida por una versión mejorada y consolidada, ITIL V3. El principal cambio que incorpora ITIL V3 respecto de la versión anterior, es que pasa de una estructura basada en procesos, a una estructura basada en el ciclo de vida de los servicios. La figura 2.4 muestra el ciclo de vida de los servicios de ITIL V3.

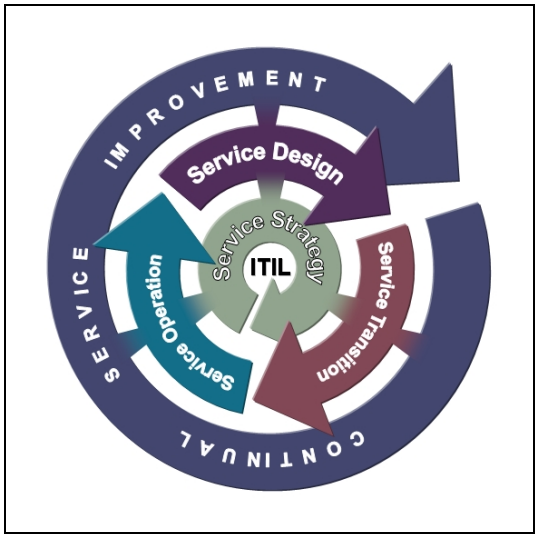

Figura 2.4. Ciclo de vida de los servicios de ITIL V3

ITIL V3 consta de cinco libros de referencia, cuyos propósitos se exponen a continuación.

- *Service Strategy* (OGC 2007a). Proporciona una guía, tanto a los proveedores de servicios de TI como a sus clientes, con la intención de ayudarles a operar y prosperar a largo plazo, mediante el establecimiento de una estrategia de negocio bien definida.
- *Service Design* (OGC 2007b). Ofrece pautas para el diseño de servicios apropiados e innovadores. Incluyendo la arquitectura, procesos, políticas y documentación, para satisfacer los requisitos de negocio, actuales y futuros, acordados.
- *Service Transition* (OGC 2007c). Aporta directrices para implantar todos los aspectos del servicio, no sólo su aplicación y uso en circunstancias normales. Se debe asegurar que el servicio puede operar en circunstancias previsibles extremas o anómalas, y que se dispone de un soporte a fallos o errores.
- *Service Operation* (OGC 2007d). Ofrece una guía para proveer los niveles de servicio acordados a los usuarios y clientes y gestionar las aplicaciones, tecnología e infraestructura necesarias para dar soporte a la provisión de los servicios.
- *Continual Service Improvement* (OGC 2007e). Ayuda a evaluar y mejorar de manera continuada la calidad de los servicios y la madurez global del ciclo de vida de los servicios y de los procesos subyacentes.

Las buenas prácticas de gestión de servicios de ITIL V3 son las que recoge la norma ISO/IEC 20000. Si bien esta norma no incluye formalmente el planteamiento de ITIL V3, sí que describe un conjunto integrado de procesos de gestión de servicios que están alineados y son complementarios a los procesos definidos en ITIL V3. Se podría decir que cada uno de los libros de ITIL ofrece una información más ampliada y una guía de buenas prácticas sobre las áreas que se tratan en la norma ISO/IEC 20000.

2.3.2. La norma ISO/IEC 20000

La norma ISO/IEC 20000 *Information technology – Service management* es un estándar de calidad de procesos de gestión de servicios de TI que promueve la adopción de un enfoque de procesos integrados para una provisión eficaz de servicios gestionados que satisfaga los requisitos del negocio y de los clientes. Actualmente, la norma ISO/IEC 20000 se compone de cinco partes. Tres de ellas, las partes 3, 4 y 5, han sido publicadas como informes técnicos (TR).

- ISO/IEC 20000-1:2011. *Part 1: Service management system requirements* (ISO20000 2011). Esta parte define los requisitos para que un proveedor de servicios pueda planificar, establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un sistema de gestión de servicios de TI. Estos requisitos comprenden el diseño, transición, provisión y mejora de los servicios.
- ISO/IEC 20000-2:2012. *Part 2: Guidance on the application of service management systems* (ISO20000 2012). Proporciona directrices para la implantación de un sistema de gestión de servicios de TI basado en los requisitos de la norma ISO/IEC 20000-1. Incluye ejemplos y sugerencias para interpretar y aplicar la norma ISO/IEC 20000-1.
- ISO/IEC TR 20000-3:2009. *Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1* (ISO20000 2009). Ofrece orientaciones sobre la definición del alcance, la aplicación y la demostración de la conformidad de los proveedores de servicios que pretenden satisfacer los requisitos de la norma ISO/IEC 20000-1
- ISO/IEC TR 20000-4:2010. *Part 4: Process reference model* (ISO20000 2010a). Describe un modelo de referencia de procesos de gestión de servicios de TI. Estos procesos son los mínimos necesarios para satisfacer los requisitos de la norma ISO/IEC 20000-1.
- ISO/IEC TR 20000-5:2010. *Part 5: Exemplar implementation plan for ISO/IEC 20000-1* (ISO20000 2010b). Ofrece un ejemplo de aproximación incremental a la adopción de la norma ISO/IEC 20000-1 en tres fases secuenciadas.

2.3.2.1. El sistema de gestión de servicios de TI. La norma ISO/IEC 20000-1

La norma ISO/IEC 20000-1 define el conjunto de requisitos necesarios para proveer un sistema de gestión, que incluye las políticas y el marco de trabajo, para hacer posible la implementación y gestión efectiva de todos los servicios de TI. Este Sistema de Gestión de Servicios de TI (SGSTI) se basa en el conocido ciclo PDCA e ilustra las relaciones entre los procesos de gestión de servicios. La figura 2.5 muestra el SGSTI propuesto por la norma ISO/IEC 20000.

ISO/IEC 20000-1:2011 está estructurada en nueve cláusulas. Las tres primeras cláusulas tratan el alcance, la aplicación de la norma y las definiciones. La cláusula cuatro define los requisitos generales de un SGSTI. La cláusula cinco define los requisitos para el diseño y la transición de nuevos servicios o servicios modificados. Las cláusulas seis a nueve están orientadas a procesos y definen los procesos de provisión, control, resolución y relaciones.

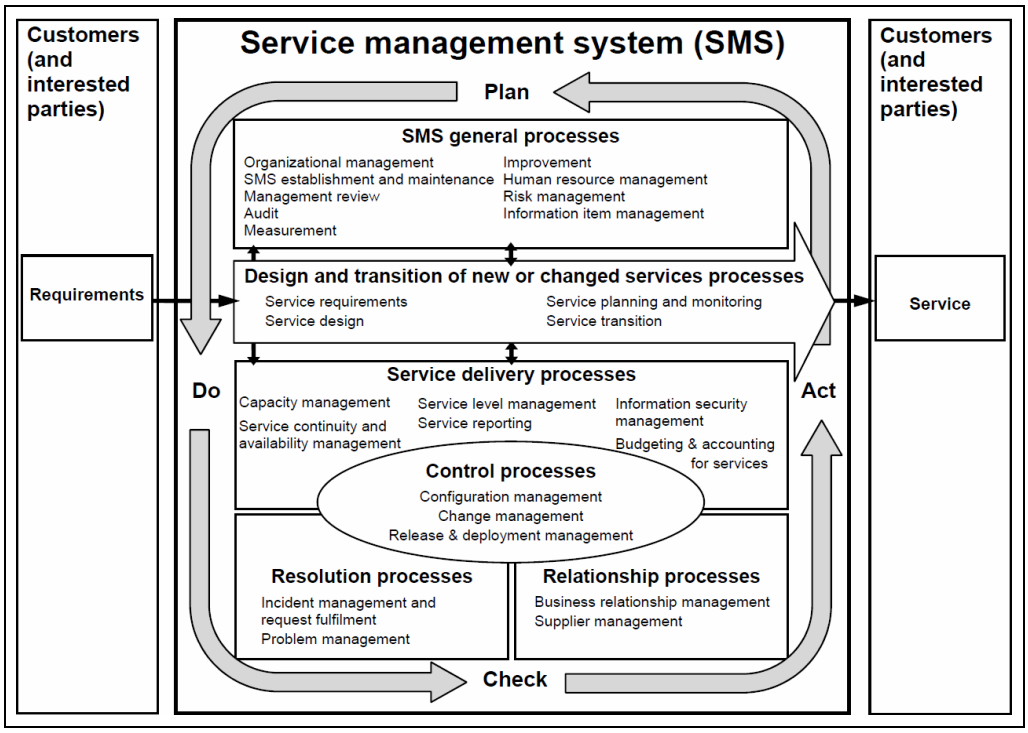

Figura 2.5. Sistema de gestión de servicios de TI de la norma ISO/IEC 20000

2.3.2.2. El Modelo de Referencia de Procesos. La norma ISO/IEC 20000-4

La norma ISO/IEC 20000-4 define el modelo de referencia de procesos de gestión de servicios de TI. Este modelo se compone de 26 procesos estructurados en las seis categorías de procesos que se muestran a continuación. Para cada proceso, esta norma define un propósito y diversos resultados, que son los efectos observables derivados de la consecución del propósito del proceso.

- **Procesos generales del SGS**. Contiene los siguientes nueve procesos: Auditoría, Gestión de recursos humanos, Mejora, Gestión de la información, Revisión de la dirección, Medición, Gestión organizativa, Gestión de riesgos y Establecimiento y mantenimiento del SGS.
- **Procesos de diseño y transición de nuevos servicios o servicios modificados**. Contiene los siguientes cuatro procesos: Diseño del servicio, Planificación y monitorización del servicio, Requisitos del servicio y Transición del servicio.
- **Procesos de provisión del servicio**. Contiene los siguientes seis procesos: Elaboración del presupuesto y contabilidad de los servicios de TI, Gestión de la capacidad, Gestión de la seguridad de la información, Gestión de la continuidad y disponibilidad del servicio, Gestión del nivel de servicio y Generación de informes del servicio.
- **Procesos de control**. Contiene los siguientes tres procesos: Gestión de cambios, Gestión de la configuración y Gestión de la entrega y del despliegue.
- **Procesos de resolución**. Contiene los siguientes dos procesos: Gestión de incidentes y cumplimiento de peticiones y Gestión de problemas.
- **Procesos de relaciones**. Contiene los siguientes dos procesos: Gestión de las relaciones con el negocio y Gestión de suministradores.

La tabla 2.6 muestra el número de procesos y resultados de cada una de las categorías de procesos que contiene la norma ISO/IEC 20000-4.

Categorías de procesos de la norma ISO/IEC 20000-4	Procesos	Resultados
Procesos generales del SGS	9	52
Procesos de diseño y transición de nuevos servicios o servicios modificados	4	28
Procesos de provisión del servicio	6	39
Procesos de control	3	19

Categorías de procesos de la norma ISO/IEC 20000-4	Procesos	Resultados
Procesos de resolución	2	11
Procesos de relaciones	2	15
	26	**164**

Tabla 2.6. Procesos y resultados de la norma ISO/IEC 20000-4

2.3.3. La gestión de servicios de TI en los modelos de madurez

Los modelos de madurez de procesos más conocidos y usados, el modelo CMMI y el estándar internacional ISO/IEC 15504, han sufrido cambios para contemplar los aspectos relacionados con la gestión de servicios. Así pues, el modelo CMMI creó un modelo propio con las áreas de proceso específicas de la gestión de servicios, mientras que la norma ISO/IEC 15504 se encuentra en proceso de actualización, con el objetivo de alinearse con el estándar de gestión de servicios ISO/IEC 20000.

2.3.3.1. La creación del modelo CMMI-SVC

El modelo del SEI específico para la gestión de servicios de TI, *CMMI for Services* (CMMI-SVC) (SEI 2010b) surgió en el año 2006, con la publicación de CMMI V1.2. CMMI-SVC incluye una colección de mejores prácticas para la gestión de servicios de TI, ofreciendo unas directrices para la aplicación del modelo en una organización proveedora de servicios. Las mejores prácticas de CMMI-SVC se centran en actividades para la provisión de servicios de calidad a los clientes y usuarios finales.

CMMI-SVC contiene 24 áreas de proceso. 16 de estas áreas de proceso pertenecen al *CMMI Foundation Model* (CMF), 7 son específicas de gestión de servicios y el área de proceso restante, es compartida con el modelo CMMI-DEV.

2.3.3.2. La alineación de la norma ISO/IEC 20000 con la norma ISO/IEC 15504

La norma ISO/IEC 15504 está siendo ampliada para cubrir los procesos de gestión de servicios. En ese sentido, y aunque no se dispone aún de información precisa de su contenido, el subcomité JTC 1/SC 7, responsable del estándar ISO/IEC 15504, trabaja en la nueva Parte 8: ISO/IEC DTS 15504-8: *An exemplar process assessment model for IT service management*. Esta parte incluirá un Modelo de Evaluación de Procesos de gestión de servicios (PAM), basado en el Modelo de Procesos de Referencia (PRM) que define la parte ISO/IEC TR 20000-4:2010 (ISO2000 2010a).

Después de la aprobación de la serie 33001-99 (ver tabla 2.1), que sustituirá a las diferentes partes del estándar ISO/IEC 15504, se prevé que la Parte 15504-8 se convierta en la futura Parte 31062 *Process Assessment Model for IT Service Management Processes*.

2.3.4. Relaciones entre los modelos de gestión de servicios de TI

La tabla 2.7 ofrece un resumen de las principales características de las cuatro normas y estándares de gestión de servicios de TI que se han descrito en la sección 2.3.

	Modelos específicos de gestión de servicios de TI		**Ampliación de modelos de madurez**	
	ITIL	ISO/IEC 20000	CMMI SVC	ISO/IEC 15504-8
Desarrollado por	*Office of Government Commerce (OGC)*	*International Organization for Standardization (ISO)*	*Software Engineering Institute (SEI)*	*International Organization for Standardization (ISO)*
Sitio web oficial	www.itil-officialsite.com	www.iso.org	www.sei.cmu.edu/cmmi	www.iso.org
Carácter	Privado	Público	Privado	Público
Versión vigente	V 3	2010	V 1.3	No publicado
Fecha de aparición de la versión vigente	Junio 2007	Diciembre 2010	Noviembre 2010	No publicado
Arquitectura del estándar	5 libros. Cada uno representa un área del ciclo de vida del servicio.	5 partes, tres de ellas publicadas como informes técnicos.	CMMI-SVC es una de las tres constelaciones del modelo CMMI.	ISO/IEC 15504-8 se encuentra en proceso de elaboración.
Procesos que abarca cada norma	27 procesos	26 procesos, agrupados en 6 categorías	24 áreas de proceso, agrupadas en 4 categorías	Pendientes de definición
Modelo de certificación acreditado	Certificación de profesionales: • *Foundation level* • *Intermediate level* • *ITIL Expert* • *ITIL Master*	Certificación de empresas. Evaluación por evaluadores acreditados. Pendiente de definición en España.	Certificación de empresas. Evaluación por evaluadores acreditados por el SEI.	Certificación de empresas. Evaluación por evaluadores acreditados. Pendiente de definición.

Tabla 2.7. Principales características de los estándares de gestión de servicios de TI

2.4. Modelos de gestión de seguridad de la información

En las empresas de desarrollo de software, así como en cualquier otra compañía, la información se ha convertido en un activo muy importante y, como cualquier otro activo importante, requiere una protección especial. De hecho, la información debe ser adecuadamente protegida con independencia de su formato o modo de transmisión. El principal objetivo de la gestión de la seguridad de la información es proteger convenientemente la información de accesos, usos, revelaciones, modificaciones o destrucciones no autorizadas.

La implantación de estándares de gestión de la seguridad de la información se ha convertido en una prioridad de las organizaciones para asegurar su continuidad, minimizar los posibles daños y maximizar el retorno de la inversión y las oportunidades de negocio. En este apartado se introduce el estándar de gestión de seguridad de la información ISO/IEC 27000.

2.4.1. La serie ISO/IEC 27000

La serie ISO/IEC 27000 *Information technology - Security techniques*, también conocida como "la familia de estándares de gestión de seguridad de la información", proporciona una serie de recomendaciones y mejores prácticas sobre gestión de la seguridad de la información, gestión de riesgos y controles, en el contexto de un Sistema de Gestión de Seguridad de la Información (SGSI).

La serie ISO/IEC 27000 consta de un gran número de partes, algunas de ellas disponibles y otras aún en fase de desarrollo. De todos modos, existe un conjunto de partes publicadas que se consideran básicas y que son las que se muestran en la tabla 2.8.

Norma	Título
ISO/IEC 27000:2009	*Information security management systems - Overview and vocabulary*
ISO/IEC 27001:2005	*Information security management systems - Requirements*
ISO/IEC 27002:2005	*Code of practice for information security management*
ISO/IEC 27003:2010	*Information security management system implementation guidance*
ISO/IEC 27004:2009	*Information security management - Measurement*
ISO/IEC 27005:2011	*Information security risk management*
ISO/IEC 27006:2011	*Requirements for bodies providing audit and certification of information security management systems*

Tabla 2.8. Normas básicas de la serie ISO/IEC 27000

La tabla 2.9 recoge otras partes de la serie ISO/IEC 27000 diseñadas con un propósito específico, ya sea ofrecer directrices para la auditoría, proporcionar guías de aplicación de la gestión de la seguridad de la información para dominios de interés concretos u ofrecer ayuda para la aplicación de determinadas técnicas relacionadas con la gestión de la seguridad. Algunas de estas partes se encuentran en desarrollo.

Propósito	**Norma**	**Estado**
Ayuda para auditoría	ISO/IEC 27007:2011 *Guidelines for information security management systems auditing*	Publicada en 2011
	ISO/IEC TR 27008:2011 *Guidance for auditors on information security controls*	Publicada en 2011
Guías sectoriales	ISO/IEC 27010:2012 *Information security management for inter-sector and inter-organizational communications*	Publicada en 2012
	ISO/IEC 27011:2008 *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*	Publicada en 2008
	ISO 27799:2008 *Health informatics - Information security management in health using ISO/IEC 27002*	Publicada en 2008
	ISO/IEC DIS 27013 *Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*	En curso
Ayudas en diferentes técnicas	ISO/IEC 27031:2011 *Guidelines for information and communication technology readiness for business continuity*	Publicada en 2011
	ISO/IEC FDIS 27032 *Guidelines for cybersecurity*	En curso
	ISO/IEC 27033-1:2009 *Network security - Part 1: Overview and concepts* ISO/IEC 27033-3:2010 *Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues* ISO/IEC 27033-2, ISO/IEC 27033-4, ISO/IEC 27033-5, ISO/IEC 27033-6 e ISO/IEC 27033-7	Publicada en 2009 Publicada en 2010 En curso
	ISO/IEC 27034-1:2011 *Application security - Part 1: Overview and concepts* ISO/IEC 27034-2, ISO/IEC 27034-3, ISO/IEC 27034-4 e ISO/IEC 27034-5	Publicada en 2011 En curso
	ISO/IEC 27035:2011 *Information security incident management*	Publicada en 2011
	ISO/IEC WD 27036 *Information security for supplier relationships*	En curso
	ISO/IEC DIS 27037 *Guidelines for identification, collection, acquisition and preservation of digital evidence*	En curso
	ISO/IEC WD 27038 *Specification for Digital Redaction*	En curso

Tabla 2.9. Normas específicas de la serie ISO/IEC 27000

2.4.1.1. El sistema de gestión de seguridad de la información. La norma ISO/IEC 27001

La norma ISO/IEC 27001:2005 *Information security management systems – Requirements* (ISO27000 2005a) promueve la adopción de un enfoque basado en procesos y especifica los requisitos para la creación, implantación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) documentado, dentro del contexto de las actividades empresariales de la organización y de los riesgos que ésta afronta. Los requisitos establecidos en esta norma son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño y naturaleza.

ISO 27001:2005 está estructurada en ocho cláusulas. Las tres primeras cláusulas tratan el alcance, la aplicación de la norma y las definiciones. Las cláusulas cuatro a ocho están orientadas a procesos y definen los requisitos para la implementación y mejora de un SGSI.

Esta norma internacional sigue el ciclo PDCA, que se aplica para estructurar todos los procesos del sistema de gestión de seguridad de la información. La figura 2.6 muestra el SGSI propuesto por la norma ISO/IEC 270001, el cual, a partir de los requisitos y expectativas de seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios, produce los elementos de salida que responden a dichos requisitos y expectativas.

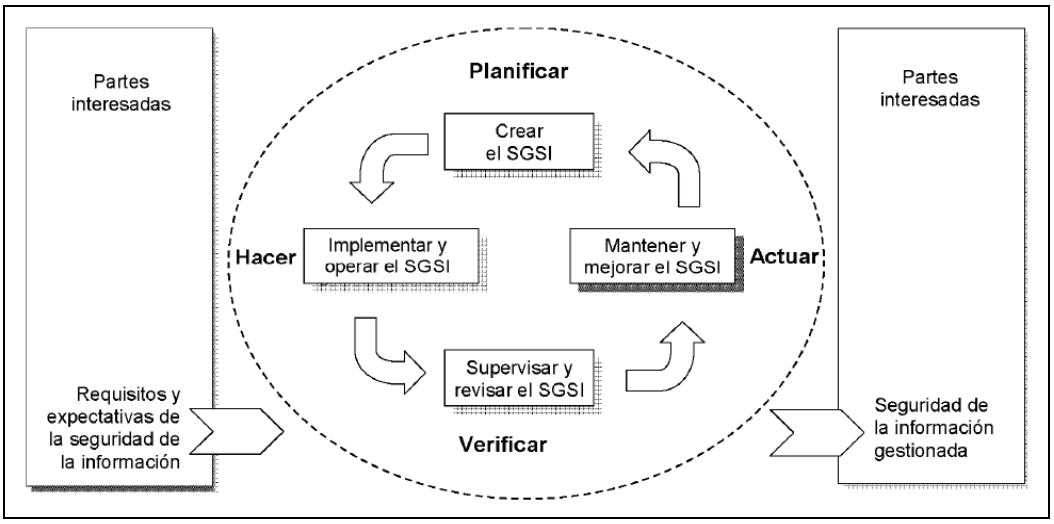

Figura 2.6. Sistema de gestión de seguridad de la información de la norma ISO/IEC 27001

2.4.1.2. Los controles de seguridad de la información. La norma ISO/IEC 27002

La norma ISO/IEC 27002:2005 *Code of practice for information security management* (ISO27000 2005b), anteriormente conocida como ISO/IEC 17799, establece las directrices y los principios generales para iniciar, implantar y mantener la gestión de la seguridad de la información en una organización. Esta norma pretende ser una guía práctica para desarrollar estándares organizacionales de seguridad y prácticas de gestión de la seguridad efectivas, así como para fortalecer la confianza a la hora de llevar a cabo actividades interorganizacionales.

Los objetivos y controles de la norma ISO/IEC 27002 proporcionan una guía general sobre las metas de gestión de la seguridad de la información más comúnmente aceptadas. Como se puede ver en la tabla 2.10, esta norma contiene 11 cláusulas de controles con un total de 39 categorías y 133 controles de seguridad.

Cláusulas	Categorías	Controles
5 Política de seguridad	1	2
6 Aspectos organizativos de la seguridad de la información	2	11
7 Gestión de activos	2	5
8 Seguridad ligada a los recursos humanos	3	9
9 Seguridad física y ambiental	2	13
10 Gestión de comunicaciones y operaciones	10	32
11 Control de acceso	7	25
12 Adquisición, desarrollo y mantenimiento de los sistemas de información	6	16
13 Gestión de incidentes de seguridad de la información	2	5
14 Gestión de la continuidad del negocio	1	5
15 Cumplimiento	3	10
Total	**39**	**133**

Tabla 2.10. Estructura de la norma ISO/IEC 27002

Cada categoría contiene un objetivo, que expone aquello que se pretende conseguir, y uno o más controles de seguridad que pueden ser aplicados para satisfacer el objetivo. La descripción de cada control se estructura en tres campos diferentes: descripción del control, directrices para su implantación y otra información adicional.

Capítulo 3. Estudio de las relaciones entre los estándares ISO/IEC 20000 e ISO/IEC 15504

Durante los últimos años, muchas empresas de desarrollo de software han considerado la mejora de sus procesos como un factor clave para tener éxito. Recientemente, estas empresas han empezado a mostrar, también, un especial interés por los estándares de gestión de servicios de TI.

Como primer paso en la construcción del modelo integrado, en este capítulo se examinan las relaciones existentes entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000 y los procesos del ciclo de vida del software que define la norma ISO/IEC 15504-5.

El análisis del sector de desarrollo de software en las Islas Baleares llevado a cabo durante las sucesivas ediciones del proyecto QuaSAR ha permitido comprobar como las empresas de este sector, además de seguir reconociendo la importancia de mejorar sus procesos de software, parecen haber puesto una especial atención a los procesos de gestión y provisión de servicios. Para las empresas de desarrollo de software es fundamental que sus clientes se formen una opinión positiva sobre los productos o servicios que reciben, y que éstos satisfagan todas sus necesidades y expectativas. Por esta razón, estas empresas también desean cubrir los procesos de gestión de servicios de TI y adoptar las mejores prácticas propuestas por esta disciplina.

Este capítulo se corresponde con la **Fase I de la construcción del Modelo Integrado de Estándares de Gestión de TI**. En él se estudian las sinergias y elementos comunes entre las normas ISO/IEC 15504 e ISO/IEC 20000. Más concretamente, se analizan todas las posibles relaciones entre las prácticas básicas de la norma ISO/IEC 15504-5 y los resultados de los procesos de la norma ISO/IEC 20000-4. La figura 3.1 muestra de manera gráfica el objetivo de esta Fase I.

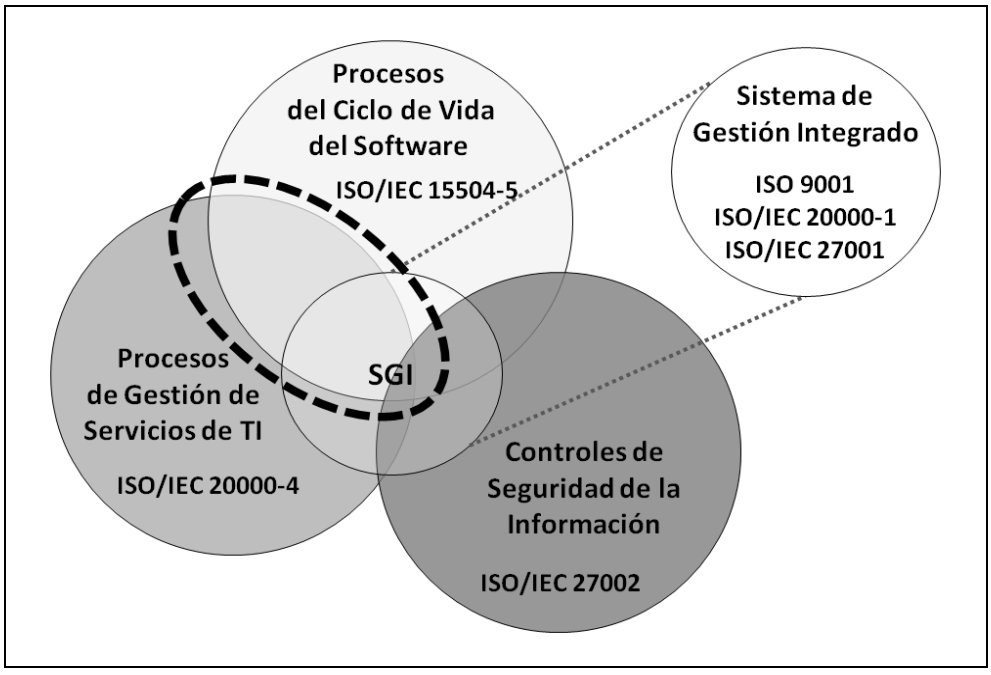

Figura 3.1. Fase I de la construcción del Modelo Integrado de Estándares de Gestión de TI

Debido a que uno de los objetivos de esta tesis doctoral era analizar las acciones llevadas a cabo para ampliar el alcance de aplicación de la norma ISO/IEC 15504 para contemplar los aspectos propios de la gestión de servicios de TI, se creyó conveniente realizar, en primer lugar, una revisión sistemática de la literatura para detectar todas las

iniciativas existentes de programas de mejora de procesos de gestión de servicios de TI basados en la norma ISO/IEC 15504. La sección 3.1 presenta esta revisión sistemática. En la sección 3.2 se define el método utilizado para realizar la comparativa entre los estándares ISO/IEC 15504-5 e ISO/IEC 20000-4. En la sección 3.3 se definen los tipos de relaciones detectadas entre ambos. En la sección 3.4 se muestran todas las relaciones detectadas entre los resultados de los procesos de la norma ISO/IEC 20000-4 y las prácticas básicas de la norma ISO/IEC 15504-5. Finalmente, en la sección 3.5 se analizan los resultados obtenidos y las conclusiones extraídas de esta investigación.

3.1. Revisión sistemática de iniciativas de mejora de procesos de gestión de servicios de TI según ISO/IEC 15504

Esta sección presenta una revisión sistemática de la literatura que trata la mejora de procesos de gestión de servicios de TI según la norma ISO/IEC 15504. Esta investigación ha sido llevada a cabo utilizando el protocolo de revisión sistemática que se presenta en el anexo A.

3.1.1. Formulación de la pregunta

Cada uno de los elementos que el protocolo propone describir fue específicamente definido con el objetivo de identificar estudios que traten iniciativas de mejora de procesos de gestión de servicios basadas en el estándar ISO/IEC 15504.

- Problema: Las empresas de desarrollo de software no sólo están interesadas en la mejora de sus procesos de software, sino también en la calidad de los servicios que proveen a sus clientes. Los modelos de mejora de procesos de software podrían ser ampliados para incluir los procesos de gestión de servicios de TI.
- Pregunta: ¿Qué iniciativas de programas de mejora de procesos de gestión de servicios de TI basadas en la norma ISO/IEC 15504 existen?
- Palabras clave y sinónimos: Mejora de Procesos de Software, *Software Process Improvement (SPI)*, Gestión de Servicios de TI, *IT Service Management (ITSM)*, ISO/IEC 15504 (SPICE).
- Intervención: Analizar la mejora de procesos de gestión de servicios de TI según ISO/IEC 15504.
- Control: No hay datos iniciales para esta revisión sistemática.
- Efecto: Identificar todas las iniciativas, marcos y modelos para la mejora de procesos de gestión de servicios de TI desarrollados de acuerdo con la norma ISO/IEC 15504.

- Métrica de salida: El número de iniciativas, marcos y modelos identificados.
- Población: El conjunto de propuestas de investigación relacionadas con la mejora de procesos de gestión de servicios de TI y con la norma ISO/IEC 15504 que hayan sido publicadas en la lista de fuentes seleccionadas para llevar a cabo la revisión sistemática.
- Aplicación: Empresas interesadas en evaluar y mejorar sus procesos de gestión de servicios de TI dentro de una iniciativa de mejora de procesos de software basada en ISO/IEC 15504. Investigadores que trabajan en modelos de mejora de procesos de software y, más concretamente, en la norma ISO/IEC 15504 o en estándares de gestión de servicios de TI.
- Diseño experimental: No se aplicará ningún método de análisis estadístico.

3.1.2. Selección de las fuentes

Las fuentes seleccionadas para ejecutar las búsquedas de estudios primarios se listan en la tabla A.1 del anexo A. A partir de las palabras clave definidas, y haciendo combinaciones con los conectores lógicos "AND" y "OR", se obtuvieron las cadenas de búsqueda que se muestran en la tabla 3.1.

Cadenas de búsqueda
(15504 OR SPICE) AND (ITSM OR "IT service" OR "service")
(ITSM OR "IT service" OR "service") AND (improvement OR assessment) AND (15504 OR SPICE)
(15504 OR SPICE) AND "service" AND (ITIL OR 20000 OR "CMMI-SVC")

Tabla 3.1. Cadenas de búsqueda para la revisión sistemática

3.1.3. Selección de los estudios

Los criterios que permitieron evaluar los estudios para decidir si debían ser seleccionados (Criterios de Inclusión, CI) o descartados (Criterios de Exclusión, CE) se muestran en la tabla 3.2.

Criterio	Descripción
CI1	Incluir artículos cuyo título esté relacionado con la mejora de procesos de gestión de servicios de TI según la norma ISO/IEC 15504.
CI2	Incluir artículos que contengan palabras clave que coincidan con aquellas definidas en la cadena de búsqueda.
CI3	Incluir artículos cuyo resumen esté relacionado con el tema en consideración.

Criterio	Descripción
CI4	Incluir artículos que contengan información relacionada con la definición o aplicación de modelos de mejora de procesos de gestión de servicios de TI.
CE1	Excluir aquellos artículos que se refieran a la mejora de procesos de gestión de servicios de TI y a la norma ISO/IEC 15504 de forma separada, sin mostrar ninguna relación entre ambos temas.
CE2	Excluir artículos duplicados.

Tabla 3.2. Criterios para la inclusión y exclusión de estudios

El proceso seguido para obtener y evaluar los estudios primarios de acuerdo con los criterios de inclusión y exclusión definidos se ilustra como un diagrama de flujo en la figura A.1 del anexo A.

Con respecto a la selección de los estudios primarios, el análisis del título y las palabras clave fueron los principales criterios de inclusión. En caso de que esta información no fuera suficiente para decidir sobre la inclusión o la exclusión del estudio, se analizó el resumen y, cuando fue necesario, el texto completo. La tabla 3.3 muestra la distribución de los estudios obtenidos de cada fuente de búsqueda. Como resultado de la ejecución de la revisión sistemática, inicialmente se obtuvieron 1.944 estudios para una evaluación posterior (ver la columna de "Descubiertos").

Fuente	Fecha de búsqueda	Descubiertos	Relevantes	No repetidos	Primarios
ACM Portal	25/07/2011	15	0	0	0
IEEE Computer Society Digital Library	25/07/2011	98	3	2	2
IEEE Xplore	25/07/2011	43	2	0	0
Springer Link	26/07/2011	178	9	3	3
ScienceDirect	25/07/2011	106	0	0	0
Wiley InterScience	25/07/2011	11	1	0	0
CiteSeerX	26/07/2011	99	2	1	1
IET Digital Library	26/07/2011	0	0	0	0
ISI Web of Knowledge	26/07/2011	39	4	2	2
Google Scholar	26/07/2011	778	42	30	9
SPICE	27/07/2011	211	8	4	4
EuroSPI	27/07/2011	366	11	7	7
	Total	**1944**	**82**	**49**	**28**

Tabla 3.3. Distribución de los estudios obtenidos por fuente de búsqueda

Después de aplicar los criterios de inclusión CI1, CI2, CI3 y CI4, definidos en la tabla 3.3, sólo 82 de los 1944 artículos descubiertos fueron considerados como artículos relevantes. Aplicando el criterio CE2 para la exclusión de artículos duplicados, se obtuvieron 49 artículos. De éstos, después de aplicar el criterio CE1, finalmente se seleccionaron 28 como estudios primarios. Estos resultados son los que se muestran en la última fila de la tabla 3.4. La lista completa con los 28 estudios primarios seleccionados se muestra en la tabla 3.4.

Estudios primarios obtenidos por la revisión sistemática		**Autores**
1	Sustainable Service Innovation Model: A Standardized IT Service Management Process Assessment Framework (Barafort and Rousseau 2009)	B. Barafort, A. Rousseau
2	Benefits resulting from the combined use of ISO/IEC 15504 with the Information Technology Infrastructure Library (ITIL) (Barafort et al. 2002)	B. Barafort, B. Di Renzo, O. Merlan
3	ITIL Based Service Management measurement and ISO/IEC 15504 process assessment: a win-win opportunity (Barafort et al. 2005)	B. Barafort, B. Di Renzo, V. Lejeune, S. Prime, J.-M. Simon
4	Modeling and Assessment in IT Service Process Improvement (Barafort et al. 2008a)	B. Barafort, D. Jezek, T. Mäkinen, S. Stolfa, T. Varkoi, I. Vondrak
5	A transformation process for building PRMs and PAMs based on a collection of requirements - Example with ISO/IEC 20000 (Barafort et al. 2008b)	B. Barafort, A. Renault, M. Picard, S. Cortina
6	SPiCE in Action - Experiences in Tailoring and Extension (Cass et al. 2002)	A. Cass, C. Völcker, P. Sutter, A. Dorling, H. Stienen
7	Integration of service management with CMMI® and SPICE (Cater-Steel 2007)	A. Cater-Steel
8	IT Service Departments Struggle to Adopt a Service-Oriented Philosophy (Cater-Steel 2009)	A. Cater-Steel
9	Process assessment for use in very small enterprise: the NOEMI assessment methodology (Di Renzo and Feltus 2003)	B. Di Renzo, C. Feltus
10	Collaborative management for ICT process improvement in SME: experience report (Di Renzo et al. 2004)	B. Di Renzo, C. Feltus, S. Prime
11	Quantifying Criticality of Dependability-Related IT Organization Processes in CobiT (Goldschmidt et al. 2009)	T. Goldschmidt, A. Dittrich, M. Malek
12	Managing the Alignment between Business and Software Services Requirements from a Capability Model Perspective (Grandry et al. 2008)	E. Grandry, E. Dubois, M. Picard, A. Rifaut
13	Assessing IT Service Management Processes with AIDA - Experience Feedback (Hilbert and Renault 2007)	R. Hilbert, A. Renault
14	TickIT Plus - the Future of TickIT! (Irving 2008)	D. Irving
15	ISO/IEC 15504 and ITIL (Kramer 2008)	A. Kramer

Estudios primarios obtenidos por la revisión sistemática		Autores
16	A service extension for SPICE? (Malzhan 2007)	D. Malzahn
17	Assessing - learning - improving, an integrated approach for self assessment and process improvement systems (Malzhan 2009)	D. Malzahn
18	SPICE Assessments for IT Service Management according to ISO/IEC 20000-1 (Nehfort 2007)	A. Nehfort
19	Comparison of CMMI-SVC and ISO20000 - A Case Study (Nevalainen and Johansson 2008)	R. Nevalainen, M. Johansson
20	Towards Mature IT Services (Niessink and Van Vliet 1998)	F. Niessink, H. Van Vliet
21	How to Improve Process Models for Better ISO/IEC 15504 Process Assessment (Picard et al. 2010)	M. Picard, A. Renault, S. Cortina
22	ITSM Process Assessment Supporting ITIL (Henry Tudor 2009)	Public Research Centre Henri Tudor: B. Barafort, V. Betry, S. Cortina, M. Picard, M.St-Jean, A. Renault, O. Valdés
23	TIPA: 7 years experience with SPICE for IT Service Management (Renault and Barafort 2011)	A. Renault, B. Barafort
24	Goal-Driven Requirements Engineering for Supporting the ISO 15504 Assessment Process (Rifaut 2005)	A. Rifaut
25	Maturity model for IT operations (MITO) (Scheuing et al. 2000)	A. Q. Scheuing, K. Frühauf, W. Schwarz
26	TIPA to keep ITIL going and going (St-Jean 2009)	M. St-Jean
27	How to evaluate benefits of Tudor's ITSM Process Assessment? (St-Jean and Mention 2009)	M. St-Jean, A.-L. Mention
28	Proactive elicitation of software process improvements (Varkoi and Makinen 2008)	T. Varkoi, T. Makinen

Tabla 3.4. Estudios primarios obtenidos por la revisión sistemática

3.1.4. Extracción de la información

En la tabla 3.5 se muestran los criterios para extraer la información de los estudios primarios seleccionados (Criterios de Inclusión de la información (Ci_{inf}).

Criterio	Descripción
$CI1_{inf}$	Identificar las metodologías, técnicas, métodos y procedimientos existentes para la mejora de procesos de gestión de servicios de TI.
$CI2_{inf}$	Recopilar información sobre las iniciativas o modelos utilizados para evaluar o mejorar procesos de gestión de servicios de TI.
$CI3_{inf}$	Recopilar información sobre las estrategias seguidas por las organizaciones de desarrollo de software para la mejora de los procesos de gestión de servicios de TI.

Criterio	Descripción
$CI4_{inf}$	Recopilar información sobre los procesos mejorados y los factores clave para la mejora exitosa de procesos de gestión de servicios de TI en las organizaciones de desarrollo de software.

Tabla 3.5. Criterios para la inclusión de la información de los estudios primarios

Mediante el formulario de extracción de la información que se muestra en el anexo A se registraron los comentarios, las impresiones y las ideas más importantes de cada estudio primario.

3.1.5. Resumen de los resultados

Este apartado presenta los datos resultantes del análisis de los 25 estudios primarios obtenidos después de la ejecución de la revisión sistemática. En primer lugar se muestra una clasificación de los estudios primarios seleccionados en cuatro categorías diferentes. En segundo lugar se muestran los estándares usados en estos estudios para la mejora de procesos de gestión de servicios de TI. En tercer lugar, se presentan los nuevos modelos de mejora de procesos de gestión de servicios de TI que han aparecido para satisfacer la demanda de las organizaciones de gestionar los servicios que proveen. En cuarto lugar, se muestra la tendencia del interés por la mejora de procesos de gestión de servicios de TI. Finalmente, se muestra la distribución de los esfuerzos o iniciativas de mejora de estos procesos por países.

3.1.5.1. Clasificación de los estudios primarios

Después de la extracción de la información relevante de cada uno de los estudios primarios, fue posible determinar que estos estudios podían ser clasificados en las cuatro categorías que muestra la tabla 3.6.

Categoría		Estudios primarios
1	Análisis de la necesidad de evaluar y mejorar los procesos de gestión de servicios de TI.	7, 8, 14, 17, 20, 25
2	Combinación del marco propuesto por la norma ISO/IEC 15504 con otros marcos de mejora de procesos de gestión de servicios de TI.	2, 5, 12, 15, 16, 24
3	Desarrollo de un modelo, marco o aproximación basada en la norma ISO/IEC 15504 para la mejora de procesos de gestión de servicios de TI.	1, 3, 4, 6, 9, 11, 18, 19, 21, 22, 28
4	Resultados de la aplicación de un modelo de mejora de procesos de gestión de servicios de TI.	10, 13, 23, 26, 27

Tabla 3.6. Clasificación de los estudios primarios

De acuerdo a la tabla 3.6, la mayoría de los estudios proporcionan un nuevo modelo o marco para la mejora de procesos de gestión de servicios de TI (un 39,3% de los estudios primarios). Además, existe una tendencia hacia el análisis de la necesidad de evaluar y mejorar los procesos de gestión de servicios de TI (21,4%), así como hacia la utilización combinada del marco de mejora propuesto por la norma ISO/IEC 15504 junto con otros marcos de mejora de procesos de gestión de servicios de TI. Finalmente, existe un creciente interés por la aplicación de nuevos modelos de mejora de procesos de gestión de servicios de TI (17,9%).

3.1.5.2. Estándares usados para la mejora de procesos de gestión de servicios de TI

La tabla 3.7 muestra una clasificación de los estudios primarios según los diferentes estándares usados para la mejora de procesos de gestión de servicios de TI. Esta clasificación incluye, por una parte, los modelos desarrollados específicamente para la gestión de servicios de TI (filas 1 a 4) y, por otra parte, los modelos no diseñados particularmente con este propósito (filas 5 a 7).

Estándar		Estudios primarios
1	**ISO/IEC 20000**	1, 3, 4, 5, 7, 8, 12, 14, 15, 16, 18, 19, 21, 22, 25, 26, 28
2	**ITIL V1**	20,25
3	**ITIL V2**	1, 2, 3, 4, 5, 6, 7, 9, 10, 12, 13, 15, 22, 26, 27
4	**ITIL V3**	4, 8, 11, 17, 19, 24, 25
5	**ISO/IEC 15504-8 & 20000-4**	4, 5, 7, 8, 19, 21, 24, 26
6	**CMM/CMMI**	7, 11, 16, 17, 20, 25
7	**CMMI-SVC**	7, 8, 16, 19

Tabla 3.7. Estándares usados para la mejora de procesos de gestión de servicios de TI

Referente a los modelos de procesos de referencia, los resultados del análisis de los estudios primarios revelan que la norma ISO/IEC 20000, que aparece en el 60,7% de los estudios, es el modelo de procesos de referencia para la gestión de servicios de TI más utilizado. Le siguen ITIL V2 (con el 53,6% de los estudios primarios) e ITIL V3 (con el 28,6%). ITIL V1 sólo es mencionado en 2 estudios primarios.

Además, las nuevas propuestas de trabajo de la ISO, ISO/IEC 15504-8 e ISO/IEC 20000-4 (con un 28,6% de los estudios), definen un modelo de evaluación de procesos de gestión de servicios de TI y un modelo de procesos de referencia de gestión de servicios de TI, respectivamente.

Finalmente, con relación a los modelos CMMI, estos modelos también han sido usados para guiar programas de mejora de procesos de gestión de servicios de TI. CMMI-SVC, ha sido considerada en el 14,3% de los estudios.

3.1.5.3. Nuevos modelos de mejora de procesos de gestión de servicios de TI

El creciente interés en la mejora de procesos de gestión de servicios de TI se pone de manifiesto gracias a la proliferación de un importante número de iniciativas surgidas con el objetivo específico de desarrollar nuevos modelos. La tabla 3.8 muestra estos nuevos modelos de mejora de procesos de gestión de servicios de TI.

Modelo	Estudios primarios	Descripción
TIPA (antes llamado AIDA)	1, 2, 3, 4, 7, 13, 22, 23, 26, 27	*"The TIPA model was inspired by ITIL best practices, with the goal to enable objective ITSM capability assessments. The references used to create the PRM and the PAM were the Service Support and Service Delivery books published by OGC."* (Estudio primario 1)
SPINI/SPINI+	4,28	*"The SPINI-methodology was supplemented with process modelling methods and the process library was extended with IT service management processes (ITIL, ISO/IEC 20000)."* (Estudio primario 25)
NOVE-IT/NiCE	6	*"A process model for IT procurement, development, operation, and service provision (also called NOVE-IT) was developed." "For the NOVE-IT project, it was decided to create an assessment model consisting of a process dimension adopted as-is from Part 2 of ISO/IEC TR 15504. The model is called NOVE-IT Capability dEtermination, or NiCE."* (Estudio primario 6)
MITO	6,25	*"A maturity model for the assessment of companies or parts of companies providing IT Operations services. The assessment is process based thus able to reveal the potentials for improvement. The model combines features of the SEI CMM and the assessment method of the EFQM."* (Estudio primario 22)
NOEMI	9, 10	*"The development and experimentation of an IT process assessment methodology especially designed to be used in very small enterprises (VSEs)." "The processes themselves are based on a combined approach of ISO/IEC 15504 and the IT Infrastructure Library."* (Estudio primario 9)
SPiCE Lite [ITSM]	11	*"SPiCE Lite [ITSM] supports the guided assessment of ITIL IT organization processes. SPiCE applies its own maturity level model to ITIL processes. It thus provides a qualitative evaluation of process maturity in accordance to the SPiCE-process maturity model (ISO/IEC 15504)."* (Estudio primario 11)

Modelo	Estudios primarios	Descripción
TickIT Plus	14	*"ISO/IEC 15504, ISO/IEC 15288 and ISO/IEC 12207 will form the core around which TickIT Plus is designed: the capability model and the process structure. Each of other three standards: ISO/IEC 20000, ISO/IEC 27001 and ISO/IEC 25030, termed 'Requirements Standards', are all optional standards that can be included under the TickIT Plus certification."* (Estudio primario 14)
SPICE 1-2-1 for ISO 20000	18	*"So ISO/IEC 15504 can be used as universal model for process assessment and process improvement. Following this idea I have defined an 'ISO 20000 – PAM', a process assessment model for IT Service Management according to ISO/IEC 20000-1:2005. Based on the ISO 20000 – PAM we have implemented an Assessment Tool for IT Service Management: SPICE 1-2-1 for ISO 20000."* (Estudio primario 18)
IT Service CMM	20	*"We propose an Information Technology Service Capability Maturity Model (IT Service CMM) that can be used to assess the maturity of IT service processes and identify directions for improvement."* (Estudio primario 20)

Tabla 3.8. Modelos de mejora de procesos de gestión de servicios de TI

La tabla 3.9 muestra la distribución de estos nuevos modelos de mejora de procesos de gestión de servicios de TI dependiendo del método de evaluación y del modelo de referencia de procesos que utilizan.

Método de evaluación	Modelo de Procesos de Referencia		
	ITIL	**ISO/IEC 20000**	**Propio**
SCAMPI	-	-	MITO IT Service CMM
ISO/IEC 15504-2	SPINI+ TIPA NOEMI SPICE Lite [ITSM]	SPINI+ TickIT Plus SPICE 1-2-1 for ISO 20000	NiCE (NOVE-IT)

Tabla 3.9. Clasificación de los modelos de mejora de procesos de gestión de servicios de TI

Como muestra la tabla 3.9, tanto SCAMPI como ISO/IEC 15504-2 han sido utilizados como métodos de evaluación de procesos. Entonces, la posibilidad de utilizar estos marcos de medición para la evaluación y mejora de procesos de gestión de servicios de TI ya ha sido probada.

Empezando por la primera fila, MITO e IT Service CMM son las dos iniciativas con un modelo de procesos de referencia propio que utilizan SCAMPI como método de evaluación.

En cuanto a las iniciativas basadas en la norma ISO/IEC 15504, el método de evaluación definido en la parte ISO/IEC 15504-2 ha sido utilizado para evaluar los procesos de ITIL y los de la norma ISO/IEC 20000, así como para evaluar nuevos modelos de referencia de procesos propios:

- SPINI+ define una biblioteca de procesos de gestión de servicios de TI a partir de ITIL e ISO/IEC 20000.
- TIPA, NOEMI y SPICE Lite [ITSM] usan ITIL (V2) como modelo de referencia de procesos.
- TickIT Plus incluye, entre otros, ISO/IEC 20000 como estándar opcional en su modelo de certificación.
- SPICE 1-2-1 for ISO 20000 usa el método de evaluación de ISO/IEC 15504-2 para evaluar los procesos de la norma ISO/IEC 20000.
- NiCE usa el método de evaluación de ISO/IEC 15504-2 para evaluar los procesos definidos por NOVE-IT, un conjunto de procesos de adquisición, desarrollo, operación y provisión de servicio de TI.

3.1.5.4. Tendencia del interés por la mejora de procesos de gestión de servicios de TI

La comunidad internacional del área de la Ingeniería del Software ha mostrado un interés creciente por la mejora de procesos de gestión de servicios de TI. Este interés se demuestra por el creciente número de estudios que tratan este tema, especialmente desde el año 2006. La figura 3.2 muestra la distribución de los estudios primarios resultante del análisis llevado a cabo.

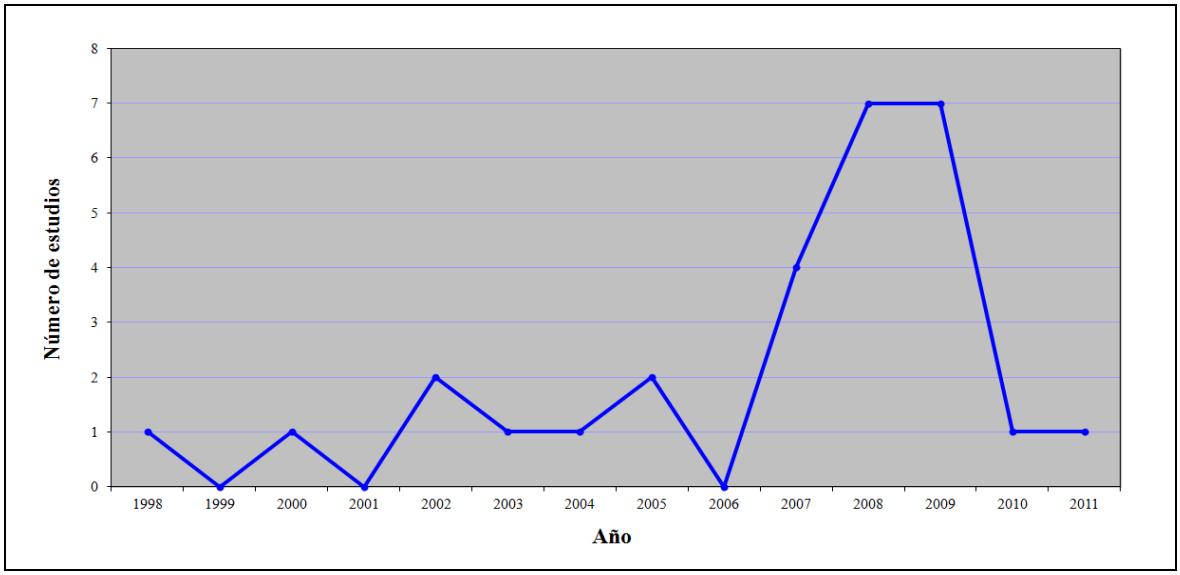

Figura 3.2. Tendencia del interés por la mejora de procesos de gestión de servicios de TI

3.1.6. Conclusiones

Al examinar los resultados obtenidos tras la ejecución de la revisión sistemática descrita en esta primera sección del capítulo tercero, se han detectado nueve iniciativas diferentes de mejora de procesos de gestión de servicios de TI en las que se han desarrollado nuevos modelos para la evaluación de este tipo de procesos. Se ha podido observar que todos estos modelos se componen de un modelo de referencia de procesos de gestión de servicios de TI y de un método de evaluación. Esta revisión sugiere que la norma ISO/IEC 20000, ITIL (V2 y V3) y CMMI SVC son los modelos de referencia de procesos de gestión de servicios de TI más utilizados. Tanto SCAMPI como ISO/IEC 15504-2 han sido utilizados por estos nuevos modelos como métodos de evaluación de procesos de gestión de servicios de TI.

Si nos centramos en los modelos basados en la norma ISO/IEC 15504, siete de los nueve modelos detectados utilizan métodos de evaluación conformes con la norma ISO/IEC 15504 para evaluar los procesos de gestión de servicios de TI definidos por ITIL o por la norma ISO/IEC 20000. Entonces, los resultados sugieren que la viabilidad de utilizar el marco de medición de la norma ISO/IEC 15504 para la evaluación y mejora de procesos de gestión de servicios de TI ya ha sido examinada y probada durante la última década.

Debido a que el objetivo principal de esta investigación consiste en la integración de las normas ISO relacionadas con mejora de procesos de gestión de servicios de TI, el primer paso debe consistir en llevar a cabo un estudio de las relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 con los procesos definidos por la norma ISO/IEC 15504-5.

3.2. Método utilizado para el estudio de las relaciones

El estudio de las relaciones entre los dos estándares fue llevado a cabo siguiendo una estrategia iterativa en la que cada resultado de los procesos de la norma ISO/IEC 20000-4 (que se muestran en la figura 2.5 y cuya estructura se presenta en la tabla 2.6) fue comparado con las prácticas básicas de los procesos de la norma ISO/IEC 15504-5 (que se muestran en la figura 2.3 y cuya estructura se presenta en la tabla 2.2). Como se ha dicho en el apartado 2.3.2.2, la norma ISO/IEC 20000-4 define un total de 164 resultados, pertenecientes a 26 procesos diferentes, que a su vez se agrupan en 6 categorías de procesos.

La figura 3.3 muestra el procedimiento seguido para detectar relaciones entre estas dos normas. Para cada uno de los procesos de la norma ISO/IEC 20000-4, se analizaron en profundidad todos sus resultados. Para cada resultado se seleccionó un conjunto de posibles procesos de la norma ISO/IEC 15504-5 relacionados con el resultado en cuestión.

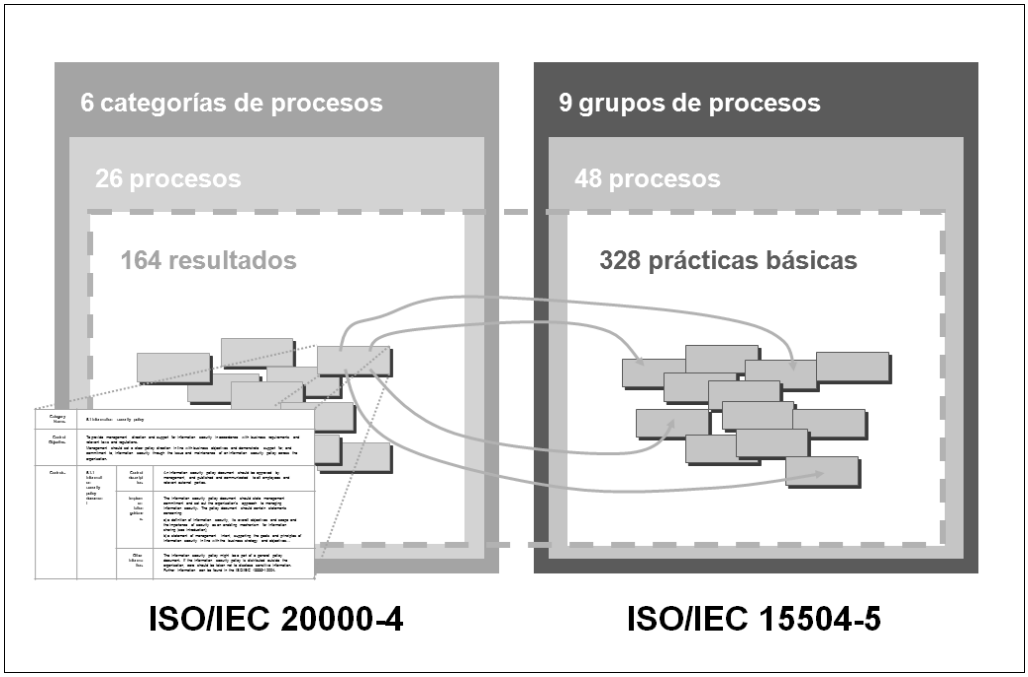

Figura 3.3. Procedimiento seguido para el estudio de las relaciones de las normas ISO/IEC 20000-4 e ISO/IEC 15504-5

Después de un análisis detallado de las prácticas básicas de los procesos seleccionados, fue posible determinar la existencia o no de conexión entre el resultado del proceso de la norma ISO/IEC 20000-4 y el proceso de la norma ISO/IEC 15504-5. Se detectaron tres tipos de correspondencia:

- Correspondencia entre un resultado de un proceso de la norma ISO/IEC 20000-4 y una o más prácticas básicas de un proceso de la norma ISO/IEC 15504-5.
- Correspondencia entre un resultado de un proceso de la norma ISO/IEC 20000-4 y una o más prácticas básicas de diferentes procesos de la norma ISO/IEC 15504-5.
- Inexistencia de una correspondencia entre un resultado de un proceso de la norma ISO/IEC 20000-4 y un proceso de la norma ISO/IEC 15504-5.

La versión final de la comparativa entre estos dos estándares internacionales es el resultado de un proceso de refinamiento sucesivo en tres etapas que se muestran en la figura 3.4 y se describen a continuación.

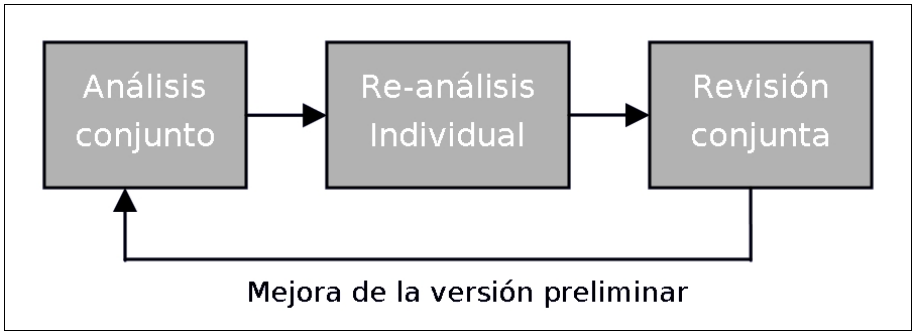

Figura 3.4. Estudio de las relaciones entre las normas ISO/IEC 20000-4 e ISO/IEC 15504-5

Con el objetivo de compartir el conocimiento y de contrastar los diferentes puntos de vista de los investigadores de nuestro grupo, durante la primera etapa, los dos estándares fueron analizados en grupo. No fue posible realizar la comparativa completa en una única sesión de trabajo, se necesitaron varias reuniones para obtener una versión preliminar de la comparativa. En cada reunión se analizaron cinco o seis procesos de la norma ISO/IEC 20000-4.

En la segunda etapa, y con la intención de consolidar los resultados obtenidos en las reuniones conjuntas, la versión preliminar de la comparativa fue nuevamente examinada de forma individual, por cada miembro del grupo, para confirmar las decisiones alcanzadas o, por el contrario, hacer algunas modificaciones sobre la versión preliminar.

Finalmente, durante la etapa de revisión conjunta, las propuestas de cada miembro del grupo fueron discutidas detenidamente, hasta llegar a un consenso general para aceptar o rechazar cada propuesta.

3.3. Tipos de relaciones detectadas

A partir del estudio de las relaciones entre los resultados de los procesos de la norma ISO/IEC 20000-4 y las prácticas básicas de los procesos de la norma IOS/IEC 15504-5, se establecieron cuatro tipos distintos de relaciones:

1. **Relación total**. En este caso, todos los resultados de un proceso de la norma ISO/IEC 20000-4 quedan cubiertos por prácticas básicas de la norma ISO/IEC 15504-5.
2. **Relación fuerte**. En este caso, no todos pero sí la mayoría de los resultados de un proceso de la norma ISO/IEC 20000-4 están cubiertos por prácticas básicas de la norma ISO/IEC 15504-5.
3. **Relación parcial**. En este tipo de relación sólo algunos de los resultados de un proceso de la norma ISO/IEC 20000-4 son parcialmente tratados por prácticas básicas de la norma ISO/IEC 15504-5.
4. **Inexistencia de relación**. En este último caso, el proceso de la norma ISO/IEC 20000-4 no está relacionado con ninguna práctica básica de la norma ISO/IEC 15504-5.

3.4. Análisis de las relaciones

La tabla 3.11 muestra, a alto nivel, un resumen de las relaciones detectadas entre las seis categorías de procesos de la norma ISO/IEC 20000-4 y los nueve grupos de procesos de la norma ISO/IEC 15504-5. Esta tabla puede ser analizada desde dos puntos de vista diferentes:

- Un análisis por columnas determina las relaciones desde la perspectiva de los grupos de procesos de la norma ISO/IEC 15504-5.
- Un análisis por filas proporciona información sobre las relaciones desde la perspectiva de las categorías de procesos de la norma ISO/IEC 20000-4.

Mediante un análisis por columnas de la tabla 3.10, puede observarse que el grupo de procesos de Reutilización (REU) es el único que no puede utilizarse para facilitar la implantación de la norma ISO/IEC 20000. El propósito de los procesos REU es gestionar la vida de los activos reutilizables y planificar, establecer, administrar, controlar y

supervisar el programa de reutilización de la organización para explotar sistemáticamente las oportunidades de reutilización. La norma ISO/IEC 15504-5 considera como activos reutilizables los requisitos, diseños, códigos, casos de prueba y las librerías, es decir, los componentes software y hardware. Como los servicios no se consideran activos reutilizables, no se han identificado evidencias de relación con las prácticas básicas de los procesos REU.

Centrándonos ahora en la columna del grupo de procesos de soporte (SUP), se puede observar que este grupo está relacionado con casi todas las categorías de proceso de la norma ISO/IEC 20000-4. Los procesos del grupo SUP dan soporte a otros procesos con propósitos distintos y contribuyen al éxito y a la calidad del proyecto. Estos procesos también son utilizados y ejecutados por varios procesos de gestión de servicios de la norma ISO/IEC 20000-4.

Categorías de procesos de ISO/IEC 20000-4	**Grupos de procesos de ISO/IEC 15504-5**								
	ACQ	SPL	ENG	OPE	MAN	PIM	RIN	REU	SUP
Procesos generales del SGS	ACQ.5	SPL.1 SPL.2	ENG.1		MAN.1 MAN.2 MAN.3 MAN.5 MAN.6	PIM.1 PIM.3	RIN.1 RIN.2		SUP.4 SUP.5 SUP.7
Procesos de diseño y transición de nuevos servicios o servicios modificados		SPL.2	ENG.1	OPE.1	MAN.3				SUP.3
Procesos de provisión del servicio				OPE.2	MAN.3 MAN.5		RIN.4		SUP.7
Procesos de control		SPL.2							SUP.8 SUP.10
Procesos de resolución					MAN.5				SUP.9
Procesos de relaciones	ACQ.2 ACQ.4			OPE.2					

Tabla 3.10. Relaciones entre las categorías de procesos de la norma ISO/IEC 20000-4 y los grupos de procesos de la norma ISO/IEC 15504-5

Mediante un análisis por filas de la tabla 3.10, puede observarse que todas las categorías de procesos de la norma ISO/IEC 20000-4 han sido relacionadas, al menos, con dos procesos de la norma ISO/IEC 15504-5.

El anexo B muestra todas las relaciones detectadas entre los resultados de los procesos de cada una de las seis categorías de procesos de la norma ISO/IEC 20000-4 y las prácticas básicas de la norma ISO/IEC 15504-5.

3.5. Resultados y discusión

Las aportaciones presentadas en este capítulo han permitido comprobar que la norma ISO/IEC 15504-5 considera un número importante de los resultados de los procesos de la norma ISO/IEC 20000-4, que son necesarios para la implantación y el mantenimiento de un sistema de gestión de servicios de TI. Estas aportaciones pueden ser utilizadas para facilitar la implantación de la norma ISO/IEC 20000 en empresas que hayan iniciado un programa de mejora de procesos según la norma ISO/IEC 15504 o que deseen implantar simultáneamente ambos estándares, reduciendo los esfuerzos que se deberían dedicar si se llevara a cabo su implantación por separado.

A modo de resumen de todas relaciones detectadas, la figura 3.5 muestra el grado de cobertura de los 26 procesos de la norma ISO/IEC 20000-4 por la norma ISO/IEC 15504-5. Para cada proceso, se indica si éste queda cubierto total, amplia o parcialmente por los procesos del ciclo de vida de la norma ISO/IEC 15504-5 o si, por el contrario, no es tratado por esta norma.

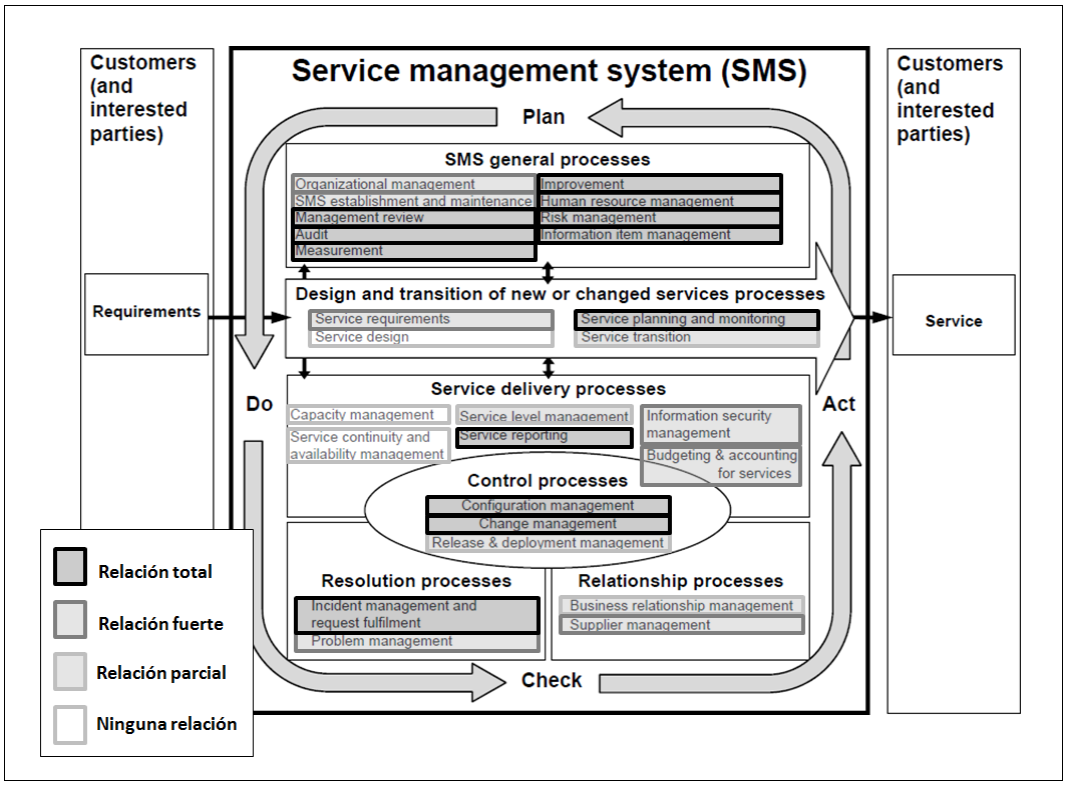

Figura 3.5. Grado de cobertura de los procesos de ISO/IEC 20000-4 por la norma ISO/IEC 15504-5

Un total de doce procesos de la norma ISO/IEC 20000-4 quedan totalmente cubiertos por prácticas básicas de la norma ISO/IEC 15504-5. La tabla 3.11 muestra estos procesos con el tipo de relación total.

Procesos de la norma ISO/IEC 20000-4	**Procesos de la norma ISO/IEC 15504-5**
Auditoría	SUP.5 Auditoría
Gestión de cambios	SUP.10 Gestión de las peticiones de cambio
Gestión de la configuración	SUP.8 Gestión de la configuración
Gestión de recursos humanos	RIN.1 Gestión de recursos humanos RIN.2 Formación
Mejora	PIM.3 Mejora de procesos
Gestión de incidentes y cumplimiento de peticiones	SUP.9 Gestión de la resolución de problemas
Gestión de la información	SUP.7 Documentación
Revisión de la dirección	SUP.4 Revisión conjunta
Medición	MAN.6 Medición
Gestión de riesgos	MAN.5 Gestión de riesgos
Planificación y monitorización del servicio	MAN.3 Gestión de proyectos
Generación de informes del servicio	SUP.7 Documentación

Tabla 3.11. Procesos de la norma ISO/IEC 20000-4 totalmente cubiertos por prácticas básicas de la norma ISO/IEC 15504-5

Los procesos de la tabla anterior, excepto uno, están directamente relacionados con un sólo proceso de la norma ISO/IEC 15504-5, en la mayoría de casos, homónimo. Sobre estas relaciones se deben tener en cuenta las siguientes consideraciones:

- Nueve de los doce procesos relacionados pertenecen al grupo de procesos de soporte (SUP) y de gestión (MAN). Estos grupos contienen procesos transversales, cuyo propósito puede ser fácilmente ampliado para cubrir también las actividades de provisión de servicios. Así pues, las prácticas básicas de los procesos SUP.8 Gestión de la configuración, SUP.9 Gestión de la resolución de problemas, SUP.10 Gestión de las peticiones de cambio, y MAN.5 Gestión de riesgos, pueden utilizarse, sin apenas introducir cambios en sus objetivos, para obtener los resultados que recomiendan los procesos de la norma ISO/IEC 20000-4 relacionados.

- Por otra parte, la infraestructura establecida mediante los procesos SUP.4 Revisión conjunta, SUP.5 Auditoría, MAN.6 Medición y PIM.3 Mejora de procesos, para desplegar, revisar y mejorar continuamente los procesos de la organización, puede utilizarse también para revisar y mejorar los procesos de gestión de servicios de TI.
- Si poner en marcha un nuevo servicio se entiende y se gestiona como un nuevo proyecto de la organización, las prácticas básicas del proceso MAN.3 Gestión de proyectos pueden utilizarse para la Planificación y monitorización del servicio. Del mismo modo, el proceso SUP.7 Documentación puede utilizarse para llevar a cabo la Gestión de la información y la Generación de informes del servicio.
- Finalmente, los resultados del proceso de Gestión de recursos humanos pueden obtenerse utilizando las prácticas básicas de los procesos de la norma ISO/IEC 15504-5 RIN.1 Gestión de recursos humanos y RIN.2 Formación.

Otros siete procesos de la norma ISO/IEC 20000-4 quedan ampliamente cubiertos por prácticas básicas de la norma ISO/IEC 15504-5. La tabla 3.12 muestra los procesos con este tipo de relación.

Procesos de la norma ISO/IEC 20000-4	**Procesos de la norma ISO/IEC 15504-5**
Elaboración del presupuesto y contabilidad de los servicios de TI	MAN.3 Gestión de proyectos
Gestión de la seguridad de la información	MAN.5 Gestión de riesgos RIN.4 Infraestructura
Gestión organizativa	ACQ.5 Aceptación del cliente SPL.1 Oferta del proveedor SPL.2 Entrega del producto ENG.1 Captura de requisitos MAN.1 Alineación de la organización MAN.2 Gestión de la organización MAN.3 Gestión de proyectos MAN.5 Gestión de riesgos SUP.4 Revisión conjunta
Gestión de problemas	MAN.5 Gestión de riesgos SUP.9 Gestión de la resolución de problemas
Requisitos del servicio	ENG.1 Captura de requisitos SUP.3 Validación
Establecimiento y mantenimiento del SGS	PIM.1 Establecimiento de procesos PIM.3 Mejora de procesos
Gestión de suministradores	ACQ.2 Selección del proveedor ACQ.4 Monitorización del proveedor

Tabla 3.12. Procesos de la norma ISO/IEC 20000-4 ampliamente cubiertos por prácticas básicas de la norma ISO/IEC 15504-5

Aunque no sea en su totalidad, la mayoría de los resultados de estos procesos pueden obtenerse mediante la realización de las prácticas básicas de los procesos de la norma ISO/IEC 15504-5 relacionados:

- Las prácticas básicas del proceso MAN.3 Gestión de proyectos relacionadas con la gestión económica pueden utilizarse para la Elaboración del presupuesto y contabilidad de los servicios de TI.
- La mayor parte de los resultados del proceso de Gestión de la seguridad de la información quedan cubiertos por los procesos MAN.5 Gestión de riesgos y RIN.4 Infraestructura. Del mismo modo, las prácticas básicas de los procesos MAN.5 Gestión de riesgos y SUP.9 Gestión de la resolución de problemas pueden utilizarse para satisfacer los resultados del proceso de Gestión de problemas.
- El proceso Gestión organizativa, al ser bastante transversal y multidisciplinar puede apoyarse en prácticas básicas de nueve procesos de la norma ISO/IEC 15504-5 diferentes.
- Los propósitos de los procesos ENG.1 Captura de requisitos y SUP.3 Validación pueden ampliarse para definir y validar los Requisitos del servicio.
- El Establecimiento y mantenimiento del SGS puede ser llevado a cabo mediante prácticas básicas de los procesos PIM.1 Establecimiento de procesos y PIM.3 Mejora de procesos.
- ACQ.2 Selección del proveedor y ACQ.4 Monitorización del proveedor son los procesos de relaciones con proveedores que se pueden utilizar para cubrir los resultados del proceso Gestión de suministradores.

Observando de nuevo la figura 3.5, los cuatro procesos: Gestión de las relaciones con el negocio, Gestión de la entrega y del despliegue, Gestión del nivel de servicio y Transición del servicio tienen algunos resultados que quedan parcialmente cubiertos por prácticas básicas de los siguientes tres procesos de la norma ISO/IEC 15504-5: OPE.1 Uso operacional, OPE.2 Soporte al cliente y SPL.2 Entrega del producto. Los propósitos de estos procesos están relacionados con actividades de entrega y provisión de productos y servicios al cliente.

Finalmente, los tres procesos restantes, Gestión de la capacidad, Gestión de la continuidad y disponibilidad del servicio y Diseño del servicio, al estar relacionados con actividades específicas de la gestión de servicios de TI, ninguno de sus resultados quedan cubiertos por la norma ISO/IEC 15504-5. Los resultados de estos procesos deberán ser implementados como se indica en las normas ISO/IEC 20000-4 e/o ISO/IEC 20000-1.

Capítulo 4. Estudio de las relaciones entre los estándares ISO/IEC 27000 e ISO/IEC 15504

En las empresas de desarrollo de software, al igual que en cualquier otro tipo de organización, la información debe ser adecuadamente protegida. Es por ello que, durante los últimos años, un gran número de empresas de este sector han mostrado un creciente interés por la implantación de estándares de seguridad de la información, y más concretamente, por la norma ISO/IEC 27001.

Siguiendo con la construcción del modelo integrado, en este capítulo se examinan las relaciones existentes entre los controles de seguridad de la información de la norma ISO/IEC 27002 y los procesos del ciclo de vida del software que define la norma ISO/IEC 15504-5.

La implantación de controles de seguridad de la información como los definidos en la norma ISO/IEC 27002 (ISO27000 2005b) se ha convertido en una prioridad de las compañías que desean asegurar o incrementar la confianza de sus clientes respecto de la información que de ellos maneja y proteger los activos propios de la organización para minimizar los posibles daños y asegurar su continuidad.

Para las empresas de desarrollo de software la seguridad de la información es también fundamental. De hecho, un número significativo de empresas de software de nuestro entorno, que han estado o están actualmente involucradas en un programa de mejora de procesos según la norma ISO/IEC 15504, demandan la implantación de la norma ISO/IEC 27000 como estándar de seguridad. Para facilitar la implantación de los controles de seguridad de la norma ISO/IEC 27002, e incluso para obtener una certificación ISO/IEC 27001 (ISO27000 2005a), sería de gran utilidad disponer de unas directrices para aplicar los controles de seguridad sobre los procesos de la norma ISO/IEC 15504-5.

Durante los últimos años han surgido diversas iniciativas que relacionan las mejores prácticas de la gestión de la seguridad con las de la gestión de la calidad. (Barafort et al. 2006) desarrollaron un modelo de referencia de procesos y un modelo de implantación de procesos que proporcionan un marco para la evaluación y mejora de la capacidad de los procesos y la madurez de la organización en el campo de la gestión de la seguridad. Por otra parte, (Valdevit et al. 2009) desarrollaron una guía para una implantación de la norma ISO/IEC 27001 asequible, fácil y rápida en pequeñas y medianas empresas.

Este capítulo se corresponde con la **Fase II de la construcción del Modelo Integrado de Estándares de Gestión de TI**. En él se analizan todas las posibles relaciones entre las prácticas básicas de la norma ISO/IEC 15504-5 y los controles de seguridad propuestos en la norma ISO/IEC 27002, con el objetivo de facilitar la implantación conjunta de las normas ISO/IEC 15504 e ISO/IEC 27001 o de facilitar la implantación de esta última en una empresa que ya tiene un determinado nivel de capacidad en algunos procesos según la norma ISO/IEC 15504. La figura 4.1 muestra de manera gráfica el objetivo de la Fase II: Relaciones entre las normas ISO/IEC 15504 e ISO/IEC 27000.

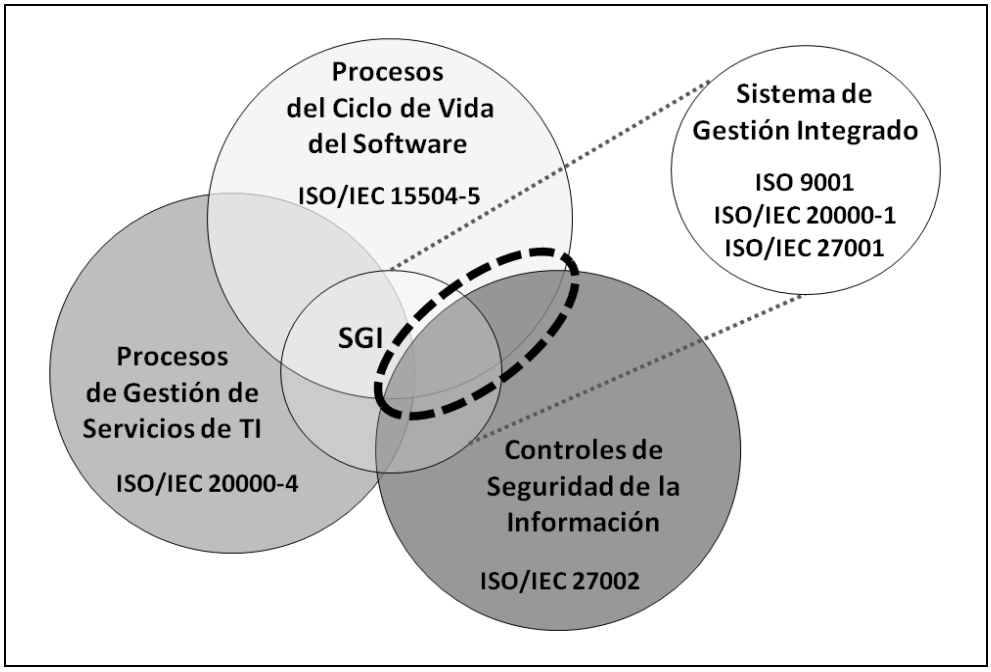

Figura 4.1. Fase II de la construcción del Modelo Integrado de Estándares de Gestión de TI

En la sección 4.1 se define el método utilizado para realizar la comparativa entre los estándares ISO/IEC 15504-5 e ISO/IEC 27002. En la sección 4.2 se definen los tipos de correspondencias detectadas entre ambos. En la sección 4.3 se analizan las relaciones detectadas entre las prácticas básicas de la norma ISO/IEC 15504-5 y los controles de seguridad de la norma ISO/IEC 27002. La sección 4.4 presenta la *ISO/IEC 15504 Security Extension*, una extensión sobre los procesos de la norma ISO/IEC 15504-5 que detalla los cambios que son necesarios realizar para implantar los controles de seguridad relacionados. Finalmente, en la sección 4.5 se analizan los resultados obtenidos y las conclusiones extraídas de esta investigación.

4.1. Método utilizado para el estudio de las relaciones

El estudio de las relaciones entre los dos estándares fue llevado a cabo siguiendo la misma estrategia iterativa que la descrita en el apartado 3.1. En este caso, cada control de seguridad de la información definido en la norma ISO/IEC 27002 (dichos controles se muestran en la tabla 2.10) fue comparado con las prácticas básicas de los procesos de la norma ISO/IEC 15504-5 (dichas prácticas básicas se muestran en la figura 2.3 y su estructura se presenta en la tabla 2.2).

La figura 4.2 muestra el procedimiento seguido para detectar relaciones entre estas dos normas. Como se ha dicho en el apartado 2.4.1.2, la norma ISO/IEC 27002 agrupa los 133 controles de seguridad en 39 categorías, que a su vez se agrupan en 11 cláusulas. Para cada una de las categorías de la norma ISO/IEC 27002, se analizaron en profundidad todos sus controles de seguridad. Para cada control se seleccionó un conjunto de posibles procesos de la norma ISO/IEC 15504-5 relacionados con el resultado en cuestión.

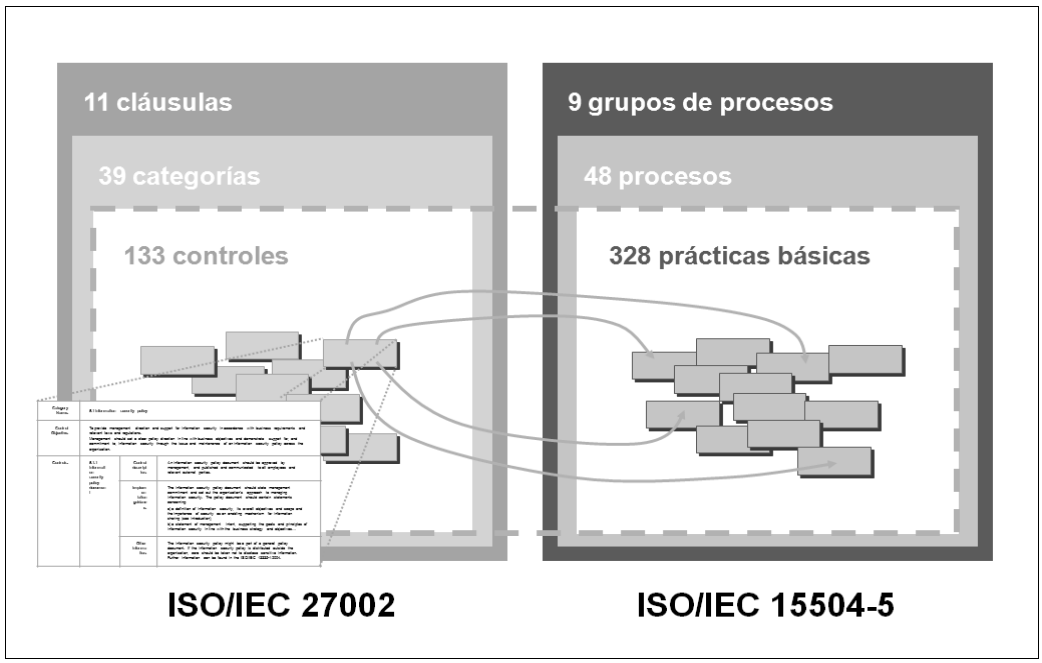

Figura 4.2. Procedimiento seguido para el estudio de las relaciones entre las normas ISO/IEC 27002 e ISO/IEC 15504-5

La versión final de la comparativa entre estos dos estándares internacionales es el resultado del proceso de refinamiento sucesivo en tres etapas descrito anteriormente en el apartado 3.1.

4.2. Tipos de correspondencias

A partir del análisis de las relaciones entre los controles de la norma ISO/IEC 27002 y las prácticas básicas de la norma ISO/IEC 15504-5, se establecieron cinco tipos diferentes de correspondencias. A continuación se citan y muestran algunos ejemplos de cada uno de estos tipos de correspondencias.

- **1. Correspondencia entre un control y todas las prácticas básicas de un proceso.** Un ejemplo de este caso puede ser la relación entre el control *10.1.2 Gestión de cambios* y todas las prácticas básicas del proceso *SUP.10 Gestión de las peticiones de cambios*. Aunque este conjunto de prácticas básicas se realizan para asegurar que se gestionan y controlan los cambios en los productos en desarrollo, se podría realizar el mismo conjunto de prácticas básicas para gestionar los cambios en los recursos y sistemas de tratamiento de la información del modo indicado por el control.

  Otro ejemplo de este caso se puede observar en la relación entre el control *10.1.1 Documentación de los procedimientos de operación* y el proceso *SUP.7 Documentación*.

- **2. Correspondencia entre un control y parte del conjunto de prácticas básicas de un proceso.** Este es el caso del control *10.5.1 Copias de seguridad de la información*, que está claramente relacionado con las prácticas básicas SUP.8.BP10 y RIN.4.BP2. La descripción de este control dice: "*se deben realizar copias de seguridad de la información y del software, y se deben probar periódicamente conforme a la política de copias de seguridad acordada*". Esta descripción encaja con la descripción de la práctica básica SUP.8.BP10: "*Gestionar las copias de seguridad, el almacenaje, la gestión y la entrega de elementos configurados. Asegurar la integridad y la consistencia de los elementos configurados a través de la planificación apropiada y de los recursos necesarios para copias de seguridad y almacenaje. Controlar la gestión y la entrega de elementos configurados*".

  Del mismo modo, la descripción del control también encaja con la descripción de la práctica básica RIN.4.BP2: "*Definir los requisitos de la infraestructura para dar soporte a la realización de los procesos apropiados. Los requisitos de la infraestructura deben incluir: requisitos de seguridad, transferencia y compartición de datos, copias de seguridad y de respaldo, acceso remoto, espacio físico de trabajo y equipamiento, requisitos de suporte al usuario y requisitos de mantenimiento*".

- **3. Correspondencia entre un control y un proceso.** En este caso, existe una correspondencia entre un control y un proceso, pero sin ninguna conexión explícita con una práctica básica del proceso. La relación ha sido identificada mediante la comparación de la descripción del control con el propósito del proceso.

  Este es el caso del control *10.7.4 Seguridad de la documentación del sistema* con el proceso *SUP.7 Documentación*. La descripción de este control dice: "*la documentación del sistema debe estar protegida contra accesos no autorizados*", mientras que el propósito del proceso SUP.7 es: "*desarrollar y mantener la información registrada producida por un proceso*".

  En este caso, para incluir los aspectos de seguridad considerados por el control en el proceso relacionado, se ofrecen dos posibles soluciones:

  - Añadir una nueva práctica básica al proceso para satisfacer el objetivo del control. La descripción de esta nueva práctica básica se podría adaptar de las directrices de implantación del control.
  - Modificar o ampliar la descripción de las prácticas básicas existentes y el propósito del proceso.

  Para el caso particular del proceso SUP.7, las prácticas básicas SUP.7.BP1, SUP.7.BP3, SUP.7.BP6, SUP.7.BP7 y SUP.7.BP8 deberían ser ampliadas para satisfacer el objetivo del control. Además, el propósito del proceso también podría ser cambiado por: "*desarrollar, mantener y proteger contra accesos no autorizados la información registrada producida por un proceso*".

- **4. Inexistencia de correspondencia entre el control y algún proceso.** Este es el caso de los controles: *10.10.4 Registros de administración y operación*, *10.10.5 Registro de fallos* y *10.10.6 Sincronización del reloj*. Debido a su naturaleza particular, estos controles están relacionados con actividades de administración de sistemas que no están cubiertas por la norma ISO/IEC 15504-5.

- **5. Correspondencia entre un control y el proceso *RIN.4 Infraestructura*.** En este caso, el control sólo está relacionado con el proceso *RIN.4 Infraestructura*, cuyo propósito es: "*mantener una infraestructura estable y fiable, necesaria para dar soporte a la realización de cualquier otro proceso*".

  Un ejemplo de este caso se puede observar en el primer control de la categoría 10.10 Supervisión, *10.10.1 Registro de auditorías*, cuyo objetivo es: "*producir y mantener registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información*". Si se entiende este objetivo como un requisito de la infraestructura de seguridad, el control puede ser relacionado con las prácticas básicas RIN.4.BP2 y RIN.4.BP4. Un caso similar ocurre con el control *10.10.2 Supervisión del uso del sistema*.

4.3. Análisis de las relaciones

La tabla 4.1 muestra, a alto nivel, las relaciones detectadas entre las once cláusulas de la norma ISO/IEC 20000-4 y los nueve grupos de procesos de la norma ISO/IEC 15504-5. Esta tabla puede ser analizada desde dos puntos de vista diferentes:

- Un análisis por columnas determina las relaciones desde la perspectiva de los grupos de procesos de la norma ISO/IEC 15504-5.
- Un análisis por filas proporciona información sobre las relaciones desde la perspectiva de las cláusulas de la norma ISO/IEC 27002.

Mediante un análisis por columnas de la tabla 4.1, puede observarse que el único grupo de procesos relacionado con todas las cláusulas de la norma ISO/IEC 27002 es el de Recursos e Infraestructura (RIN). Este grupo de procesos está compuesto por los procesos que se realizan para proporcionar los recursos humanos adecuados y la infraestructura necesaria requerida por cualquier otro proceso. Es por ello que, las relaciones establecidas entre este grupo de procesos y las cláusulas de la norma ISO/IEC 27002, son bastante evidentes.

Por el contrario, los grupos de procesos de Operación (OPE), Mejora de Procesos (PIM) y Reutilización (REU) muestran una muy débil o inexistente relación con alguna cláusula de la norma ISO/IEC 27002. El grupo de procesos de Operación (OPE) contiene prácticas básicas para la correcta operación y uso del producto y/o servicio software. Por lo tanto, no resulta sorprendente que no se haya detectado ninguna relación con la norma ISO/IEC 27002.

El grupo de procesos de Mejora de Procesos (PIM) contiene los procesos realizados para definir, desplegar, evaluar y mejorar los procesos realizados en la organización. Este tipo de aspectos no han sido específicamente considerados por la norma ISO/IEC 27002. Más bien, están relacionados con la norma ISO/IEC 27001, y más concretamente con los procesos del modelo PDCA.

El propósito de los procesos de Reutilización (REU) es gestionar el ciclo de vida de los activos reutilizables y planificar, establecer, gestionar, controlar y supervisar el programa de reutilización de una organización para explotar sistemáticamente las oportunidades de reutilización. Todas estas actividades están mejor relacionadas con la norma ISO/IEC 27001 que con la norma ISO/IEC 27002. Es por ello que no se han identificado evidencias de prácticas básicas de los procesos de Reutilización (REU) en las cláusulas de la norma ISO/IEC 27002.

	Grupos de procesos de ISO/IEC 15504-5								
Cláusulas de ISO/IEC 27002	ACQ	SPL	ENG	OPE	MAN	PIM	RIN	REU	SUP
5 Política de seguridad					✓		✓		
6 Aspectos organizativos de la seguridad de la información	✓	✓			✓		✓		✓
7 Gestión de activos							✓		
8 Seguridad ligada a recursos humanos					✓		✓		
9 Seguridad física y ambiental							✓		
10 Gestión de comunicaciones y operaciones	✓	✓	✓				✓		✓
11 Control de acceso							✓		
12 Adquisición, desarrollo y mantenimiento de los sistemas de información	✓		✓		✓		✓		✓
13 Gestión de incidentes de seguridad de la información					✓		✓		✓
14 Gestión de la continuidad del negocio					✓		✓		
15 Cumplimiento	✓	✓	✓			✓	✓		✓

Tabla 4.1. Relaciones entre las cláusulas de la norma ISO/IEC 27002 y los grupos de procesos de la norma ISO/IEC 15504-5

Mediante un análisis por filas de la tabla 4.1, puede observarse que las cláusulas *7 Gestión de activos*, 9 *Seguridad física y ambiental* y *11 Control de acceso* sólo tienen relaciones débiles con el grupo de procesos de Recursos e Infraestructura (RIN). Del

mismo modo, las cláusulas: *5 Política de seguridad*, *8 Seguridad ligada a recursos humanos* y *14 Gestión de la continuidad del negocio,* solamente están relacionadas con los grupos de procesos de Gestión (MAN) y Recursos e Infraestructura (RIN).

El anexo C muestra todas las relaciones detectadas entre los controles de seguridad de cada una de las once cláusulas de la norma ISO/IEC 27002 y las prácticas básicas de la norma ISO/IEC 15504-5.

4.4. ISO/IEC 15504 Security Extension

En esta sección se presenta la *ISO/IEC 15504 Security Extension*. Ha sido elaborada a partir de las relaciones entre las prácticas básicas de la norma ISO/IEC 15504-5 y los controles de seguridad de la norma ISO/IEC 27002 presentadas en el anexo C. La *ISO/IEC 15504 Security Extension* detalla los cambios que son necesarios realizar sobre los procesos de la norma ISO/IEC 15504-5 para implantar los controles de seguridad relacionados.

La ISO/IEC 15504 Security Extension tiene una doble aplicación:

- Por una parte, puede ser usada para facilitar la implantación del estándar ISO/IEC 27001 en organizaciones de desarrollo de software que están o han estado involucradas en programas de mejora de procesos según la norma ISO/IEC 15504.
- Por otra parte, puede ser usada para facilitar la implantación simultánea de las normas ISO/IEC 27001 e ISO/IEC 15504, evitando la repetición de tareas similares incluidas en los dos estándares y, por lo tanto, reduciendo la cantidad de esfuerzo requerido por la organización.

En ambos casos, la organización debe seleccionar los controles de la norma ISO/IEC 27002 que le son aplicables, dependiendo del tipo de organización y de la actividad principal.

4.4.1. Tipos de acciones propuestas por la *ISO/IEC 15504 Security Extension*

Las modificaciones y ampliaciones que propone realizar la *ISO/IEC 15504 Security Extension* sobre los procesos de la norma ISO/IEC 15504-5 con el fin de hacerlos compatibles con los requisitos de seguridad de los controles de la norma ISO/IEC 27002 relacionados, pueden afectar a diferentes componentes de los procesos: propósito, prácticas básicas y/o productos de trabajo. Se establecieron cuatro tipos distintos de acciones a realizar sobre un proceso de la norma ISO/IEC 15504-5 para que cubriera los requisitos de seguridad de un control de la norma ISO/IEC 27002 determinado:

- **Utilizar el propósito del proceso o sus prácticas básicas para satisfacer los requisitos de seguridad del control relacionado, sin necesidad de realizar ningún tipo de modificación o ampliación en el proceso**.

  Un ejemplo de este caso puede observarse en la relación entre el control *10.1.2 Gestión de cambios* ("Deben controlarse los cambios en los recursos y los sistemas de tratamiento de la información.") y el proceso *SUP.10 Gestión de las peticiones de cambio*, cuyo propósito es asegurar que los cambios en los productos en desarrollo son gestionados y controlados. Se pueden realizar las prácticas básicas SUP.10.BP1 a SUP.10.BP9 para gestionar los cambios en los recursos de tratamiento de la información en la forma indicada por el control relacionado.

  Otro ejemplo de este caso es la relación entre el control *10.1.1 Documentación de los procedimientos de operación* ("Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.") y el proceso *SUP.7 Documentación*, cuyo propósito es desarrollar y mantener la información registrada producida por un proceso. Se pueden realizar las prácticas básicas SUP.7.BP1 a SUP.7.BP8 para desarrollar, mantener y poner a disposición de los usuarios los procedimientos de operación.

- **Modificar o ampliar una o más prácticas básicas**.

  Un ejemplo de este caso puede observarse en la relación entre el control *13.1.1 Notificación de los eventos de seguridad de la información* ("Los eventos de seguridad de la información se deben notificar a través de los canales adecuados de gestión lo antes posible") y la práctica básica *RIN.3.BP4 Capturar conocimiento*, cuyo propósito es identificar y registrar cada elemento de conocimiento de acuerdo con el esquema de clasificación y los criterios de los activos. Para cubrir todos los aspectos de seguridad del control, la descripción de la práctica básica *RIN.3.BP4* debería ser ampliada para decir:

  "Identificar y registrar cada elemento de conocimiento de acuerdo con el esquema de clasificación y los criterios de los activos, incluyendo los eventos de seguridad de la información a través de los canales de gestión adecuados lo antes posible".

  Otro ejemplo de este caso es la relación entre el control *8.2.2 Concienciación, formación y capacitación en seguridad de la información* ("Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deben recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo") y la práctica básica *RIN.2.BP2 Identificar las necesidades de información*

("Identificar y evaluar las habilidades y competencias que deben facilitarse o mejorarse a través de la formación"). Al igual que en el ejemplo anterior, la descripción de esta práctica básica debería ser ampliada para decir:

"Identificar y evaluar las habilidades y competencias que deben facilitarse o mejorarse a través de la formación, incluyendo los requisitos de seguridad, las responsabilidades legales y los controles de negocio, así como la capacitación en el uso correcto de los recursos de tratamiento de la información".

- **Añadir una nueva práctica básica a partir del objetivo del control relacionado, que estará estrechamente vinculada a las prácticas básicas ya existentes**. En este caso, el proceso de la norma ISO/IEC 15504-5 relacionado no tiene ninguna práctica básica que cubra el control de seguridad y, por lo tanto, es necesario crear una nueva.

  Un ejemplo de este caso puede observarse en el control *10.7.4 Seguridad de la documentación del sistema* ("La documentación del sistema debe estar protegida contra accesos no autorizados"), que está relacionado con el propósito del proceso *SUP.7 Documentación* ("Desarrollar y mantener la información registrada producida por un proceso"). Para que cubra los aspectos de seguridad del control, la descripción de la nueva práctica básica, llamada *SUP.7.BP9 Proteger documentos*, debería ser:

  "Proteger la documentación del sistema contra accesos no autorizados".

  Un segundo ejemplo de este caso es el control *12.4.2 Protección de los datos de prueba del sistema* ("Los datos de prueba se deben seleccionar con cuidado y deben estar protegidos y controlados"). Este control está relacionado con el proceso *ENG.8 Pruebas del software* cuyo propósito es confirmar que el producto de software cumple los requisitos definidos. En este caso, se creó una nueva práctica básica:

  *"**ENG.8.BP0 Proteger los datos de prueba**: Eliminar o hacer irreconocible antes de su uso, proteger y controlar toda la información personal o confidencial utilizada para propósitos de pruebas".*

- **Modificar o ampliar el propósito del proceso**. En este caso, existe una correspondencia entre un control y un proceso sin una conexión explícita con una práctica básica del proceso. La relación ha sido identificada al comparar la descripción del control con el propósito del proceso. En consecuencia, la acción a realizar consiste en la modificación o ampliación del propósito del proceso con el fin de cubrir los requisitos de seguridad del control.

Un ejemplo de este caso puede observarse en la relación del control control *10.7.4 Seguridad de la documentación del sistema* ("La documentación del sistema debe estar protegida contra accesos no autorizados") con el proceso *SUP.7 Documentación* ("Desarrollar y mantener la información registrada producida por un proceso"). Para cubrir los aspectos de seguridad el propósito del proceso se amplió para que enunciara explícitamente:

"Desarrollar, mantener y proteger contra accesos no autorizados la información registrada producida por un proceso".

Otro ejemplo de este caso puede observarse en el proceso *ACQ.3 Acuerdo contractual*. Este proceso está relacionado con los nueve controles de seguridad de la norma ISO/IEC 27002 que se muestran en la tabla 4.2.

Controles de la norma ISO/IEC 27002 cubiertos por el proceso ACQ.3 Acuerdo contractual	
6.2.1	Identificación de los riesgos derivados del acceso de terceros
6.2.3	Tratamiento de la seguridad en contratos con terceros
10.2.1	Provisión de servicios
10.6.2	Seguridad de los servicios de red
10.8.2	Acuerdos de intercambio
12.5.5	Externalización del desarrollo de software
15.1.2	Derechos de propiedad intelectual (DPI)
15.1.4	Protección de datos y privacidad de la información personal
15.1.6	Regulación de los controles criptográficos

Tabla 4.2. Controles de la norma ISO/IEC 27002 cubiertos por el proceso ACQ.3 Acuerdo contractual

Para satisfacer estos controles, los contratos o acuerdos que se negocien o aprueben siguiendo el proceso *ACQ.3 Acuerdo contractual* deben ser ampliados, incluyendo cláusulas específicas:

- que traten el acceso, tratamiento, comunicación o gestión de la información de la organización o los recursos de tratamiento de la información del proceso (para satisfacer los controles 6.2.1 y 6.2.3).
- que obliguen a terceros a implementar, operar y mantener los controles de seguridad, las definiciones de servicio y los niveles de entrega acordados (para satisfacer el control 10.2.1).
- que incluyan todas las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red (para satisfacer el control 10.6.2).

- que traten el intercambio de información y software entre la organización y las partes externas (para satisfacer el control 10.8.2).
- que incluyan los aspectos relacionados con los acuerdos de licencias, propiedad del código, derechos de propiedad intelectual, derechos de acceso para auditorías de calidad y los requisitos contractuales de calidad y seguridad, cuando el desarrollo de software sea externalizado (para satisfacer el control de 12.5. 5).
- que garanticen el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material con derechos de propiedad intelectual y en el uso de productos software propietarios (para satisfacer el control 15.1.2).
- que garanticen la protección de datos y la privacidad según lo dispuesto en la legislación y la regulación acordada (para satisfacer el control 15.1.4).
- que traten los controles criptográficos que deben ser utilizados de conformidad con todos los acuerdos, leyes y regulaciones establecidos (para satisfacer el control 15.1.6).

De esta manera, si una organización que ha implantado las prácticas básicas del proceso *ACQ.3 Acuerdo contractual* añade al contrato estándar cláusulas anteriores, habrá implantado los nueve controles de seguridad de la norma ISO/IEC 27002 relacionados con este proceso.

4.4.2. Utilización de la *ISO/IEC 15504 Security Extension*

Para cada uno de los controles de seguridad de la norma ISO/IEC 27002, la *ISO/IEC 15504 Security Extension* propone realizar una serie de acciones sobre los procesos de la norma ISO/IEC 15504-5 para que satisfagan los requisitos de seguridad del control en cuestión. Para ilustrar la utilización de la esta extensión de seguridad, en este apartado se considera la implantación del control *13.2.2 Aprendizaje de los incidentes de seguridad de la información*, cuya descripción es:

> *"Deben existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información. La información obtenida de la evaluación de los incidentes de seguridad de la información debe ser utilizada para identificar los incidentes recurrentes o de alto impacto. La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de controles mejorados o adicionales para limitar la frecuencia, el daño y el coste de sucesos futuros o que deben tenerse en cuenta en el proceso de revisión de la política de seguridad."*

Con el fin de satisfacer los requisitos de seguridad relacionados con este control, la *ISO/IEC 15504 Security Extension* propone llevar a cabo diferentes acciones en tres procesos diferentes de la norma ISO/IEC 15504-5: *SUP.9 Gestión de la resolución de problemas*, *MAN.5 Gestión de riesgos* y *RIN.3 Gestión del conocimiento*. La tabla 4.3 recoge las acciones a realizar en estos procesos. Así pues, los propósitos de los dos primeros procesos, *SUP.9* y *MAN.5*, deben ser modificados o ampliados, tal y como se ha visto en la descripción del cuarto tipo de acción. En relación al proceso RIN.3, su práctica básica RIN.3.BP4 debe ser ampliada como se ha visto en el segundo tipo de acción.

Proceso de la norma ISO/IEC 15504-5	Tipo de acción	Descripción de la acción
SUP.9 Gestión de la resolución de problemas	4. Modificar o ampliar el propósito del proceso	El proceso SUP.9 debe garantizar que los incidentes de seguridad de la información se identifican, analizan, gestionan y controlan hasta su resolución según lo indicado en la política de seguridad.
MAN.5 Gestión de riesgos	4. Modificar o ampliar el propósito del proceso	El proceso MAN.5 debe garantizar que los incidentes de seguridad de la información se identifican, analizan, cuantifican, tratan y controlan continuamente.
RIN.3 Gestión del conocimiento	2. Modificar o ampliar una práctica básica	La práctica básica RIN.3.BP4 *Capturar conocimiento* debe ser ampliada para incluir la captura de la información obtenida de la evaluación de los incidentes de seguridad de la información.

Tabla 4.3. Acciones propuestas por la *ISO/IEC 15504 Security Extension* para satisfacer el control 13.2.2 Aprendizaje de los incidentes de seguridad de la información

4.5. Resultados y discusión

Los resultados presentados en este capítulo han permitido comprobar que la norma ISO/IEC 15504-5 considera un número importante de los aspectos y controles de seguridad recogidos en la norma ISO/IEC 27002, que son necesarios para la implantación y el mantenimiento de un sistema de gestión de seguridad de la información. Estos resultados pueden ser utilizados para facilitar la implantación de la norma ISO/IEC 27000 en empresas que hayan iniciado un programa de mejora de procesos según la norma ISO/IEC 15504 o que deseen implantar simultáneamente ambos estándares reduciendo los esfuerzos que se deberían dedicar si se llevara a cabo su implantación por separado.

Los procesos de la norma ISO/IEC 15504-5 pueden llegar a cubrir 100 de los 133 controles de seguridad que recoge la norma ISO/IEC 27002. A continuación se presentan los controles cubiertos por los procesos de cada uno de los niveles de madurez que define el Modelo de Madurez de la Organización (*Organizational Maturity Model*) de la norma ISO/IEC 15504-7. Este modelo define el subconjunto mínimo de procesos de la norma ISO/IEC 15504-5 que debe tener implementados una organización para tener un cierto nivel de madurez.

La tabla 4.4 muestra los 17 controles de seguridad de la norma ISO/IEC 27002 que quedan cubiertos por los procesos del nivel de madurez 1 de la norma ISO/IEC 15504-7. Como se puede observar, los procesos de Ingeniería (ENG) permiten desplegar controles de seguridad de las cláusulas 10 Gestión de comunicaciones y operaciones, 12 Adquisición, desarrollo y mantenimiento de los sistemas de información y 15 Cumplimiento.

Procesos del nivel de madurez 1 de la norma ISO/IEC 15504-7	**Controles cubiertos de la norma ISO/IEC 27002**
ENG.1 Captura de requisitos ENG.2 Análisis de requisitos del sistema ENG.3 Diseño de la arquitectura del sistema ENG.4 Análisis de requisitos del software ENG.5 Diseño de software ENG.6 Construcción del software ENG.7 Integración del software ENG.8 Pruebas del software ENG.9 Integración del sistema ENG.10 Pruebas del sistema ENG.11 Instalación del software ENG.12 Mantenimiento del software y el sistema SPL.2 Entrega del producto	10.1.4 Separación de los recursos de desarrollo, prueba y operación 10.8.3 Soportes físicos en tránsito 10.9.1 Comercio electrónico 10.9.2 Transacciones en línea 10.9.3 Información puesta a disposición pública 12.1.1 Análisis y especificación de los requisitos de seguridad 12.2.1 Validación de los datos de entrada 12.2.2 Control del procesamiento interno 12.2.3 Integridad de los mensajes 12.2.4 Validación de los datos de salida 12.4.1 Control del software en explotación 12.4.2 Protección de los datos de prueba del sistema 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 15.1.1 Identificación de la legislación aplicable 15.1.2 Derechos de propiedad intelectual (DPI) 15.1.4 Protección de datos y privacidad de la información personal 15.1.6 Regulación de los controles criptográficos

Tabla 4.4. Controles de la norma ISO/IEC 27002 cubiertos por los procesos del nivel de madurez 1 de la norma ISO/IEC 15504-7

Los procesos del nivel de madurez 2 de la norma ISO/IEC 15504-7 cubren 29 controles de la norma ISO/IEC 27002. La tabla 4.5 muestra estos controles. Los controles marcados con un asterisco han sido también considerados por procesos del nivel de madurez 1. Sin

embargo, estos controles también aparecen en esta tabla porque algunos procesos del nivel de madurez 2, cubren nuevos requisitos de seguridad de estos controles que no son considerados por los procesos del nivel de madurez anterior.

Procesos del nivel de madurez 2 de la norma ISO/IEC 15504-7	**Controles cubiertos de la norma ISO/IEC 27002**
SUP.1 Aseguramiento de la calidad SUP.2 Verificación SUP.3 Validación SUP.4 Revisión conjunta SUP.7 Documentación SUP.8 Gestión de la configuración SUP.9 Gestión de la resolución de problemas SUP.10 Gestión de las peticiones de cambios MAN.3 Gestión de proyectos MAN.5 Gestión de riesgos ACQ.3 Acuerdo contractual ACQ.4 Monitorización del proveedor ACQ.5 Aceptación del cliente SPL.3 Soporte a la aceptación del producto	6.2.1 Identificación de los riesgos derivados del acceso de terceros 6.2.3 Tratamiento de la seguridad en contratos con terceros 10.1.1 Documentación de los procedimientos de operación 10.1.2 Gestión de cambios 10.2.1 Provisión de servicios 10.2.2 Supervisión y revisión de los servicios prestados por terceros 10.2.3 Gestión de cambios en los servicios prestados por terceros 10.3.2 Aceptación del sistema 10.5.1 Copias de seguridad de la información 10.6.2 Seguridad de los servicios de red 10.7.3 Procedimientos de manipulación de la información 10.7.4 Seguridad de la documentación del sistema 10.8.2 Acuerdos de intercambio 12.4.3 Control de acceso al código fuente de los programas 12.5.1 Procedimientos de control de cambios 12.5.3 Restricciones a los cambios en los paquetes de software 12.5.5 Externalización del desarrollo de software 12.6.1 Control de las vulnerabilidades técnicas 13.1.1 Notificación de los eventos de seguridad de la información 13.1.2 Notificación de los puntos débiles de la seguridad 13.2.1 Responsabilidades y procedimientos 13.2.2 Aprendizaje de los incidentes de seguridad de la información 13.2.3 Recopilación de evidencias 15.1.2 Derechos de propiedad intelectual (DPI)* 15.1.3 Protección de los documentos de la organización 15.1.4 Protección de datos y privacidad de la información personal* 15.1.6 Regulación de los controles criptográficos* 15.2.1 Cumplimiento de las políticas y normas de seguridad 15.2.2 Comprobación del cumplimiento técnico

Tabla 4.5. Controles de la norma ISO/IEC 27002 cubiertos por los procesos del nivel de madurez 2 de la norma ISO/IEC 15504-7

Finalmente, los procesos del nivel de madurez 3 cubren 57 controles de seguridad. Aunque 11 de estos controles ya han sido considerados por procesos de los niveles de madurez 1 y 2, los procesos del nivel 3 cubren otros requisitos de seguridad no contemplados en las relaciones con los procesos de niveles inferiores.

Los 33 controles de seguridad restantes, que no guardan ninguna relación con ningún proceso de la norma ISO/IEC 15504-5, deberán ser implementados tal y como se indica en la norma ISO/IEC 27002.

La *ISO/IEC 15504 Security Extension* desarrollada puede ser utilizada para facilitar la implantación de la norma ISO/IEC 27001 en empresas de desarrollo de software que participen, o que piensen hacerlo en un futuro próximo, en un programa de mejora de procesos de software según el estándar ISO/IEC 15504. Así pues, cuando una organización decida implementar un determinado control de seguridad de la norma ISO/IEC 27002, podrá observar en la *ISO/IEC 15504 Security Extension* si el control en cuestión guarda alguna relación con algún proceso de la norma ISO/IEC 15504-5, y en caso afirmativo, valorar las modificaciones que este/os proceso/s debe/n sufrir para cubrir todos los requisitos de seguridad propuestos por el control.

Capítulo 5. Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001

En este capítulo se analizan las relaciones existentes entre los requisitos de los sistemas de gestión que describen las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001. Se presenta un nuevo Sistema de Gestión Integrado (SGI) que amplía los requisitos del sistema de gestión de calidad de la norma ISO 9001, con los requisitos específicos del sistema de gestión de servicios de TI de la norma ISO/IEC 20000-1 y del sistema de gestión de seguridad de la información de la norma ISO/IEC 27001. Además, se muestran las guías que se han desarrollado para dar soporte a las organizaciones en la implantación de un SGI que aúne los requisitos de los tres sistemas de gestión.

Desde mediados de los noventa, algunas organizaciones del sector TIC han optado por la implantación de estándares para demostrar su capacidad para proporcionar productos que se adapten a las necesidades de los clientes y aumenten su satisfacción. Una de las normas genéricas más aplicadas es la norma ISO 9001, cuya versión actual data del año 2008, *ISO 9001:2008 Quality management systems - Requirements* (ISO9001 2008), y define un Sistema de Gestión de la Calidad (SGC) que garantiza la eficacia y la fiabilidad de los procesos de negocio de la organización. Por otra parte, durante los últimos años, han aparecido normas específicas que definen sistemas de gestión para mejorar los procesos de áreas de conocimiento concretas.

La aparición de distintos sistemas de gestión ha generado una carga para las organizaciones, pues normalmente se implantan de manera independiente, suponiendo un notable incremento del esfuerzo dedicado y, por tanto, del coste interno. Mientras que la primera vez que una organización adopta una norma debe hacer importantes esfuerzos para seguir todos los requisitos definidos por la misma, a partir de la implantación del segundo estándar, la empresa puede aprovecharse de los esfuerzos previos realizados, las lecciones aprendidas y la buenas prácticas desplegadas anteriormente. Así pues, las organizaciones que ya disponen de un SGC según la norma ISO 9001 y que están interesadas en implantar un SGSTI según la norma ISO/IEC 20000-1, o un SGSI según la norma ISO/IEC 27001, pueden y deberían reutilizar los procesos, experiencias y conocimientos obtenidos durante la implantación del SGC. En cambio, casi todas ellas, han optado por la implantación de un SGC, un SGSTI o un SGSI, entre otros, de forma independiente o escasamente integrada.

Dado que en todos los sistemas de gestión existen ciertos elementos comunes, una implantación integrada de sistemas de gestión tendrá un impacto en el corto o medio plazo, en las operaciones diarias del negocio, dando como resultado una reducción de la carga de trabajo y de las duplicidades, y una optimización de las tareas relacionadas con la implementación y mantenimiento de los sistemas de gestión.

La idea de integrar diferentes sistemas de gestión ha sido objeto de numerosos estudios en los últimos años. No existe una única definición válida para el término Sistema de Gestión Integrado (SGI). En muchos casos, la interpretación varía dependiendo de la organización o el tipo de integración. Karapetrovic define un SGI como una combinación de procesos interdependientes que operan en armonía, comparten los mismos recursos humanos, materiales, financieros, información e infraestructura, y que están enfocados hacia el cumplimiento de los objetivos establecidos (Karapetrovic and Jonker 2003). Griffith y Bhutto definen un SGI como el sistema de gestión único que proporciona los procesos de negocio a través de funciones de gestión modulares y estructuradas, establecidas según las necesidades de la organización (Griffith and Bhutto

2008). Para Pojasek, un SGI es el que combina sistemas de gestión usando un enfoque en los empleados, una visión por procesos y una perspectiva de sistemas (Pojasek 2006). Bernardo et al. resumen la integración como el proceso de vinculación de los diferentes sistemas de gestión estandarizados en un único sistema de gestión con recursos comunes destinados a mejorar la satisfacción de las partes interesadas (Bernardo et al. 2009).

Durante la última década, la demanda de integración de sistemas de gestión se ha centrado en las áreas de calidad, medio ambiente y seguridad y salud laboral. Se han publicado diferentes estudios en los que se identifican las similitudes entre los sistemas de gestión de las normas ISO 9001, ISO 14001 y OHSAS 18001 y las ventajas de su implantación integrada en las organizaciones (Aboulnaga 1998; Karapetrovic and Willborn 1998; Karapetrovic and Jonker 2003; Labodová 2004; Asif et al. 2008; Rajkovic and Aleksic 2009). Por otra parte, también han surgido diferentes proyectos de investigación destinados a implantar un SGI según estas normas en diferentes países: Austria (Fresner and Engelhardt 2004), China (Zeng et al. 2007), Italia (Salomone 2008), España (Karapetrovic and Casadesús 2009) y el Reino Unido (Griffith and Bhutto 2008).

Debido a la reciente proliferación de estándares que describen sistemas de gestión específicos para áreas de conocimiento concretas, ha surgido la necesidad de integrarlos de alguna manera en un SGI que cubra los requisitos de diversos grupos de interés con el fin de reducir las redundancias antieconómicas y generar efectos de sinergia (Karapetrovic 2002; Asif et al. 2010; Abrahamsson et al. 2010). Se han realizado algunos intentos para integrar las diferentes normas de gestión y definir el término "sistema de gestión empresarial" que pueda servir como denominador común para la integración de todas las normas de gestión de una organización (Pojasek 2006). Sin embargo, la dinámica del proceso de integración no es del todo clara y las investigaciones realizadas aún no han establecido cómo la integración de los sistemas de gestión da lugar a diferentes tipos de mejoras organizativas (Asif et al. 2010).

Con el fin de llevar a cabo una aplicación integrada de un SGSTI según la norma ISO/IEC 20000-1 y/o de un SGSI según la norma ISO/IEC 27001 en organizaciones que ya disponen de un SGC según la norma ISO 9001, en este capítulo se persiguen los siguientes objetivos:

- Identificar las iniciativas existentes para la creación de un SGI que integre el SGC de la norma ISO 9001, el SGSTI de la norma ISO/IEC 20000-1 y el SGSI de la norma ISO/IEC 27001.
- Interpretar los requisitos de los tres sistemas de gestión anteriores y analizar las relaciones entre ellos.

- Elaborar una guía completa con directrices para la alineación y/o integración de estos tres sistemas de gestión que permita la implantación efectiva de más de una de ellas en una organización.

Este capítulo se corresponde con la **Fase III de la construcción del Modelo Integrado de Estándares de Gestión de TI**. La figura 5.1 muestra de manera gráfica el objetivo de la Fase III: Definición de un Sistema de Gestión Integrado según las norma ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001.

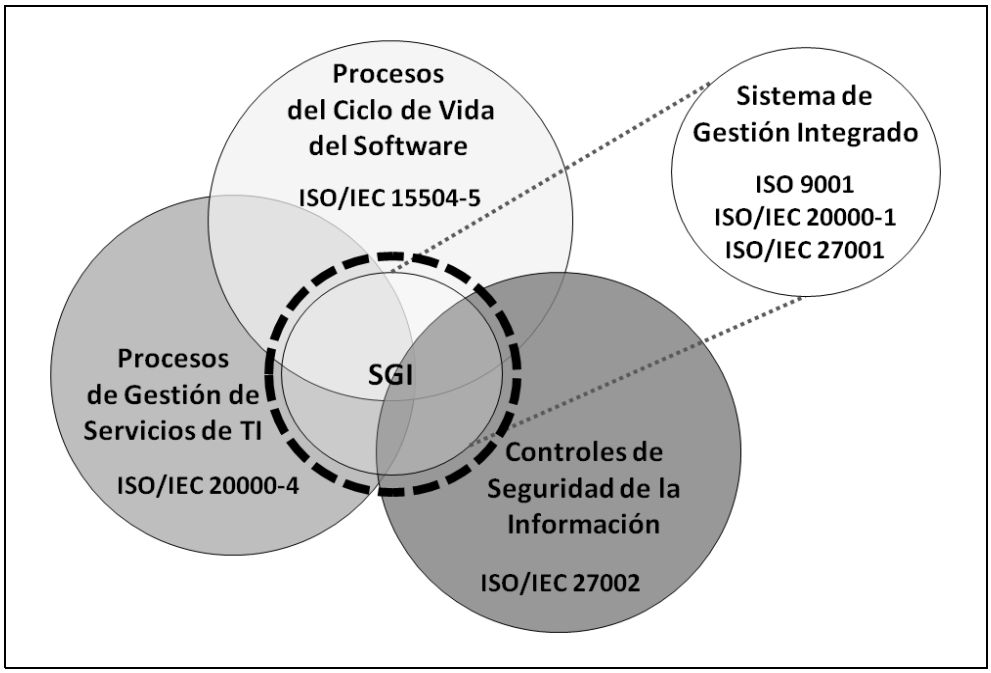

Figura 5.1. Fase III de la construcción del Modelo Integrado de Estándares de Gestión de TI

En la sección 5.1 se presentan los diferentes estándares o modelos desarrollados para integrar diversos sistemas de gestión. En la sección 5.2 se trata la compatibilidad entre los tres sistemas de gestión analizados. En la sección 5.3 se realiza una revisión sistemática de todas las iniciativas de integración de los sistemas de gestión que definen las tres normas. En la sección 5.4 se analizan todas las relaciones existentes entre los requisitos de los tres sistemas de gestión. La sección 5.5 presenta un SGI que integra los requisitos del SGC, del SGSTSI y del SGSI. La sección 5.6 describe las guías que se han desarrollado para dar soporte a las organizaciones en la implantación del SGI desarrollado. Finalmente, en la sección 5.7 se analizan los resultados obtenidos y las conclusiones extraídas de esta investigación.

5.1. Estándares para la integración de sistemas de gestión

Durante la última década han surgido diversas iniciativas para ofrecer una solución a la falta de integración entre los sistemas de gestión. En ese sentido, ISO publicó en 2001 un manual de buenas prácticas para la integración de sistemas de gestión llamado *ISO Guide 72:2001 Guidelines for the justification and development of management of system standards* (ISOG72 2001). *ISO Guide 72:2001* proporciona directrices:

- para justificar y evaluar una propuesta de proyecto de estándar de sistema de gestión con el fin de analizar su relevancia en el mercado,
- sobre la metodología de desarrollo y mantenimiento de los estándares de sistemas de gestión con el fin de garantizar la compatibilidad y la mejora de la alineación, y
- sobre la terminología, la estructura y los elementos comunes de las normas de sistemas de gestión con el fin de garantizar la compatibilidad, así como la mejora de la alineación y la facilidad de uso.

ISO Guide 72:2001 clasifica los elementos comunes que define cualquier sistema de gestión en los siguientes seis grupos: Políticas, Planificación, Implementación y operación, Rendimiento, Mejora, y Revisión de la dirección. *ISO Guide 72:2001* ha sido utilizada como base para múltiples sistemas de gestión, tales como ISO 9001, ISO 14001, OHSAS 18001, ISO 22000 e ISO/IEC 27001. Mientras que cada norma tiene sus propios requisitos específicos, estas seis categorías están presentes en todos los casos.

Algunos de los países que han hecho importantes esfuerzos para integrar diferentes sistemas de gestión son: Australia/Nueva Zelanda, España y el Reino Unido. En Australia y Nueva Zelanda la norma AS/NZS 4581:1999 (AS/NZS 1999) proporciona una guía para identificar los componentes que son comunes a todos los sistemas de gestión.

En España, AENOR publicó en 2005, la norma UNE 66177:2005 Sistemas de gestión - Guía para la integración de los sistemas de gestión (AENOR 2005) con la intención de proporcionar directrices para desarrollar, implantar y evaluar procesos de integración de los sistemas de gestión existentes en una organización. La norma consta de ocho capítulos y cinco anexos que contienen directrices para desarrollar, implementar y evaluar, a través de los procesos de revisión y mejora, el SGI resultante. Aunque estas pautas permiten una fácil integración de sistemas de gestión de cualquier naturaleza, en la introducción de la norma se menciona que las directrices se refieren específicamente a la norma ISO 9001, ISO 14001 y OHSAS 18001, por tratarse de los sistemas de gestión más extendidos en el momento de publicación de la norma.

En el Reino Unido, la *British Standards Institution* (BSI) publicó en 2006 la *PAS 99:2006 Publicly Available Specification - Specification of common management system as a framework for Requirements integration* (BSI 2006). Está formada por una especificación de requisitos comunes de los sistemas de gestión y un marco para la integración. Fue desarrollada como respuesta a la demanda del mercado de alinear los procesos y procedimientos de dos o más estándares en una estructura integrada que permitiera operar con mayor eficacia. Los requisitos de *PAS 99:2006* fueron organizados bajo las seis categorías de elementos comunes propuestos en la *ISO Guide 72:2001*. *PAS 99:2006* presenta un marco genérico para organizar de una manera integrada los requisitos comunes de estándares como, por ejemplo, ISO 9001, ISO 14001, OHSAS 18001, entre otros.

En 2008, ISO publicó *The integrated use of management system standards* (ISO 2008). Este libro no es una norma o especificación, sino que presenta las metodologías, herramientas y prácticas extraídas a partir de la experiencia del autor en casos prácticos. Trata algunos de los estándares de sistemas de gestión ISO, como el sistema de gestión de calidad ISO 9001, de gestión medioambiental ISO 14001, de seguridad alimentaria ISO 22000, de cadena de suministro ISO 28000 y de seguridad de la información ISO/IEC 27001.

5.2. Compatibilidad entre los sistemas de gestión de las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001

Las normas ISO 9001:2008, ISO/IEC 20000-1:2011 e ISO/IEC 27001:2005 tratan, en sus capítulos iniciales, la integración de los sistemas de gestión que proponen, con otros sistemas de gestión externos.

La norma ISO 9001:2008, en su apartado 0.4 Compatibilidad con otros sistemas de gestión, hace referencia a la integración con otros sistemas de gestión de la siguiente forma: "Esta norma internacional no incluye requisitos específicos de otros sistemas de gestión, tales como aquellos particulares para la gestión ambiental, gestión de la seguridad y salud ocupacional, gestión financiera o gestión de riesgos. Sin embargo, esta norma internacional permite a una organización alinear o integrar su propio sistema de gestión de la calidad con requisitos de sistemas de gestión relacionados. Es posible para una organización adaptar su(s) sistema(s) de gestión existente(s) con la finalidad de establecer un sistema de gestión de la calidad que cumpla con los requisitos de esta norma internacional".

La norma ISO/IEC 20000-1:2011 hace referencia a la integración de su sistema de gestión con otros sistemas de gestión en su introducción: "Esta parte de la norma ISO/IEC 20000 permite a un proveedor de servicios integrar su SGSTI con los otros sistemas de gestión de la organización. La adopción de un enfoque de procesos integrados y la metodología PDCA permiten que el proveedor de servicios pueda alinear o integrar totalmente las múltiples normas de sistemas de gestión. Por ejemplo, un SGSTI puede ser integrado con un sistema de gestión de calidad basado en ISO 9001 o un sistema de gestión de seguridad de la información basado en ISO/IEC 27001."

La norma ISO/IEC 27001:2005, en su apartado 0.3 Compatibilidad con otros sistemas de gestión, asegura que: "Esta norma internacional sigue las pautas marcadas en las normas ISO 9001:2000 e ISO 14001:2004 para asegurar una implementación integrada y consistente con las mencionadas normas de gestión. Esta norma internacional está diseñada para posibilitar a una organización el adaptar su SGSI a los requisitos de los sistemas de gestión mencionados". Más concretamente, en el anexo C.1 de la misma se muestra la relación entre este estándar y la norma ISO 9001:2000.

Al observar la relación de la norma ISO/IEC 20000-1 con la norma ISO/IEC 27001:2005, ISO lanzó en 2010 un nuevo proyecto para desarrollar una guía de implantación integrada de ambas normas llamado ISO/IEC DIS 27013 *Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*, que actualmente se encuentra aún en fase de desarrollo.

5.3. Revisión sistemática de las iniciativas de integración de los tres sistemas de gestión

Debido a que uno de los objetivos de esta tesis doctoral era identificar los requisitos comunes del SGC, del SGSTI y del SGSI, se creyó conveniente realizar, en primer lugar, una revisión sistemática de la literatura para detectar todas las iniciativas existentes de integración de los sistemas de gestión de las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001. Esta revisión sistemática ha sido llevada a cabo utilizando el protocolo de revisión sistemática que se describe en el anexo A.

5.3.1. Formulación de la pregunta

Cada uno de los elementos que propone describir el protocolo fue específicamente definido con el objetivo de identificar estudios que traten la integración de los sistemas de gestión de los tres estándares bajo estudio.

- Problema: Las organizaciones que ya disponen de un SGC según la norma ISO 9001 operativo y que están interesadas en implantar un SGSTI según la norma ISO/IEC 20000-1 o un SGSI según la norma ISO/IEC 27001, deben satisfacer ciertos requisitos que ya han sido parcial o totalmente implantados, implicando una repetición de tareas.
- Pregunta: ¿Qué iniciativas centradas en la integración de los sistemas de gestión de las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001 existen?
- Palabras clave y sinónimos: ISO 9001, *Quality Management System* (QMS), ISO/IEC 20000-1, *IT Service Management System* (ITSMS), ISO 20000, ISO/IEC 27001, *Information Security Management System* (ISMS), ISO 27000, *Integrated Management System* (IMS).
- Intervención: Analizar los sistemas de gestión integrados que aúnen los tres sistemas de gestión anteriores.
- Control: No existen datos iniciales para esta revisión sistemática.
- Efecto: Identificar todas las iniciativas, marcos y modelos que definen un sistema de gestión integrado de acuerdo con los requisitos de los tres sistemas de gestión anteriores.
- Métrica de salida: El número de estudios, iniciativas y sistemas de gestión integrados identificados.
- Población: El conjunto de artículos relacionados con la integración de los sistemas de gestión de las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001 que hayan sido publicados en la lista de fuentes seleccionadas para ejecutar la revisión sistemática.
- Aplicación: Organizaciones de cualquier tipo o tamaño que hayan implantado un sistema de gestión de la calidad según la norma ISO 9001 y que estén interesadas en minimizar los esfuerzos de implantación al adoptar las normas ISO/IEC 20000-1 y/o ISO/IEC 27001. Investigadores que trabajen en modelos de calidad, gestión de servicios de TI o en seguridad de la información.
- Diseño experimental: No se aplicará ningún método de análisis estadístico.

5.3.2. Selección de las fuentes

Las fuentes seleccionadas para ejecutar las búsquedas de estudios primarios se listan en la tabla A.1 del anexo A. A partir de las palabras clave definidas en la fase anterior, y haciendo combinaciones con los operadores lógicos "AND" y "OR", se obtuvieron las cadenas de búsqueda que se muestran en la tabla 5.1.

Cadenas de búsqueda
("ISO 9001" and "ISO 20000" and ("ISO 27000" or "ISO 27001")) and ("IMS" or "integrated management system")
("QMS" or "quality management system") and ("ITSMS" or "SMS" or "service management") and ("ISMS" or "information security") and ("IMS" or "integrated")

Tabla 5.1. Cadenas de búsqueda para la revisión sistemática

5.3.3. Selección de los estudios

Los criterios que permitieron evaluar los estudios para decidir si debían ser seleccionados (Criterios de Inclusión, CI) o descartados (Criterios de Exclusión, CE) se muestran en la tabla 5.2.

Criterio	Descripción
CI1	Incluir artículos cuyo título esté relacionado con la integración de los sistemas de gestión de las normas ISO 9001, ISO 20000-1 e ISO/IEC 27000.
CI2	Incluir artículos que contengan palabras clave que coincidan con las definidas en las cadenas de búsqueda.
CI3	Incluir artículos cuyo resumen esté relacionado con el tema de estudio.
CI4	Incluir artículos que contengan información relacionada con la definición o aplicación de un sistema de gestión integrado.
CE1	Excluir aquellos artículos que se refieren al SGC de la norma ISO 9001, al SGSTI de la norma ISO/IEC 20000-1 o al SGSI de la norma ISO/IEC 27001 de forma separada, sin mostrar ninguna relación entre ambos sistemas de gestión o entre sus requisitos.
CE2	Excluir los artículos duplicados.

Tabla 5.2. Criterios para la inclusión y exclusión de estudios

El proceso seguido para obtener y evaluar los estudios primarios de acuerdo con los criterios de inclusión y exclusión definidos se ilustra como un diagrama de flujo en la figura A.1 del anexo A.

Con respecto a la selección de los estudios primarios, el análisis del título y las palabras clave fueron los principales criterios de inclusión. En caso de que esta información no fuera suficiente para decidir sobre la inclusión o la exclusión del estudio, se analizó el resumen y, cuando fue necesario, el texto completo. Inicialmente se seleccionaron todos los tipos de estudios primarios relacionados con la definición o implantación de un sistema de gestión integrado. Más concretamente, la atención se centró en los estudios que presentaban un SGI que cubriera los requisitos de las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001. La tabla 5.3 muestra la distribución de los estudios obtenidos a partir de cada fuente de búsqueda. Como resultado de la ejecución de la revisión sistemática se obtuvieron 1.064 estudios para una evaluación posterior (ver la columna de "Descubiertos").

Fuente	Fecha de búsqueda	Descubiertos	Relevantes	No repetidos	Primarios
ACM Portal (Digital Library & Guide)	09/05/2011	37	1	1	0
CiteSeerX	10/05/2011	30	11	9	0
Google Scholar	10/05/2011	867	39	17	3
IEEE Computer Society Digital Library	09/05/2011	10	4	4	0
IEEE Xplore	09/05/2011	33	8	8	1
IET Digital Library	10/05/2011	5	1	0	0
SAGE Journals	10/05/2011	1	0	0	0
ScienceDirect	09/05/2011	29	5	5	0
Springer Link	10/05/2011	14	5	5	0
Wiley InterScience	10/05/2011	38	8	8	0
	Total	**1.064**	**82**	**57**	**4**

Tabla 5.3. Distribución de estudios primarios por fuente de búsqueda

Después de aplicar los criterios de inclusión CI1, CI2, CI3 y CI4, definidos en la tabla 5.2, sólo 82 de los 1.064 artículos descubiertos fueron considerados como artículos relevantes. Aplicando el criterio CE2 para la exclusión de los artículos duplicados, se obtuvieron 57 artículos. De éstos, aplicando el criterio CE1, finalmente se seleccionaron 4 como estudios primarios. Estos resultados se muestran en la última fila de la tabla 5.3. La lista completa de los estudios primarios seleccionados se muestra en la tabla 5.4.

Estudio primario		Autores
1	Integrated management systems - Requirement of contemporary business practices (Djapic and Lukic 2008)	Mirko Djapic y Ljubomir Lukic
2	Integrated information management systems - Security and protection of information (Novák 2005)	Ludek Novák
3	Integrated installing ISO 9000 and ISO 27000 management systems on an organization (Wang and Tsai 2009)	Chi-Hsiang Wang y Dwen-Ren Tsai
4	The Development of Business Standardization and Integrated Management Systems (Majstorovic and Marinkovic 2011)	Vidosav D. Majstorovic y Valentina Marinkovic

Tabla 5.4. Estudios primarios obtenidos por la revisión sistemática

5.3.4. Extracción de la información

En la tabla 5.5 se muestran los criterios para extraer la información de los estudios primarios seleccionados (Criterios de Inclusión de la información (Ci_{inf}).

Criterio	Descripción
$CI1_{inf}$	Identificar las iniciativas de integración de sistemas de gestión.
$CI2_{inf}$	Identificar metodologías, técnicas, métodos y procedimientos para implantar y mantener sistemas de gestión integrados.
$CI3_{inf}$	Recopilar información sobre las relaciones entre los requisitos de los sistemas de gestión que han sido integrados.

Tabla 5.5. Criterios para la inclusión de la información de los estudios primarios

Mediante el formulario de extracción de la información que se muestra en el anexo A se registraron los comentarios, las impresiones y las ideas más importantes de cada estudio primario. La tabla 5.6 muestra, para cada estudio primario, el contenido del campo conclusiones del formulario de extracción de la información.

Estudio primario	Campo "Conclusiones" en el formulario de extracción de información
Integrated management systems - Requirement of contemporary business practices (Djapic and Lukic 2008)	*This paper provides an approach to the integration of different standards requirements, based on the interrelation of mutually connected business processes. Integration of several systems into one is more efficient and economical than developing and implementing separate systems. The paper presents and explains several key definitions related to integration aspects. Orientation toward business processes is the key to integration.*

Estudio primario	Campo "Conclusiones" en el formulario de extracción de información
Integrated information management systems - Security and protection of information (Novák 2005)	*This paper tries to find consensus in three different types of management systems: the quality management system, the IT service management system and the information security management system. An aim is to compose a complex framework based on advantages and synergies. Author's experience with integrations of the tree types of management systems into one consistent information management framework is described. The integration is based on similarities of the management systems especially on the PDCA Model, which is a key shared principle. The second principle is an effort to incorporate information risks into each type of systems.*
Integrated installing ISO 9000 and ISO 27000 management systems on an organization (Wang and Tsai 2009)	*In this paper, an integrated management system model suitable for ISO 9001, ISO 27001 and other PDCA based implementations is built. This integrated system model may facilitate the management efficiency of organizations complied with multiple PDCA based management systems. This integrated research work intends to realize the PDCA cyclic management mechanism for integrated ISO management systems.*
The Development of Business Standardization and Integrated Management Systems (Majstorovic and Marinkovic 2011)	*The basic question that is arisen in this paper is how to apply ISO standards in an integrated fashion. This paper deals with the development of individual models of business standardization, and their integration in the design and implementation of IMS, from the viewpoint of quality management requirements, environmental protection, the safety and health protection of employees and some other demands.*

Tabla 5.6. Conclusiones extraídas de los estudios primarios

5.3.5. Resumen de los resultados

Después de la ejecución de la revisión sistemática, se detectaron 1.064 estudios y 4 de ellos fueron considerados como estudios primarios. Los resultados obtenidos muestran un pobre interés por la integración de diferentes sistemas de gestión.

Los estudios primarios obtenidos identifican y determinan las principales razones para la integración y definen marcos y directrices en términos muy abstractos. Estos modelos son definidos siempre a alto nivel, desde una perspectiva muy teórica. Ninguno de ellos proporciona procedimientos operativos específicos y concretos que puedan ser de utilidad a las organizaciones que deseen implantar un sistema de gestión integrado según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001.

Puesto que la integración debe realizarse a nivel de procesos y requisitos, el análisis de los requisitos de los sistemas de gestión a ser integrados es uno de los factores clave para una integración exitosa. Los estudios primarios seleccionados no abordan directamente los requisitos de los tres sistemas de gestión a ser integrados.

Teniendo en cuenta todo lo anterior, los estudios primarios obtenidos por el proceso de revisión sistemática no pueden ser utilizados como punto de partida para alcanzar el objetivo fijado por esta investigación.

5.4. Estudio de las relaciones entre los sistemas de gestión de las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001

Después de años de relaciones y de trabajo continuado en la aplicación de resultados de investigación con algunas empresas del sector TIC de nuestro entorno más próximo, se ha podido observar que, en la mayoría de casos, cuando una empresa decide implantar una norma relativa a la gestión de servicios o a la gestión de la seguridad de la información, ya ha tenido otras experiencias previas, principalmente, la implantación de alguna versión de la norma ISO 9001. Para realizar el trabajo que se presenta en este capítulo se parte de la última versión del estándar, ISO 9001:2008.

5.4.1. Método de investigación

El primer paso de la investigación realizada consistió en realizar un estudio en profundidad de los diferentes sistemas de gestión para determinar las posibilidades de integración. Tal y como se ha mencionado en el apartado 5.2, las tres normas se refieren explícitamente a la compatibilidad con otros sistemas de gestión.

La investigación fue llevada a cabo siguiendo una estrategia iterativa, en la cual:

- cada uno de los requisitos del SGSTI de la norma ISO/IEC 20000-1 fue comparado con todos los requisitos del SGC de la norma ISO 9001, y
- cada uno de los requisitos del SGSI de la norma ISO/IEC 27001 fue comparado con todos los requisitos del SGC de la norma ISO 9001.

Para asegurar una buena trazabilidad entre las normas, este proceso iterativo se llevó a cabo también en la dirección opuesta, es decir, comparando cada uno de los requisitos del SGC de la norma ISO 9001 con todos los requisitos del SGSTI de la norma ISO/IEC 20000-1 y, de manera análoga, con todos los del SGSI de la norma ISO/IEC 27001.

La integración realizada se conoce como integración por conversión, que toma como base el SGC ya existente y lo amplía con los elementos o requisitos del SGSTI o del SGSI. Este tipo de integración permite a las organizaciones reducir los recursos humanos, presupuesto y tiempo necesarios para planificar, implementar y mantener un nuevo sistema de gestión.

5.4.2. Tipos de relaciones

Después de realizar un análisis exhaustivo de los requisitos de los tres sistemas de gestión, se establecieron tres tipos distintos de correspondencias:

- **Relación total ('F')**. En este caso, el requisito del SGSTI de la norma ISO/IEC 20000-1 o del SGSI de la norma ISO/IEC 27001 en cuestión, ya está contemplado por algún requisito del SGC de la norma ISO 9001. En este caso, al definir el nuevo sistema de gestión integrado, no se deberá añadir ningún aspecto específico, referente a la gestión de servicios de TI o a la seguridad de la información, al SGC ya implantado. Un ejemplo de este tipo de relación es el siguiente: La norma ISO/IEC 20000-1:2011 trata los requisitos de la documentación en su apartado 4.3:

  "Los proveedores del servicio deben facilitar documentos y registros para asegurar una planificación, operación y control de la gestión del servicio efectivas".

  Sin embargo, este requisito ya queda cubierto por la norma ISO 9001:2008 en su apartado 4.2.1.d:

  "La documentación del sistema de gestión de la calidad debe incluir los documentos, incluidos los registros que la organización determina que son necesarios para asegurarse de la eficaz planificación, operación y control de sus procesos".

  Del mismo modo, la norma ISO/IEC 27001 también cubre este requisito en su apartado 4.3.1.g:

  "Los procedimientos documentados que necesita la organización para asegurar una correcta planificación, operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles".

- **Relación parcial ('P')**. En este caso, el requisito del SGSTI de la norma ISO/IEC 20000-1 o del SGSI de la norma ISO/IEC 27001 en cuestión, amplía algún requisito del SGC de la norma ISO 9001 con aspectos propios de la gestión de servicios de TI o de la seguridad de la información. Un ejemplo de este tipo de relación es el caso de los requisitos relacionados con el compromiso de la dirección, recogidos en el apartado 5.1 de la norma ISO 9001:2008:

  "La alta dirección debe proporcionar evidencia de su compromiso con el desarrollo e implementación del sistema de gestión de la calidad, así como con la mejora continua de su eficacia:

  a) comunicando a la organización la importancia de satisfacer tanto los requisitos del cliente como los legales y reglamentarios,

b) estableciendo la política de la calidad,

c) asegurando que se establecen los objetivos de la calidad,

d) llevando a cabo las revisiones por la dirección, y

e) asegurando la disponibilidad de recursos."

En este caso, los requisitos del SGC de la norma ISO 9001 deben ser ampliados con aspectos específicos de la gestión de servicios, recogidos en los apartados 4.1.1 de la norma ISO/IEC 20000-1:2011:

"La alta dirección debe proveer, a través del liderazgo y de acciones, evidencias de su compromiso para desarrollar, implementar y mejorar sus capacidades de gestión del servicio dentro del contexto de los requisitos de negocio de la organización y de los requisitos de los clientes. La dirección debe:

a) establecer la política de la gestión del servicio, sus objetivos y planes;

b) comunicar la importancia de cumplir con los objetivos de gestión del servicio y la necesidad de la mejora continua;

c) asegurar que los requisitos del cliente se determinan y se cumplen con el objetivo de mejorar la satisfacción del cliente;

d) designar un miembro de la dirección como responsable para la coordinación y gestión de todos los servicios;

e) determinar y proveer recursos para planificar, implementar, monitorizar, revisar y mejorar la provisión y la gestión de los servicios, por ejemplo, contratando el personal apropiado o gestionando la rotación de personal;

f) gestionar los riesgos para la organización de la gestión del servicio y para los servicios; y

g) llevar a cabo revisiones de la gestión del servicio, a intervalos planificados, para asegurar la continuidad de su idoneidad, su adecuación y su efectividad."

y con aspectos específicos de la seguridad de la información, detallados en el apartado 5.1 de la norma ISO/IEC 27001.

"La Dirección debe suministrar evidencias de su compromiso para crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI, a través de las siguientes acciones:

a) formulando la política del SGSI;

b) velando por el establecimiento de los objetivos y planes del SGSI;

c) estableciendo los roles y responsabilidades en materia de seguridad de la información;

d) comunicando a la organización la importancia de cumplir los objetivos y la

política de seguridad de la información, sus responsabilidades legales y la necesidad de la mejora continua;

e) proporcionando recursos suficientes para crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI;

f) decidiendo los criterios de aceptación de riesgos y los niveles aceptables de riesgo;

g) velando por que se realicen las auditorías internas del SGSI; y

h) dirigiendo las revisiones del SGSI."

- **Inexistencia de relación (‘ ’)**. En este caso, las normas ISO/IEC 20000-1 o ISO/IEC 27001 añaden requisitos propios de la gestión de servicios de TI o de la seguridad de la información no cubiertos por el SGC de la norma ISO 9001. Un ejemplo de este caso se da en la definición de las cuatro etapas de la metodología Planificar-Hacer-Verificar-Actuar (PDCA), introducidas en el apartado 0.2 de la norma ISO 9001:2008:

  "Planificar-Hacer-Verificar-Actuar puede describirse brevemente como:

  Planificar: establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente y las políticas de la organización.

  Hacer: implementar los procesos.

  Verificar: realizar el seguimiento y la medición de los procesos y los productos respecto a las políticas, los objetivos y los requisitos para el producto, e informar sobre los resultados.

  Actuar: tomar acciones para mejorar continuamente el desempeño de los procesos."

  que se amplían con aspectos específicos de la gestión de servicios de TI en los los apartados 4.5.1 a 4.5.5 de la norma ISO/IEC 20000-1:2011:

  "Planificar: Planificar la implementación y la provisión de la gestión del servicio."

  "Hacer: Implementar los objetivos y el plan de gestión del servicio."

  "Verificar: Monitorizar, medir y revisar que los objetivos y el plan de gestión del servicio se están cumpliendo."

  "Actuar: Mejorar la eficacia y la eficiencia de la entrega y de la gestión del servicio."

5.4.3. Relaciones entre los sistemas de gestión de las normas ISO 9001 e ISO/IEC 20000-1

La tabla 5.7 muestra las relaciones detectadas entre los requisitos del SGC de la norma ISO 9001:2008 y los requisitos del SGSTI de la norma ISO/IEC 20000-1:2011. La primera columna contiene todas las cláusulas de la norma ISO 9001. Los valores definidos en la

segunda columna, Tipo de relación, representan la relación existente con los requisitos SGSTI de la norma ISO/IEC 20000-1, que se muestran en la tercera columna. Estos valores son orientativos y no exactos, ya que no todas las organizaciones otorgan la misma importancia o peso a los mismos requisitos dentro de sus sistemas de gestión personalizados. Cabe destacar que las normas que definen sistemas de gestión establecen qué es lo que se tiene que cumplir, pero no cómo se debe llevar a cabo.

Una organización con un SGC según la norma ISO 9001 que desee implantar un SGSTI según la norma ISO/IEC 20000-1 deberá:

- ampliar el alcance del SGC ya existente teniendo en cuenta los requisitos de la norma ISO/IEC 20000-1 parcialmente relacionados e
- integrar todos los demás requisitos del SGSTI aplicables a la organización que no aparezcan en la tercera columna de la tabla.

Como resultado, la organización habrá implantado un SGI con una reducción sustancial de duplicidades e inconsistencias, y con un importante ahorro de esfuerzos y recursos en el momento de la implantación.

ISO/IEC 9001:2008		**Tipo de relación**	**ISO/IEC 20000-1:2011**	
Introducción	**0**			
Generalidades	0.1			
Enfoque basado en procesos	0.2	**P**	4.5	Establecer y mejorar el SGS
Relación con la norma ISO 9004	0.3			
Compatibilidad con otros sistemas de gestión	0.4			
Objeto y campo de aplicación	**1**	**P**	1	Objeto y campo de aplicación
Generalidades	1.1	**P**	1.1	Generalidades
Aplicación	1.2	**P**	1.2	Aplicación
Normas para consulta	**2**			
Términos y definiciones	**3**			
Sistema de gestión de calidad	**4**			
Requisitos generales	4.1			
Requisitos de la documentación	4.2	**P**	4.3	Gestión de la documentación
Generalidades	4.2.1	**P**	4.3.1	Establecer y mantener documentos

ISO/IEC 9001:2008		**Tipo de relación**	**ISO/IEC 20000-1:2011**	
Manual de la calidad	4.2.2	**P**	4.3.1	Establecer y mantener documentos
Control de los documentos	4.2.3	**P**	4.3.2	Control de documentos
Control de los registros	4.2.4	**P**	4.3.3	Control de registros
Responsabilidad de la dirección	**5**	**P**	4.1	Responsabilidad de la dirección
Compromiso de la dirección	5.1	**P**	4.1.1	Compromiso de la dirección
Enfoque al cliente	5.2	**T**	4.1.1	Compromiso de la dirección
Política de calidad	5.3	**P**	4.1.2	Política de gestión de servicios
Planificación	5.4			
Objetivos de la calidad	5.4.1	**P**	4.5.2	Planificación del SGS (Plan)
Planificación del sistema de gestión de la calidad	5.4.2	**P**	4.5.2	Planificación del SGS (Plan)
Responsabilidad, autoridad y comunicación	5.5			
Responsabilidad y autoridad	5.5.1	**P**	4.1.3	Autoridad, responsabilidad y comunicación
Representante de la dirección	5.5.2	**T**	4.1.4	Representante de la dirección
Comunicación interna	5.5.3			
Revisión por la dirección	5.6			
Generalidades	5.6.1			
Información de entrada para la revisión	5.6.2			
Resultados de la revisión	5.6.3			
Gestión de los recursos	**6**	**P**	4.4	Gestión de los recursos
Provisión de recursos	6.1	**T**	4.4.1	Provisión de recursos
Recursos humanos	6.2	**P**	4.4.2	Recursos humanos
Generalidades	6.2.1	**P**	4.4.2	Recursos humanos
Competencia, formación y toma de conciencia	6.2.2	**P**	4.4.2	Recursos humanos
Infraestructura	6.3			
Ambiente de trabajo	6.4			
Realización del producto	**7**			
Planificación de la realización del producto	7.1			
Procesos relacionados con el cliente	7.2			

ISO/IEC 9001:2008		**Tipo de relación**	**ISO/IEC 20000-1:2011**	
Determinación de los requisitos relacionados con el producto	7.2.1			
Revisión de los requisitos relacionados con el producto	7.2.2			
Comunicación con el cliente	7.2.3			
Diseño y desarrollo	7.3	**P**	5	Diseño y transición de nuevos servicios o de servicios modificados
Planificación del diseño y desarrollo	7.3.1			
Elementos de entrada para el diseño y desarrollo	7.3.2			
Resultados del diseño y desarrollo	7.3.3			
Revisión del diseño y desarrollo	7.3.4			
Verificación del diseño y desarrollo	7.3.5			
Validación del diseño y desarrollo	7.3.6			
Control de los cambios del diseño y desarrollo	7.3.7			
Compras	7.4			
Proceso de compras	7.4.1			
Información de las compras	7.4.2			
Verificación de los productos comprados	7.4.3			
Producción y prestación del servicio	7.5	**P**	4.5.3	Implementación y operación del SGS (Do)
Control de la producción y de la prestación del servicio	7.5.1			
Validación de los procesos de la producción y de la prestación del servicio	7.5.2			
Identificación y trazabilidad	7.5.3			
Propiedad del cliente	7.5.4			
Preservación del producto	7.5.5			
Control de los equipos de seguimiento y de medición	7.6			
Medición, análisis y mejora	**8**			

ISO/IEC 9001:2008		Tipo de relación	ISO/IEC 20000-1:2011	
Generalidades	8.1			
Seguimiento y medición	8.2			
Satisfacción del cliente	8.2.1			
Auditoría interna	8.2.2	**P**	4.5.4	Monitorización y revisión del SGS (Check)
Seguimiento y medición de los procesos	8.2.3	**P**	4.5.4	Monitorización y revisión del SGS (Check)
Seguimiento y medición del producto	8.2.4			
Control del producto no conforme	8.3			
Análisis de datos	8.4			
Mejora	8.5	**P**	4.5.5	Mantenimiento y mejora del SGS (Act)
Mejora continua	8.5.1	**P**	4.5.5	Mantenimiento y mejora del SGS (Act)
Acción correctiva	8.5.2			
Acción preventiva	8.5.3			

Tabla 5.7. Relaciones entre los sistemas de gestión de las normas ISO 9001:2008 e ISO/IEC 20000-1:2011

5.4.4. Relaciones entre los sistemas de gestión de las normas ISO 9001 e ISO/IEC 27001

La tabla 5.8 muestra las relaciones detectadas entre los requisitos del SGC de la norma ISO 9001:2008 y los requisitos del SGSI de la norma ISO/IEC 27001:2005. La primera columna contiene todas las cláusulas de la norma ISO 9001. Los valores definidos en la segunda columna, Tipo de relación, representan la relación existente con los requisitos SGSI de la norma ISO/IEC 27001, que se muestran en la tercera columna. Del mismo modo que en el apartado anterior, una organización con un SGC según la norma ISO 9001 que desee implantar un SGSI según la norma ISO/IEC 27001 deberá:

- ampliar el alcance del SGC ya existente teniendo en cuenta los requisitos de la norma ISO/IEC 27001 parcialmente relacionados e
- integrar todos los demás requisitos del SGSI aplicables a la organización que no aparezcan en la tercera columna de la tabla.

ISO/IEC 9001:2008		Tipo de relación	ISO/IEC 27001:2005	
Introducción	**0**			
Generalidades	0.1			
Enfoque basado en procesos	0.2	**P**	0	Enfoque por proceso
Relación con la norma ISO 9004	0.3			
Compatibilidad con otros sistemas de gestión	0.4			
Objeto y campo de aplicación	**1**			
Generalidades	1.1			
Aplicación	1.2			
Normas para consulta	**2**			
Términos y definiciones	**3**	**P**	3	Términos y definiciones
Sistema de gestión de calidad	**4**	**P**	4	Sistema de gestión de seguridad de la información
Requisitos generales	4.1	**P**	4.1	Requisitos generales
Requisitos de la documentación	4.2	**P**	4.3	Requisitos de la documentación
Generalidades	4.2.1	**P**	4.3.1	Generalidades
Manual de la calidad	4.2.2	**P**	4.2.1	Creación del SGSI
Control de los documentos	4.2.3	**T**	4.3.2	Control de documentos
Control de los registros	4.2.4	**T**	4.3.3	Control de registros
Responsabilidad de la dirección	**5**			
Compromiso de la dirección	5.1	**P**	5.1	Compromiso de la dirección
Enfoque al cliente	5.2			
Política de calidad	5.3	**P**	4.2.1	Creación del SGSI
Planificación	5.4			
Objetivos de la calidad	5.4.1			
Planificación del sistema de gestión de la calidad	5.4.2			
Responsabilidad, autoridad y comunicación	5.5			
Responsabilidad y autoridad	5.5.1			
Representante de la dirección	5.5.2			
Comunicación interna	5.5.3			
Revisión por la dirección	5.6	**T**	7	Revisión del SGSI por la dirección

ISO/IEC 9001:2008		**Tipo de relación**	**ISO/IEC 27001:2005**	
Generalidades	5.6.1	**T**	7.1	Generalidades
Información de entrada para la revisión	5.6.2	**P**	7.2	Datos iniciales de la revisión
Resultados de la revisión	5.6.3	**P**	7.3	Resultados de la revisión
Gestión de los recursos	**6**	**P**	5.2	Gestión de los recursos
Provisión de recursos	6.1	**P**	5.2.1	Provisión de los recursos
Recursos humanos	6.2			
Generalidades	6.2.1			
Competencia, formación y toma de conciencia	6.2.2	**T**	5.2.2	Concienciación, formación y capacitación
Infraestructura	6.3			
Ambiente de trabajo	6.4			
Realización del producto	**7**			
Planificación de la realización del producto	7.1			
Procesos relacionados con el cliente	7.2			
Determinación de los requisitos relacionados con el producto	7.2.1			
Revisión de los requisitos relacionados con el producto	7.2.2			
Comunicación con el cliente	7.2.3			
Diseño y desarrollo	7.3			
Planificación del diseño y desarrollo	7.3.1			
Elementos de entrada para el diseño y desarrollo	7.3.2			
Resultados del diseño y desarrollo	7.3.3			
Revisión del diseño y desarrollo	7.3.4			
Verificación del diseño y desarrollo	7.3.5			
Validación del diseño y desarrollo	7.3.6			
Control de los cambios del diseño y desarrollo	7.3.7			
Compras	7.4			
Proceso de compras	7.4.1			

ISO/IEC 9001:2008		Tipo de relación	ISO/IEC 27001:2005	
Información de las compras	7.4.2			
Verificación de los productos comprados	7.4.3			
Producción y prestación del servicio	7.5			
Control de la producción y de la prestación del servicio	7.5.1			
Validación de los procesos de la producción y de la prestación del servicio	7.5.2			
Identificación y trazabilidad	7.5.3			
Propiedad del cliente	7.5.4			
Preservación del producto	7.5.5			
Control de los equipos de seguimiento y de medición	7.6			
Medición, análisis y mejora	**8**			
Generalidades	8.1	**P**	4.2.4	Mantenimiento y mejora del SGSI
Seguimiento y medición	8.2			
Satisfacción del cliente	8.2.1			
Auditoría interna	8.2.2	**T**	6	Auditorías internas
Seguimiento y medición de los procesos	8.2.3			
Seguimiento y medición del producto	8.2.4			
Control del producto no conforme	8.3			
Análisis de datos	8.4			
Mejora	8.5	**P**	8	Mejora del SGSI
Mejora continua	8.5.1	**T**	8.1	Mejora continua
Acción correctiva	8.5.2	**T**	8.2	Acción correctiva
Acción preventiva	8.5.3	**T**	8.3	Acción preventiva

Tabla 5.8. Relaciones entre los sistemas de gestión de las normas ISO 9001:2008 e ISO/IEC 27001:2005

5.5. El nuevo sistema de gestión integrado

El sistema de gestión integrado resultante de esta investigación parte de los requisitos del SGC propuesto por la norma ISO 9001:2008 y los amplía con todos los requisitos específicos de gestión de servicios de TI y de gestión de seguridad de la información que describen las normas ISO/IEC 20000-1:2011 e ISO/IEC 27001:2005 respectivamente. La tabla 5.9 muestra el nuevo sistema de gestión integrado obtenido.

- La primera columna muestra los requisitos del SGC de la norma ISO 9001:2008.
- La segunda columna muestra las ampliaciones sobre los requisitos del SGC de la norma ISO 9001 con los aspectos propios de la gestión de servicios de TI de la norma ISO/IEC 20000-1:2011.
- La tercera columna muestra las ampliaciones sobre los requisitos del SGC de la norma ISO 9001 con los aspectos propios de la gestión de la seguridad de la información de la norma ISO/IEC 27001:2005.

ISO/IEC 9001:2008	ISO/IEC 20000-1:2011	ISO/IEC 27001:2005
0 Introducción		
0.1 Generalidades		
0.2 Enfoque basado en procesos	4.5 Establecer y mejorar el SGS	0 Enfoque por proceso
0.3 Relación con la Norma ISO 9004		
0.4 Compatibilidad con otros sistemas de gestión		
1 Objeto y campo de aplicación	1 Objeto y campo de aplicación	
1.1 Generalidades	1.1 Generalidades	
1.2 Aplicación	1.2 Aplicación	
2 Normas para consulta		
3 Términos y definiciones		3 Términos y definiciones
4 Sistema de gestión de la calidad		4 Sistema de gestión de seguridad de la información
4.1 Requisitos generales		4.1 Requisitos generales
4.2 Requisitos de la documentación	4.3 Gestión de la documentación	4.3 Requisitos de la documentación
4.2.1 Generalidades	4.3.1 Establecer y mantener documentos	4.3.1 Generalidades
4.2.2 Manual de la calidad	4.3.1 Establecer y mantener documentos	4.2.1 Creación del SGSI

ISO/IEC 9001:2008	ISO/IEC 20000-1:2011	ISO/IEC 27001:2005
4.2.3 Control de los documentos	4.3.2 Control de documentos	4.3.2 Control de documentos
4.2.4 Control de los registros	4.3.3 Control de registros	4.3.3 Control de registros
5 Responsabilidad de la dirección	4.1 Responsabilidad de la dirección	
5.1 Compromiso de la dirección	4.1.1 Compromiso de la dirección	5.1 Compromiso de la dirección
5.2 Enfoque al cliente	4.1.1 Compromiso de la dirección	
5.3 Política de la calidad	4.1.2 Política de gestión de servicios	4.2.1 Creación del SGSI
5.4 Planificación		
5.4.1 Objetivos de la calidad	4.5.2 Planificación del SGS (Plan)	
5.4.2 Planificación del sistema de gestión de la calidad	4.5.2 Planificación del SGS (Plan)	
5.5 Responsabilidad, autoridad y comunicación		
5.5.1 Responsabilidad y autoridad	4.1.3 Autoridad, responsabilidad y comunicación	
5.5.2 Representante de la dirección	4.1.4 Representante de la dirección	
5.5.3 Comunicación interna		
5.6 Revisión por la dirección		7 Revisión del SGSI por la dirección
5.6.1 Generalidades		7.1 Generalidades
5.6.2 Información de entrada para la revisión		7.2 Datos iniciales de la revisión
5.6.3 Resultados de la revisión		7.3 Resultados de la revisión
6 Gestión de los recursos	4.4 Gestión de los recursos	5.2 Gestión de los recursos
6.1 Provisión de recursos	4.4.1 Provisión de recursos	5.2.1 Provisión de los recursos
6.2 Recursos humanos	4.4.2 Recursos humanos	
6.2.1 Generalidades	4.4.2 Recursos humanos	
6.2.2 Competencia, formación y toma de conciencia	4.4.2 Recursos humanos	5.2.2 Concienciación, formación y capacitación
6.3 Infraestructura		
6.4 Ambiente de trabajo		

ISO/IEC 9001:2008	ISO/IEC 20000-1:2011	ISO/IEC 27001:2005
7 Realización del producto		
7.1 Planificación de la realización del producto		
7.2 Procesos relacionados con el cliente		
7.2.1 Determinación de los requisitos relacionados con el producto		
7.2.2 Revisión de los requisitos relacionados con el producto		
7.2.3 Comunicación con el cliente		
7.3 Diseño y desarrollo	5 Diseño y transición de nuevos servicios o de servicios modificados	
7.3.1 Planificación del diseño y desarrollo		
7.3.2 Elementos de entrada para el diseño y desarrollo		
7.3.3 Resultados del diseño y desarrollo		
7.3.4 Revisión del diseño y desarrollo		
7.3.5 Verificación del diseño y desarrollo		
7.3.6 Validación del diseño y desarrollo		
7.3.7 Control de los cambios del diseño y desarrollo		
7.4 Compras		
7.4.1 Proceso de compras		
7.4.2 Información de las compras		
7.4.3 Verificación de los productos comprados		
7.5 Producción y prestación del servicio	4.5.3 Implementación y operación del SGS (Do)	
7.5.1 Control de la producción y de la prestación del servicio		

ISO/IEC 9001:2008	ISO/IEC 20000-1:2011	ISO/IEC 27001:2005
7.5.2 Validación de los procesos de la producción y prestación del servicio		
7.5.3 Identificación y trazabilidad		
7.5.4 Propiedad del cliente		
7.5.5 Preservación del producto		
7.6 Control de los equipos de seguimiento y de medición		
8 Medición, análisis y mejora		
8.1 Generalidades		4.2.4 Mantenimiento y mejora del SGSI
8.2 Seguimiento y medición		
8.2.1 Satisfacción del cliente		
8.2.2 Auditoría interna	4.5.4 Monitorización y revisión del SGS (Check)	6 Auditorías internas
8.2.3 Seguimiento y medición de los procesos	4.5.4 Monitorización y revisión del SGS (Check)	
8.2.4 Seguimiento y medición del producto		
8.3 Control del producto no conforme		
8.4 Análisis de datos		
8.5 Mejora	4.5.5 Mantenimiento y mejora del SGS (Act)	8 Mejora del SGSI
8.5.1 Mejora continua	4.5.5 Mantenimiento y mejora del SGS (Act)	8.1 Mejora continua
8.5.2 Acción correctiva		8.2 Acción correctiva
8.5.3 Acción preventiva		8.3 Acción preventiva

Tabla 5.9. Sistema de Gestión Integrado según las normas ISO 9001:2008, ISO/IEC 20000-1:2011 e ISO/IEC 27001:2005

Es importante observar que el sistema de gestión integrado también deberá contemplar los requisitos propios de la gestión de servicios de TI de la norma ISO/IEC 20000-1:2011 y de la gestión de seguridad de la información de la norma ISO/IEC 27001:2005. Estos requisitos son los que no guardan ninguna relación con ningún requisito del SGC de la norma ISO 9001, es decir, el tercer tipo de relación descrito en el apartado 5.4.2.

5.6. Guías de soporte a la implantación de sistemas de gestión integrados

Con el objetivo de ofrecer una aproximación incremental a la integración de sistemas de gestión, a partir de todas las relaciones extraídas durante la investigación, se elaboraron dos guías de soporte a la implantación efectiva de sistemas de gestión integrados:

- La primera de ellas, *Guía para la integración del Sistema de Gestión de Servicios de TI de la norma ISO/IEC 20000-1 con el Sistema de Gestión de Calidad de la norma ISO 9001*, ha sido diseñada con el objetivo de implantar el SGSTI que propone la norma ISO/IEC 20000-1 de forma integrada con el SGC de la norma ISO 9001. Se ofrece más información sobre esta guía en el anexo E.
- La segunda guía, *Guía para la integración del Sistema de Gestión de Seguridad de la Información de la norma ISO/IEC 270001 con el Sistema de Gestión de Calidad de la norma ISO 9001*, pretende facilitar la implantación integrada del SGSI de la norma ISO/IEC 27001 con el SGC de la norma ISO 9001. Se ofrece más información sobre esta guía en el anexo E.

Ambas guías siguen la filosofía y estructura utilizadas por ISO en sus guías de aplicación de la norma ISO 9001, tales como *ISO/IEC 90003:2004 Software engineering - Guidelines for the application of ISO 9001:2000 to computer software* (ISO90003 2004) e *ISO/IEC TR 90005:2008 Systems engineering - Guidelines for the application of ISO 9001 to system life cycle processes* (ISO90005 2008). Estos dos documentos proporcionan una guía para las organizaciones en la aplicación de la norma ISO 9001:2000 a la adquisición, suministro, desarrollo, operación y mantenimiento de software y sistemas, respectivamente.

La figura 5.2 muestra la información que proporciona cada una de las guías para cada requisito de la norma ISO 9001:2008, y contiene:

- El título y el contenido de la sección de la norma ISO/IEC 9001:2008.
- El tipo de relación con la norma ISO/IEC 20000-1:2011 o ISO/IEC 27001:2005.
- Una explicación detallada de los requisitos del SGSTI o del SGSI que deben ser añadidos a los requisitos del SGC ya implantado en la organización.
- El texto del(los) requisito(s) de la norma ISO/IEC 20000-1:2011 o ISO/IEC 27001:2005 relacionados. Esta información únicamente aparece en caso de una relación parcial.

ISO 9001:2008 Sistemas de gestión de la calidad - Requisitos

<Título de la sección de la norma ISO 9001:2008>

<Contenido de la sección>

Relación: <Tipo de relación detectada>

Observaciones: <Descripción de la relación detectada>

<Texto del(los) requisito(s) de la norma ISO/IEC 20000-1:2011 o ISO/IEC 27001:2005 relacionado(s)>

Figura 5.2. Información proporcionada por las guías para cada requisito de la norma ISO 9001

5.7. Resultados y discusión

Durante esta investigación se ha podido observar que tanto el SGC de la norma ISO 9001, el SGSTI de la norma ISO/IEC 20000-1 como el SGSI de la norma ISO/IEC 27001 pueden ser conectados e integrados, debido a que todos ellos siguen una orientación a procesos y se basan en el ciclo PDCA.

El nuevo sistema de gestión integrado resultante de este trabajo toma como base los requisitos del SGC propuestos por la norma ISO 9001 y los amplía con todos los requisitos específicos de gestión de servicios de TI y de gestión de seguridad de la información. Los requisitos de los tres sistemas de gestión que han sido integrados en mayor grado son los que hacen referencia a:

- la gestión de la documentación,
- la responsabilidad y el compromiso de la dirección,
- la provisión de recursos materiales,
- la concienciación, formación y capacitación de los recursos humanos,
- la monitorización, revisión y realización de auditorías internas y
- la definición de acciones de mejora correctivas y preventivas.

El esfuerzo necesario para implantar el sistema de gestión integrado es mucho menor que el esfuerzo que supondría implantar los tres sistemas de gestión de manera independiente. Los principales beneficios derivados del nuevo sistema de gestión integrado son:

- ahorro significativo de costes,
- aumento de la flexibilidad, la eficiencia y la coherencia,
- creación de sinergias entre los tres sistemas de gestión e

- integración de políticas y controles operativos.

Las guías de soporte a la implantación de sistemas de gestión integrados desarrolladas especifican las acciones concretas que se deben llevar a cabo para obtener una integración eficiente. Estas guías pueden ser de utilidad a las organizaciones para:

- facilitar la compatibilidad entre sus sistemas de gestión,
- alinear sus objetivos,
- facilitar la toma de decisiones y
- reducir los recursos necesarios para su implantación, gestión y mantenimiento.

Capítulo 6. Aplicación del Modelo Integrado de Estándares de Gestión de TI

6.1 Características de las empresas

6.2 Aplicación del Modelo Integrado de Estándares de Gestión de TI

En este capítulo se presenta la aplicación de los resultados obtenidos durante la investigación realizada en esta tesis doctoral en dos empresas de desarrollo de software de las Illes Balears.

El contacto mantenido desde el año 2002 con las empresas de las Illes Balears que han participado en las sucesivas ediciones del proyecto QuaSAR, ha propiciado la consolidación de un entorno de colaboración que ha facilitado la aplicación de nuestras investigaciones en entornos de producción real.

En este capítulo se analiza la validez del modelo desarrollado en esta tesis doctoral, a partir de su aplicación en dos empresas de desarrollo de software. Más concretamente, se muestran los resultados de la utilización de los siguientes productos obtenidos durante el desarrollo del modelo:

- Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-4.
- *ISO/IEC 15504 Security Extension*.
- Guía para la implantación del Sistema de Gestión de Servicios de TI de la norma ISO/IEC 20000-1 con el Sistema de Gestión de Calidad de la norma ISO 9001.
- Guía para la implantación del Sistema de Gestión de Seguridad de la Información de la norma ISO/IEC 27001 con el Sistema de Gestión de Calidad de la norma ISO 9001.

Es importante observar que debido a que cada organización puede tener un punto de partida distinto (uno o diversos estándares ya implantados) y diferentes objetivos a cumplir (alcanzar una determinada certificación), el modelo desarrollado ofrece diversas posibilidades de parametrización con el objetivo de ser versátil y adaptable al mayor número de organizaciones posible.

En la sección 6.1 se presentan las compañías en el que se ha aplicado el nuevo Modelo Integrado de Estándares de Gestión de TI. En la sección 6.2 se muestran los resultados obtenidos de la aplicación del modelo en estas empresas.

6.1. Características de las empresas

Las dos empresas en las que se ha aplicado el modelo desarrollado, iniciaron un programa de mejora de procesos de software según el estándar internacional ISO/IEC 15504 gracias a las ayudas públicas del Plan Avanza. La primera empresa inició la implantación de esta norma a finales del año 2007, mientras que la segunda lo hizo a finales de 2008.

Hasta la fecha, ambas empresas han seguido trabajando en la mejora de sus procesos y en el despliegue de éstos en todos los proyectos de la organización.

6.1.1. Empresa E1

E1 es una empresa que inició su actividad en el año 2000. Hoy en día, E1 cuenta con 82 empleados dedicados al desarrollo de aplicaciones basadas en Internet y a la implementación de la infraestructura que les da soporte. La implantación de un sistema de gestión de la calidad y la posterior certificación según la norma ISO 9000 obtenida por la empresa en el año 2002 se ha convertido en una de las principales señas de identidad de E1 como empresa: la calidad como estrategia de gestión. En 2005 la compañía introdujo el Modelo de Excelencia EFQM a su sistema de gestión y al final de 2007 inició la adaptación de sus procesos de acuerdo al estándar internacional ISO/IEC 15504. En 2009 la empresa implantó un sistema de gestión de seguridad de la información según la norma ISO/IEC 27001 y obtuvo esta certificación. Actualmente está considerando certificarse según la norma ISO/IEC 20000-1.

La tabla 6.1 muestra la capacidad que tenían a finales de 2009 los catorce procesos de la norma ISO/IEC 15504-5 implantados en E1.

Procesos de la norma ISO/IEC 15504-5 implantados	Nivel de capacidad
ACQ.3 Acuerdo contractual	1
ACQ.4 Monitorización del proveedor	1
ACQ.5 Aceptación del cliente	1
SPL.2 Entrega del producto	2
ENG.1 Captura de requisitos	1
ENG.4 Análisis de requisitos del software	1
ENG.8 Pruebas del software	1
ENG.11 Instalación del sistema	1
ENG.12 Mantenimiento del software y el sistema	1
MAN.3 Gestión de proyectos	1
MAN.5 Gestión de riesgos	2
SUP.1 Aseguramiento de la calidad	2
SUP.7 Documentación	2
SUP.9 Gestión de la resolución de problemas	1

Tabla 6.1. Capacidad de los procesos de la norma ISO/IEC 15504-5 implantados en E1

6.1.2. Empresa E2

E2 es una empresa de desarrollo de software que inició su actividad en el año 2004. Cuenta con un equipo joven de 30 empleados con diferentes perfiles profesionales del sector de las TI. La compañía ha llevado a cabo numerosos proyectos, tanto para la administración pública de las Islas Baleares como para otras organizaciones privadas de todo tipo de sectores, pero especialmente para el sector turístico. Por otra parte, ha desarrollado algunos de sus propios sistemas de información para la gestión interna.

La tabla 6.2 muestra la capacidad a finales de 2009 de los ocho procesos de la norma ISO/IEC 15504-5 implantados en E2.

Procesos de la norma ISO/IEC 15504-5 implantados	Nivel de capacidad
ENG.1 Captura de requisitos	2
ENG.4 Análisis de requisitos del software	2
ENG.5 Diseño de software	1
ENG.8 Pruebas del software	1
MAN.3 Gestión de proyectos	1
SUP.4 Revisión conjunta	1
SUP.8 Gestión de la configuración	1
SUP.9 Gestión de la resolución de problemas	1

Tabla 6.2. Capacidad de los procesos de la norma ISO/IEC 15504-5 implantados en E2

6.2. Aplicación del Modelo Integrado de Estándares de Gestión de TI

En esta sección se presenta la experiencia extraída de la aplicación del Modelo Integrado de Estándares de Gestión de TI en las empresas E1 y E2. Dado que el punto de partida en cuanto a los estándares implantados difiere bastante de una empresa a otra, no se han aplicado y validado los mismos productos en las dos empresas. Así pues, los resultados que se presentan en esta sección son de gran utilidad para demostrar la versatilidad del modelo desarrollado durante esta investigación.

6.2.1. Aplicación en E1

Al iniciar la aplicación de los resultados de esta tesis doctoral en E1, la empresa ya disponía de los siguientes estándares implantados: ISO/IEC 9001, ISO/IEC 15504-5 e ISO/IEC 27001. Además, estaba decidida a implantar la norma ISO/IEC 20000-1.

Así pues, en esta empresa se han podido aplicar los siguientes productos obtenidos durante el desarrollo del Modelo Integrado de Estándares de Gestión de TI:

- *ISO/IEC 15504 Security Extension*. Al ya disponer de la certificación ISO/IEC 27001 la empresa aplicó la *ISO/IEC 15504 Security Extension* para validar su utilidad, completitud, e idoneidad.
- Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5. Al estar también interesada en implantar la norma ISO/IEC 20000, la empresa ha utilizado este mapa para determinar los esfuerzos de implantación que puede aprovechar gracias a tener algunos procesos de la norma ISO/IEC 15504-5 ya implantados a un cierto nivel de capacidad y los esfuerzos adicionales que debería realizar para desplegar las buenas prácticas de gestión de servicios de TI de la norma ISO/IEC 20000 no contemplados hasta la fecha.
- Guías para la implantación de sistemas de gestión integrados a partir de la norma ISO 9001. Al disponer la empresa de un sistema de gestión de calidad según la norma ISO 9001 y de un sistema de gestión de seguridad de la información según la norma ISO/IEC 27001, la empresa podrá utilizar, una vez iniciada la implantación de la norma ISO/IEC 20000-1, la *Guía para la implantación del Sistema de Gestión de Servicios de TI de la norma ISO/IEC 20000-1 con el Sistema de Gestión de Calidad de la norma ISO 9001* para localizar los requisitos compartidos del nuevo sistema de gestión de servicios de TI con los ya existentes, y facilitar la integración de todos ellos en un único sistema de gestión integrado.

A continuación se muestran los resultados de la utilización de estos productos.

6.2.1.1. Aplicación de la *ISO/IEC 15504 Security Extension*

E1 utilizó la *ISO/IEC 15504 Security Extension* para identificar y validar los controles de seguridad de la norma ISO/IEC 27002 que se habían desplegado sobre cada uno de los procesos de la norma ISO/IEC 15504-5 ya implantados en la organización. Además, la empresa pudo observar que existían otros nuevos controles de seguridad no contemplados hasta la fecha que serían fácilmente desplegables sobre estos procesos.

La tabla 6.3 muestra, una vez aplicada la *ISO/IEC 15504 Security Extension*, los controles de seguridad de la norma ISO/IEC 27002 desplegados sobre los procesos de la norma ISO/IEC 15504-5 ya implantados en E1. Un total de 36 controles de seguridad de la norma ISO/IEC 27002 han sido desplegados sobre doce de los catorce procesos de la norma ISO/IEC 15504-5 implantados. Los procesos ENG.12 Mantenimiento del software y el

sistema y MAN.3 Gestión de proyectos, no pudieron utilizarse para facilitar la implantación de ningún control, al no estar estos dos procesos directamente relacionados con la gestión de la seguridad de la información.

Procesos de la norma ISO/IEC 15504-5 implantados	**Controles de seguridad de la norma ISO/IEC 27002 desplegados sobre el proceso de la norma ISO/IEC 15504-5**
ACQ.3 Acuerdo contractual	6.2.1 Identificación de los riesgos derivados del acceso a terceros 6.2.3 Tratamiento de la seguridad en contratos con terceros 10.2.1 Provisión de servicios 10.6.2 Seguridad de los servicios de red 10.8.2 Acuerdos de intercambio 12.5.5 Externalización del desarrollo de software 15.1.2 Derechos de propiedad intelectual (DPI) 15.1.4 Protección de datos y privacidad de la información personal 15.1.6 Regulación de los controles criptográficos
ACQ.4 Monitorización del proveedor	6.2.1 Identificación de los riesgos derivados del acceso a terceros 10.2.2 Supervisión y revisión de los servicios prestados por terceros 10.2.3 Gestión de cambios en los servicios prestados por terceros 12.5.5 Externalización del desarrollo de software
ACQ.5 Aceptación del cliente	10.3.2 Aceptación del sistema 12.5.5 Externalización del desarrollo de software
SPL.2 Entrega del producto	10.8.3 Soportes físicos en tránsito
ENG.1 Captura de requisitos	10.9.1 Comercio electrónico 10.9.2 Transacciones en línea 10.9.3 Información puesta a disposición pública 12.1.1 Análisis y especificación de los requisitos de seguridad 12.5.4 Fugas de información 15.1.1 Identificación de la legislación aplicable 15.1.2 Derechos de propiedad intelectual (DPI) 15.1.4 Protección de datos y privacidad de la información personal 15.1.6 Regulación de los controles criptográficos
ENG.4 Análisis de requisitos del software	12.1.1 Análisis y especificación de los requisitos de seguridad 12.2.1 Validación de los datos de entrada 12.2.2 Control del procesamiento interno 12.2.3 Integridad de los mensajes 12.2.4 Validación de los datos de salida 12.4.2 Protección de los datos de prueba del sistema 15.1.1 Identificación de la legislación aplicable
ENG.8 Pruebas del software	10.1.4 Separación de los recursos de desarrollo, prueba y operación
ENG.11 Instalación del sistema	12.4.1 Control del software en explotación

Procesos de la norma ISO/IEC 15504-5 implantados	Controles de seguridad de la norma ISO/IEC 27002 desplegados sobre el proceso de la norma ISO/IEC 15504-5
MAN.5 Gestión de riesgos	6.2.1 Identificación de los riesgos derivados del acceso a terceros 12.6.1 Control de las vulnerabilidades técnicas 13.1.1 Notificación de los eventos de seguridad de la información 13.1.2 Notificación de los puntos débiles de la seguridad 13.2.1 Responsabilidades y procedimientos 13.2.2 Aprendizaje de los incidentes de seguridad de la información
SUP.1 Aseguramiento de la calidad	15.2.1 Cumplimiento de las políticas y normas de seguridad
SUP.7 Documentación	10.1.1 Documentación de los procedimientos de operación 10.7.4 Seguridad de la documentación del sistema 15.1.3 Protección de los documentos de la organización
SUP.9 Gestión de la resolución de problemas	13.1.1 Notificación de los eventos de seguridad de la información 13.1.2 Notificación de los puntos débiles de la seguridad 13.2.1 Responsabilidades y procedimientos 13.2.2 Aprendizaje de los incidentes de seguridad de la información 13.2.3 Recopilación de evidencias

Tabla 6.3. Controles de seguridad de la norma ISO/IEC 270002 desplegados sobre los procesos de la norma ISO/IEC 15504-5 implantados en E1

6.2.1.2. Aplicación del mapa de relaciones entre la norma ISO/IEC 20000-4 y la norma ISO/IEC 15504-5

Gracias a la utilización del *Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida de la norma ISO/IEC 15504-5*, la empresa ha podido conocer antes de empezar la implantación de la norma ISO/IEC 20000:

- los esfuerzos de implantación que ya no deberán dedicar gracias a tener ciertos procesos de la norma ISO/IEC 15504-5 previamente implantados.
- los esfuerzos adicionales que deberán llevar a cabo para obtener los resultados de los procesos de gestión de servicios de TI no cubiertos por los procesos del ciclo de vida del software ya implantados.

La tabla 6.4 muestra los resultados de los procesos de la norma ISO/IEC 20000-4 que quedan cubiertos por ocho de los procesos de la norma ISO/IEC 15504-5 ya implantados en E1. Las prácticas básicas de los otros seis procesos implantados, ACQ.3 Acuerdo contractual, ENG.4 Análisis de requisitos del software, ENG.8 Pruebas del software, ENG.11 Instalación del sistema, ENG.12 Mantenimiento del software y el sistema y

SUP.1 Aseguramiento de la calidad, al no estar relacionadas con ningún proceso de la norma ISO/IEC 20000-4, no podrán aprovecharse para facilitar la implantación de ningún proceso de gestión de servicios de TI.

Procesos de la norma ISO/IEC 15504-5 implantados	**Resultados de los procesos de la norma ISO/IEC 20000-4 cubiertos**	
	Proceso	**Resultados cubiertos**
ACQ.4 Monitorización del proveedor	Gestión de suministradores	Resultados 1, 5 y 6
ACQ.5 Aceptación del cliente	Gestión organizativa	Resultado 10
SPL.2 Entrega del producto	Gestión organizativa	Resultado 9
	Gestión de la entrega y del despliegue	Resultados 1, 3, 5 y 8
	Transición del servicio	Resultados 10 y 11
ENG.1 Captura de requisitos	Gestión organizativa	Resultados 1 y 2
	Requisitos del servicio	Resultados 1, 2, 3 y 5
MAN.3 Gestión de proyectos	Gestión organizativa	Resultado 11
	Planificación y monitorización del servicio	Resultados 1, 2, 3, 4, 5, 6, 7 y 8
	Elaboración del presupuesto y contabilidad de los servicios de TI	Resultados 2, 3 y 4
MAN.5 Gestión de riesgos	Gestión organizativa	Resultado 13
	Gestión de riesgos	Resultados 1, 2, 4 y 5
	Gestión de la seguridad de la información	Resultados 2, 3, 4, 5 y 6
	Gestión de problemas	Resultados 1, 2, 3 y 4
SUP.7 Documentación	Gestión de la información	Resultados 1, 2, 3 y 4
	Generación de informes del servicio	Resultados 1, 2, 3 y 4
SUP.9 Gestión de la resolución de problemas	Gestión de incidentes y cumplimiento de peticiones	Resultados 1, 2, 3 y 5
	Gestión de problemas	Resultados 2 y 3

Tabla 6.4. Resultados de los procesos de la norma ISO/IEC 20000-4 cubiertos por los procesos de la norma ISO/IEC 15504-5 implantados en E1

6.2.1.3. Aplicación de las Guías para la implantación de sistemas de gestión integrados a partir de la norma ISO 9001.

Una vez iniciada la implantación de la norma ISO/IEC 20000-1, la empresa podrá utilizar también la *Guía para la implantación del Sistema de Gestión de Servicios de TI de la norma ISO/IEC 20000-1 con el Sistema de Gestión de Calidad de la norma ISO 9001* para facilitar la integración con los sistemas de gestión de las normas ISO 9001 e ISO/IEC 27001 ya implantados.

La tabla 6.5 muestra los requisitos del sistema de gestión de servicios de TI de la norma ISO/IEC 20000-1 que quedan cubiertos por los requisitos de los sistemas de gestión de calidad y de gestión de seguridad de la información ya existentes en E1.

Requisitos de los sistemas de gestión implantados		**Requisitos del sistema de gestión de la norma ISO/IEC 20000-1 cubiertos**
ISO/IEC 9001	**ISO/IEC 27001**	
0.2 Enfoque basado en procesos	0 Enfoque por proceso	4.5 Establecer y mejorar el SGS
1 Objeto y campo de aplicación		1 Objeto y campo de aplicación
1.1 Generalidades		1.1 Generalidades
1.2 Aplicación		1.2 Aplicación
4.2 Requisitos de la documentación	4.3 Requisitos de la documentación	4.3 Gestión de la documentación
4.2.1 Generalidades	4.3.1 Generalidades	4.3.1 Establecer y mantener documentos
4.2.2 Manual de la calidad	4.2.1 Creación del SGSI	4.3.1 Establecer y mantener documentos
4.2.3 Control de los documentos	4.3.2 Control de documentos	4.3.2 Control de documentos
4.2.4 Control de los registros	4.3.3 Control de registros	4.3.3 Control de registros
5 Responsabilidad de la dirección		4.1 Responsabilidad de la dirección
5.1 Compromiso de la dirección	5.1 Compromiso de la dirección	4.1.1 Compromiso de la dirección
5.2 Enfoque al cliente		4.1.1 Compromiso de la dirección
5.3 Política de la calidad	4.2.1 Creación del SGSI	4.1.2 Política de gestión de servicios
5.4.1 Objetivos de la calidad		4.5.2 Planificación del SGS (Plan)
5.4.2 Planificación del sistema de gestión de la calidad		4.5.2 Planificación del SGS (Plan)
5.5.1 Responsabilidad y autoridad		4.1.3 Autoridad, responsabilidad y comunicación

Requisitos de los sistemas de gestión implantados		Requisitos del sistema de gestión de la norma ISO/IEC 20000-1 cubiertos
ISO/IEC 9001	**ISO/IEC 27001**	
5.5.2 Representante de la dirección		4.1.4 Representante de la dirección
6 Gestión de los recursos	5.2 Gestión de los recursos	4.4 Gestión de los recursos
6.1 Provisión de recursos	5.2.1 Provisión de los recursos	4.4.1 Provisión de recursos
6.2 Recursos humanos		4.4.2 Recursos humanos
6.2.1 Generalidades		4.4.2 Recursos humanos
6.2.2 Competencia, formación y toma de conciencia	5.2.2 Concienciación, formación y capacitación	4.4.2 Recursos humanos
7.3 Diseño y desarrollo		5 Diseño y transición de nuevos servicios o de servicios modificados
7.5 Producción y prestación del servicio		4.5.3 Implementación y operación del SGS (Do)
8.2.2 Auditoría interna	6 Auditorías internas	4.5.4 Monitorización y revisión del SGS (Check)
8.2.3 Seguimiento y medición de los procesos		4.5.4 Monitorización y revisión del SGS (Check)
8.5 Mejora	8 Mejora del SGSI	4.5.5 Mantenimiento y mejora del SGS (Act)
8.5.1 Mejora continua	8.1 Mejora continua	4.5.5 Mantenimiento y mejora del SGS (Act)

Tabla 6.5. Requisitos del sistema de gestión de la norma ISO/IEC 20000-1 cubiertos por los sistemas de gestión según las normas ISO 9001 e ISO/IEC 27001 implantados en E1

6.2.2. Aplicación en E2

Al iniciar la aplicación de los resultados de esta tesis doctoral en E2, la empresa no había iniciado la implantación de las normas ISO/IEC 20000-1 e ISO/IEC 27001. Sin embargo, la aplicación del Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5 y de la *ISO/IEC 15504 Security Extension*, le ha permitido valorar los esfuerzos que debería realizar si se planteara iniciar la implantación de estas normas. A continuación se muestran los resultados de la utilización de estos dos resultados.

6.2.2.1. Aplicación del mapa de relaciones entre la norma ISO/IEC 20000-4 y la norma ISO/IEC 15504-5

Antes de iniciar la implantación de la norma ISO/IEC 20000, mediante el *Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida de la norma ISO/IEC 15504-5*, E2 ha podido determinar:

- los esfuerzos de implantación de la norma ISO/IEC 20000-1 que podrá ahorrarse por tener ciertos procesos de la norma ISO/IEC 15504-5 previamente implantados.
- los esfuerzos adicionales que deberán realizar para obtener los resultados de los procesos de la norma ISO/IEC 20000-4 no cubiertos por los procesos del ciclo de vida del software que se muestran en la tabla 6.2 ya implantados.

La tabla 6.6 muestra los resultados de los procesos de la norma ISO/IEC 20000-4 cubiertos por cinco de los procesos de la norma ISO/IEC 15504-5 ya implantados en E2. Las prácticas básicas de los tres procesos ENG.4 Análisis de requisitos del software, ENG.5 Diseño de software y ENG.8 Pruebas del software, al ser propios del área de ingeniería, no facilitan la implantación de resultados de la gestión de servicios de TI.

Procesos de la norma ISO/IEC 15504-5 implantados	**Resultados de los procesos de la norma ISO/IEC 20000-4 cubiertos**	
	Proceso	**Resultados cubiertos**
ENG.1 Captura de requisitos	Gestión organizativa	Resultados 1 y 2
	Requisitos del servicio	Resultados 1, 2, 3 y 5
MAN.3 Gestión de proyectos	Gestión organizativa	Resultado 11
	Planificación y monitorización del servicio	Resultados 1, 2, 3, 4, 5, 6, 7 y 8
	Elaboración del presupuesto y contabilidad de los servicios de TI	Resultados 2, 3 y 4
SUP.4 Revisión conjunta	Revisión de la dirección	Resultados 1, 2, 3, 4 y 5
	Gestión organizativa	Resultado 12
SUP.8 Gestión de la configuración	Gestión de la configuración	Resultados 1, 2, 3 y 5
SUP.9 Gestión de la resolución de problemas	Gestión de incidentes y cumplimiento de peticiones	Resultados 1, 2, 3 y 5
	Gestión de problemas	Resultados 2 y 3

Tabla 6.6. Resultados de los procesos de la norma ISO/IEC 20000-4 cubiertos por los procesos de la norma ISO/IEC 15504-5 implantados en E2

6.2.2.2. Aplicación de la ISO/IEC 15504 Security Extension

Mediante la utilización de la *ISO/IEC 15504 Security Extension*, E2 ha podido identificar los controles de seguridad de la norma ISO/IEC 27002 que se podrían desplegar sobre los procesos de la norma ISO/IEC 15504-5 ya implantados.

La tabla 6.7 muestra los controles de seguridad de la norma ISO/IEC 27002 que se pudieron desplegar sobre los ocho procesos de la norma ISO/IEC 15504-5 ya implantados en E2. De estos ocho, cinco procesos pudieron ser utilizados para desplegar sobre ellos un total de 25 controles de seguridad de la norma ISO/IEC 27002. Los tres procesos ENG.5 Diseño de software, MAN.3 Gestión de proyectos y SUP.4 Revisión conjunta, al no tener ninguna relación con ningún control de seguridad, no pudieron utilizarse para facilitar la implantación de la norma ISO/IEC 27002.

Procesos de la norma ISO/IEC 15504-5 implantados	**Controles de seguridad de la norma ISO/IEC 27002 desplegados sobre el proceso de la norma ISO/IEC 15504-5**
ENG.1 Captura de requisitos	10.9.1 Comercio electrónico 10.9.2 Transacciones en línea 10.9.3 Información puesta a disposición pública 12.1.1 Análisis y especificación de los requisitos de seguridad 12.5.4 Fugas de información 15.1.1 Identificación de la legislación aplicable 15.1.2 Derechos de propiedad intelectual (DPI) 15.1.4 Protección de datos y privacidad de la información personal 15.1.6 Regulación de los controles criptográficos
ENG.4 Análisis de requisitos del software	12.1.1 Análisis y especificación de los requisitos de seguridad 12.2.1 Validación de los datos de entrada 12.2.2 Control del procesamiento interno 12.2.3 Integridad de los mensajes 12.2.4 Validación de los datos de salida 12.4.2 Protección de los datos de prueba del sistema 15.1.1 Identificación de la legislación aplicable
ENG.8 Pruebas del software	10.1.4 Separación de los recursos de desarrollo, prueba y operación
SUP.8 Gestión de la configuración	10.5.1 Copias de seguridad de la información 10.7.3 Procedimientos de manipulación de la información 12.4.3 Control de acceso al código fuente de los programas 12.5.1 Procedimientos de control de cambios 15.1.3 Protección de los documentos de la organización
SUP.9 Gestión de la resolución de problemas	13.1.1 Notificación de los eventos de seguridad de la información 13.1.2 Notificación de los puntos débiles de la seguridad 13.2.1 Responsabilidades y procedimientos 13.2.2 Aprendizaje de los incidentes de seguridad de la información 13.2.3 Recopilación de evidencias

Tabla 6.7. Controles de seguridad de la norma ISO/IEC 270002 desplegados sobre los procesos de la norma ISO/IEC 15504-5 implantados en E2

Capítulo 7. Conclusiones y trabajo futuro

En este último capítulo se presentan las principales conclusiones derivadas de la realización del trabajo de investigación presentado en esta memoria. Se proponen algunas líneas de investigación futuras y se presentan las publicaciones relacionadas con esta tesis doctoral.

7.1. Conclusiones

En esta tesis doctoral se ha ofrecido una visión de la situación actual de los estándares de gestión de TI para identificar sus elementos comunes y crear un nuevo modelo integrado que facilite la implantación de estos estándares reduciendo esfuerzos y duplicidades. El nuevo Modelo Integrado de Estándares de Gestión de TI desarrollado está compuesto por:

- Un modelo de referencia de procesos y mejores prácticas que toma como base los procesos del ciclo de vida del software definidos por la norma ISO/IEC 15504-5 y los amplía con los procesos de las normas ISO/IEC 20000-4 e ISO/IEC 27002.
- Un sistema de gestión integrado, a partir de los requisitos de los sistemas de gestión propuestos por las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001.

Para desarrollar este nuevo modelo integrado, se han llevado a cabo diversas actividades de investigación, que se citan a continuación:

- Se ha realizado un estudio sobre el estado actual de los estándares y normas de calidad más demandadas por las empresas del sector del desarrollo de software. Se ha podido constatar como la necesidad de conocer el nivel de capacidad de todos los procesos que se realizan en este tipo de organizaciones ya fue percibida por los organismos que desarrollan los modelos de calidad de procesos de software (CMMI e ISO/IEC 15504), quienes propiciaron e impulsaron la ampliación de sus modelos de referencia de procesos y/o su alineación con otros procesos de dominios de interés diferentes, como pueden ser la gestión de servicios de TI o la gestión de seguridad de la información.
- Se han identificado todas las iniciativas existentes de programas de mejora de procesos de gestión de servicios de TI (principalmente de las normas ITIL o ISO/IEC 20000) basadas en el modelo de capacidad de la norma ISO/IEC 15504. Al haberse detectado algunos modelos de mejora de procesos de gestión de servicios de TI basados en esta norma, ha quedado probada la posibilidad de utilizar el marco de medición de la norma ISO/IEC 15504 para la evaluación y mejora de los procesos de gestión de servicios de TI.
- Se han analizado las relaciones, totales o parciales, entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y las mejores prácticas de los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5. A partir de estas relaciones se ha elaborado un *Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5*. Este mapa puede ser utilizado

para facilitar la implantación de los procesos de gestión de servicios de TI en empresas de desarrollo de software involucradas en un programa de mejora de procesos según la norma ISO/IEC 15504, y también para maximizar la eficiencia de la implantación simultánea de ambos estándares reduciendo la cantidad de esfuerzo en una organización que vaya a comenzar la implantación de sus procesos por vez primera.

- Se han analizado las relaciones, totales o parciales, entre los controles de seguridad de la norma ISO/IEC 27002 y las prácticas básicas de los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5. Se ha podido comprobar que la norma ISO/IEC 15504 considera un gran número de los controles de seguridad necesarios para implantar un sistema de gestión de seguridad de la información. Es por ello que se puede concluir que las empresas de desarrollo de software involucradas en un programa de mejora de procesos según la norma ISO/IEC 15504 ya han realizado algunos pasos importantes que facilitan, en gran medida, la implantación de la norma ISO/IEC 27001. Además, se ha desarrollado la *ISO/IEC 15504-5 Security Extension*, que ofrece a estas empresas directrices para facilitar el despliegue de los controles de seguridad sobre los procesos de la norma ISO/IEC 15504-5.
- Se han analizado todas las relaciones existentes entre los requisitos de los sistemas de gestión de las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001, con el objetivo final de desarrollar un sistema de gestión único, integrando los requisitos de estas tres normas. A partir de las relaciones entre los diferentes sistemas de gestión, se han desarrollado dos guías para la implantación de sistemas de gestión integrados: la *Guía para la integración del Sistema de Gestión de Servicios de TI de la norma ISO/IEC 20000-1 con el Sistema de Gestión de la Calidad de la norma ISO 9001* y la *Guía para la integración del Sistema de Gestión de Seguridad de la Información de la norma ISO/IEC 27001 con el Sistema de Gestión de la Calidad de la norma ISO 9001*. Se puede concluir que, debido al gran número de elementos comunes entre los tres sistemas de gestión, el esfuerzo necesario para implantar el sistema de gestión integrado propuesto, sería mucho menor que el esfuerzo que supondría implantar las tres normas de manera independiente.

Una vez desarrollado el Modelo Integrado de Estándares de Gestión de TI, éste se ha validado mediante su aplicación real en dos empresas de desarrollo de software de nuestro entorno. En base a los resultados obtenidos durante la aplicación del modelo se ha podido constatar que:

- tener determinados procesos de la norma ISO/IEC 15004-5 a un cierto nivel de capacidad facilita la implantación de las normas ISO/IEC 20000-1 e ISO/IEC 27001.
- implantar los procesos de la norma ISO/IEC 15504-5, que ya integran las buenas prácticas y requisitos propios de las normas ISO/IEC 20000-1 o ISO/IEC 27001, permite reducir gran cantidad de esfuerzos, recursos humanos y recursos materiales y, por consiguiente, un importante ahorre de costes.

Finalmente, y con el objetivo de facilitar a los empleados de estas empresas la consolidación de conocimientos sobre los estándares integrados en el nuevo modelo, se ha desarrollado el juego de preguntas y respuestas MiProJOC.

7.2. Trabajo futuro

A continuación se exponen las líneas de investigación futuras que podrían dar continuidad a las ya presentadas en esta tesis doctoral y que van encaminadas a la mejora del Modelo Integrado de Estándares de Gestión de TI desarrollado.

1. En primer lugar, se observa que sería conveniente analizar las relaciones entre las dos normas ISO/IEC 20000-4 e ISO/IEC 27002 y las prácticas genéricas de los niveles de capacidad 2 a 5 propuestos por la norma ISO/IEC 15504, para determinar si tener un nivel de capacidad determinado en un conjunto de procesos de la norma ISO/IEC 15504, podría ayudar a la empresa a desplegar un programa de certificación según ISO/IEC 20001 o ISO/IEC 27001. Hasta el momento, se ha estudiado la relación con las mejores prácticas que la norma ISO/IEC 15504-5 propone para la obtención del nivel de capacidad 1.
2. En segundo lugar, se podría ampliar el enfoque del sistema de gestión integrado desarrollado con el modelo propuesto por la reciente norma ISO 9004, que promueve la mejora sistemática y continua del desempeño global de la organización, mediante la revisión de su sistema de gestión de la calidad utilizando una autoevaluación según un modelo de madurez por niveles.
3. Finalmente, se espera aplicar el modelo desarrollado en este trabajo en nuevas empresas de desarrollo de software con el objetivo de detectar posibles puntos débiles y de mejorarlo, si cabe, a partir de las lecciones aprendidas.

7.3. Publicaciones relacionadas con la investigación

La tabla 7.1 muestra las categorías de las publicaciones relacionadas con la investigación presentada en esta memoria. Las tablas siguientes (7.2 – 7.11) muestran, para cada publicación: el título, el lugar de publicación, la fecha de publicación, el resumen, las palabras clave y la relación con la investigación.

Categorías	Publicaciones en cada categoría			
Congresos internacionales	6	ENASE 2010	ISO/IEC 15504 best practices to facilitate ISO/IEC 27000 implementation	Tabla 7.5
		EuroSPI 2010	Application of ISO/IEC 15504 in Very Small Enterprises	Tabla 7.9
		SPICE 2011	An ISO/IEC 15504 Security Extension	Tabla 7.6
		EuroSPI 2011	ISO/IEC 15504-5 Best Practices for IT Service Management	Tabla 7.4
		CISTI 2011	MiProJOC: Una herramienta Software de soporte a la Docencia y a la Evaluación de Conocimientos	Tabla 7.10
		EuroSPI 2012	The long way to maturity: a road map to success	Tabla 7.11
Revistas internacionales	1	Journal of Information and Software Technology	IT Service Management: A Systematic Review	Tabla 7.3
		Journal of Service Research (Enviado)	Integrating IT Service Management Requirements into the Organizational Management System	Tabla 7.8
Revistas nacionales	2	REICIS 2009	La madurez de los servicios de TI	Tabla 7.2
		REICIS 2010	Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001	Tabla 7.7

Tabla 7.1. Publicaciones relacionadas con la investigación

7.3.1. Publicaciones relacionadas con el capítulo 3

A continuación las tablas 7.2, 7.3 y 7.4 muestran un resumen de las publicaciones relacionadas con el capítulo 3: Estudio de las relaciones entre los estándares ISO/IEC 20000 e ISO/IEC 15504.

La Madurez de los Servicios TI	
Lugar de publicación:	Revista Española de Innovación, Calidad e Ingeniería del Software (REICIS). Volumen 5, Número 2, Septiembre 2009.
Fecha:	Septiembre de 2009.
Resumen:	El interés que la calidad del servicio ha despertado en las organizaciones proveedoras de servicios de Tecnologías de la Información ha propiciado el nacimiento de una nueva disciplina, la gestión de servicios de Tecnologías de la Información. Con el objetivo de centrar la atención, no solamente en el desarrollo de sus productos y/o servicios, sino también en la relación con sus clientes, han ido surgiendo diferentes iniciativas que se analizan este artículo. Algunas de estas iniciativas están relacionadas con la ampliación de los modelos de evaluación y mejora de los procesos de software (CMMI y SPICE), extendiendo estos modelos con nuevos procesos de gestión de servicios. Otras, están basadas en la creación de nuevas normas o estándares específicos de calidad de servicios (ITIL e ISO/IEC 20000).
Palabras clave:	Gestión de servicios TI, modelos de madurez, CMMI, ISO/IEC 15504 (SPICE), ISO/IEC 20000.
Relación con la investigación:	En esta publicación se analiza el estado actual de la disciplina de la gestión de servicios de TI. Se muestran todas las iniciativas llevadas a cabo para desarrollar marcos normativos que agruparan todos los procesos relacionados con el ciclo de vida del software y la gestión de los servicios. Como se ha visto en el apartado 2.2 Modelos de gestión de servicios de TI, estas iniciativas se han centrado en la creación y desarrollo de nuevos modelos o estándares específicos de calidad de servicios, como son ITIL e ISO/IEC 20000 o en la ampliación de los modelos de evaluación y mejora de procesos existentes, como CMMI e ISO/IEC 15504.

Tabla 7.2. "La Madurez de los Servicios TI" (Publicación en REICIS 2009)

IT Service Management: A Systematic Review	
Lugar de publicación:	Journal Information and Software Technology.
Fecha:	20 Noviembre de 2011.

IT Service Management: A Systematic Review	
Resumen:	Context: In recent years, many software companies have considered Software Process Improvement (SPI) as essential for successful software development. These companies have also shown special interest in IT Service Management (ITSM). SPI standards have evolved to incorporate ITSM best practices. Objective: This paper presents a systematic literature review of ITSM Process Improvement initiatives based on the ISO/IEC 15504 standard for process assessment and improvement. Method: A systematic literature review based on the guidelines proposed by Kitchenham and the review protocol template developed by Biolchini et al. is performed. Results: Twenty-eight relevant studies related to ITSM Process Improvement have been found. From the analysis of these studies, nine different ITSM Process Improvement initiatives have been detected. Seven of these initiatives use ISO/IEC 15504 conformant process assessment methods. Conclusion: During the last decade, in order to satisfy the on-going demand of mature software development companies for assessing and improving ITSM processes, different models which use the measurement framework of ISO/IEC 15504 have been developed. However, it is still necessary to define a method with the necessary guidelines to implement both software development processes and ITSM processes reducing the amount of effort, especially because some processes of both categories are overlapped.
Palabras clave:	Software Process Improvement (SPI), ISO/IEC 15504 (SPICE), IT Service Management (ITSM), Systematic review.
Relación con la investigación:	En esta publicación se presenta la revisión sistemática de la literatura para detectar todas las iniciativas existentes de programas de mejora de procesos de gestión de servicios de TI basados en la norma ISO/IEC 15504 realizada para satisfacer el objetivo de esta tesis doctoral de analizar las acciones llevadas a cabo para ampliar el alcance de aplicación de la norma ISO/IEC 15504 para contemplar los aspectos propios de la gestión de servicios de TI. Esta revisión sistemática se presenta en la sección 3.1.

Tabla 7.3. "*IT Service Management: A Systematic Review*" (Publicación en Journal of Information and Software Technology)

ISO/IEC 15504-5 Best Practices for IT Service Management	
Lugar de publicación:	Systems, Software and Services Process Improvement. Communications in Computer and Information Science, Vol. 172, pp 14-24. European Systems & Software Process Improvement and Innovation (EUROSPI^2 2011). Roskilde (Dinamarca). 27-29 de Junio de 2011.
Fecha:	Junio de 2011.
Resumen:	Software companies which have been involved in a process improvement programme according to ISO/IEC 15504 are showing an increasing interest in the ISO/IEC 20000 standard for Information Technology Service Management. With the intention of supporting these companies in the implementation of the ISO/IEC 20000 standard and in order to facilitate the simultaneous application of both standards, the existing relations between ISO/IEC 15504-5 base practices and ISO/IEC 20000-4 process outcomes have been analysed and the results are presented in this paper.

ISO/IEC 15504-5 Best Practices for IT Service Management	
Palabras clave:	ISO/IEC 15504 (SPICE), ISO/IEC 20000, IT Service Management (ITSM), Software Process Improvement (SPI).
Relación con la investigación:	En esta publicación se presenta el Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5. Además, se analizan las relaciones, totales o parciales, entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y las mejores prácticas de los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5. La comparativa completa con todas las relaciones entre los resultados de los procesos de la norma ISO/IEC 20000-4 y las prácticas básicas de la norma ISO/IEC 15504-5 se presenta en en anexo B.

Tabla 7.4. "*ISO/IEC 15504-5 Best Practices for IT Service Management*" (Publicación en EuroSPI 2011)

7.3.2. Publicaciones relacionadas con el capítulo 4

A continuación las tablas 7.5 y 7.6 muestran un resumen de las publicaciones relacionadas con el capítulo 4: Estudio de las relaciones entre los estándares ISO/IEC 27000 e ISO/IEC 15504.

ISO/IEC 15504 best practices to facilitate ISO/IEC 27000 implementation	
Lugar de publicación:	Proceedings of the 5th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2010). Atenas (Grecia). 22-24 de Julio de 2010.
Fecha:	Julio de 2010.
Resumen:	In software development companies, as well as in any company, information must be adequately protected. Therefore, the implementation of information security standards has also become crucial in software organizations. Software companies involved in a process improvement initiative according to the ISO/IEC 15504 standard for process assessment and improvement are showing an increasing interest in the implementation of the ISO/IEC 27000 standard for information security management. With the intention of supporting these companies in the implementation of the ISO/IEC 27000 standard, our main goal is the development of a method which provides guidance on the application of both frameworks. As a first step of this work, in this article a mapping between ISO/IEC 27002 and ISO/IEC 15504-5 is presented.
Palabras clave:	ISO/IEC 15504 (SPICE), ISO/IEC 27000, Information security, SPI.
Relación con la investigación:	En esta publicación se presenta una comparativa que muestra todas las relaciones entre los controles de seguridad de la información propuestos en la norma ISO/IEC 27002 y las prácticas básicas de la norma ISO/IEC 15504-5. Se demuestra que la norma ISO/IEC 15504 considera muchos de los aspectos y controles de seguridad necesarios para la implantación del sistema de gestión de seguridad de la información que propone la norma ISO/IEC 27001. La comparativa completa se presenta en en anexo C.

Tabla 7.5. "*ISO/IEC 15504 best practices to facilitate ISO/IEC 27000 implementation*" (Publicación en ENASE 2010)

An ISO/IEC 15504 Security Extension	
Lugar de publicación:	Software Process Improvement and Capability Determination. Communications in Computer and Information Science, 2011, Vol. 155, Part 2, pp 64-72 Software Process Improvement and Capability Determination (SPICE 2011). Dublin (Irlanda). 10 de Mayo - 1 de Junio de 2011.
Fecha:	Mayo de 2011.
Resumen:	Software companies which have been involved in a process improvement programme according to ISO/IEC 15504 have already performed some steps in order to implement ISO/IEC 27000 as an information security management framework. After analysing in depth the existing relations between ISO/IEC 15504-5 base practices and ISO/IEC 27002 security controls, in this paper the security controls covered by the ISO/IEC 15504-5 processes are described, the changes over these processes which would be necessary for the implementation of the controls are detailed and an ISO/IEC 15504 Security Extension that facilitates the implementation of both standards is presented.
Palabras clave:	ISO/IEC 15504 (SPICE), ISO/IEC 27000, Information security, Software Process Improvement (SPI).
Relación con la investigación:	En esta publicación se describe la *ISO/IEC 15504 Security Extension* desarrollada a partir de las relaciones detectadas entre las prácticas básicas de la norma ISO/IEC 15504-4 y los controles de seguridad de la norma ISO/IEC 27002. Esta extensión de seguridad ofrece, para cada uno de los procesos de la norma ISO/IEC 15504-5, directrices e indicaciones para facilitar a las organizaciones la implantación de los controles de controles de seguridad relacionados. La *ISO/IEC 15504 Security Extension* se ha presentado en la sección 4.4 de esta tesis doctoral.

Tabla 7.6. "*An ISO/IEC 15504 Security Extension*" (Publicación en SPICE 2011)

7.3.3. Publicaciones relacionadas con el capítulo 5

Las tablas 7.7 y 7.8 muestran un resumen de las publicaciones relacionadas con el capítulo 5: Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001.

Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000e ISO/IEC 27001	
Lugar de publicación:	Revista Española de Innovación, Calidad e Ingeniería del Software (REICIS). Volumen 6, Número 3, Noviembre 2010.
Fecha:	Noviembre 2010

Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000e ISO/IEC 27001	
Resumen:	Dada la gran aceptación que tuvo en su momento la implantación de un Sistema de Gestión de Calidad (SGC) de acuerdo con la norma ISO 9001, actualmente la mayoría de organizaciones que deciden implantar una nueva norma para gestionar sus servicios, como ISO/IEC 20000, o la seguridad de su información, como ISO/IEC 27001, normalmente ya cuentan con un SGC basado en ISO 9001. Con el objetivo de facilitar a las empresas la implantación de estas normas se ha realizado un estudio, tanto para analizar las posibles relaciones existentes entre los requisitos de los sistemas de gestión propuestos por estas normas, como para identificar los requisitos no compartidos entre ellos. En este artículo se presenta un nuevo Sistema de Gestión Integrado que amplía los requisitos de un SGC según ISO 9001 con los requisitos específicos de los otros dos estándares antes mencionados.
Palabras clave:	Sistema de Gestión Integrado, Sistema de Gestión de Calidad (SGC), ISO 9001, ISO/IEC 20000, ISO/IEC 27001, ISO/IEC 9004.
Relación con la investigación:	En esta publicación se presenta el Sistema de Gestión Integrado que se describe en la sección 5.5. Este nuevo Sistema de Gestión Integrado, basado en el sistema de gestión de calidad de la norma ISO 9001, facilita la implantación del sistema de gestión de servicios de TI de la norma ISO/IEC 20000 y del sistema de gestión de seguridad de la información de la norma ISO/IEC 27001.

Tabla 7.7. "Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001" (Publicación en REICIS 2010)

Integrating IT Service Management Requirements into the Organizational Management System	
Lugar de publicación:	Journal of Service Research
Fecha:	Enviado el 30 de Marzo de 2012
Resumen:	As a consequence of the implementation of a Quality Management System (QMS) according to ISO 9001 performed during the last decade by an important number of IT service provider organizations, these companies can take advantage of all the efforts previously made when implementing an IT Service Management System (ITSMS) according to the ISO/IEC 20000-1 standard. In order to facilitate the integration of these two management systems, a study has been carried out to analyse the existing relations between the requirements of the ISO 9001 QMS and ISO/IEC 20000-1 ITSMS. This paper provides a new Integrated Management System (IMS) which widens the scope of the ISO 9001 QMS with the IT service management specific requirements of the ISO/IEC 20000-1 standard and presents a guide to support organizations in implementing this quality and IT service management IMS.
Palabras clave:	Integrated Management System (IMS), Quality Management System (QMS), IT Service Management System (ITSMS), ISO 9001, ISO/IEC 20000.
Relación con la investigación:	En esta publicación se presenta la parte del Sistema de Gestión Integrado que integra los requisitos del sistema de gestión de calidad de la norma ISO 9001 y del sistema de gestión de servicios de TI de la norma ISO/IEC 20000-1. Esta parte del Sistema de Gestión Integrado se describe en la sección 5.5.

Tabla 7.8. "Integrating IT Service Management Requirements into the Organizational Management System" (Enviado al Journal of Service Research)

7.3.4. Publicaciones relacionadas con el capítulo 6

A continuación las tablas 7.9, 7.10 y 7.11 muestran un resumen de las publicaciones relacionadas con el capítulo 6: Aplicación del Modelo Integrado de Estándares de Gestión de TI.

Application of ISO/IEC 15504 in Very Small Enterprises	
Lugar de publicación:	Systems, Software and Services Process Improvement. Communications in Computer and Information Science, Vol. 99. European Systems & Software Process Improvement and Innovation (EUROSPI^2 2010). Grenoble (Francia). 1-3 de Septiembre de 2010.
Fecha:	Septiembre de 2010.
Resumen:	This paper presents the experience of application of the ISO/IEC 15504 standard in eight software companies. Firstly, the objectives, the participants and the work plan are exposed. Secondly, the implementation of the project activities and its results are summarized. And finally, the cost of the implementation is detailed. The project which has allowed this improvement effort in these organizations has been named "QuaSAR II" and represents the continuance of the "QuaSAR" project, a software process improvement initiative started in 2002 in the Balearic Islands.
Relación con la investigación:	Última publicación acerca del proyecto QuaSAR (*Qualitat de Software BaleAR*). En ella se resume el proyecto como experiencia de aplicación de un programa de mejora del proceso software en 8 pequeñas y medianas empresas de las Illes Balears. El proyecto QuaSAR supuso una primera experiencia de evaluación de los procesos de desarrollo de software en empresas del sector. Una vez elaborado el nuevo Modelo Integrado de Estándares de Gestión de TI, se espera validarlo en una nueva edición del proyecto QuaSAR, durante el año 2012.

Tabla 7.9. "*Application of ISO/IEC 15504 in Very Small Enterprises*" (Publicación en EuroSPI 2010)

MiProJOC: Una herramienta Software de soporte a la Docencia y a la Evaluación de Conocimientos	
Lugar de publicación:	Actas de la 6º Conferencia Ibérica de Sistemas y Tecnologías de la Información (CISTI 2011). Chaves (Portugal). 15-18 de Junio de 2011.
Fecha:	Junio de 2011.
Resumen:	La combinación de métodos tradicionales de enseñanza con mecanismos de innovación docente genera un efecto positivo en el aprendizaje de cualquier materia. Como complemento de las clases teóricas y prácticas en los estudios de educación superior, se ha desarrollado una herramienta en forma de juego denominada MiProJOC. La herramienta también puede ser utilizada para la evaluación de conocimientos en actividades de estudio y trabajo autónomo del alumno. MiProJOC está diseñada para facilitar el mantenimiento de un repositorio de preguntas de diferentes áreas, definir distintas modalidades de juego y presentar los resultados estadísticos derivados de la utilización del juego.

MiProJOC: Una herramienta Software de soporte a la Docencia y a la Evaluación de Conocimientos	
Palabras clave:	Educación, aprendizaje, juego, evaluación de conocimientos, herramienta de software
Relación con la investigación:	Esta publicación presenta la herramienta en forma de juego de preguntas y respuestas MiProJOC, que ha sido diseñada para ofrecer a sus usuarios un soporte automatizado para la consolidación y evaluación de conocimientos sobre diferentes campos o áreas de conocimiento, como pueden ser la mejora de procesos de software, la gestión de servicios de TI o la gestión de la seguridad de la información. La herramienta MiProJOC se describe en el anexo D.

Tabla 7.10. "MiProJOC: Una herramienta Software de soporte a la Docencia y a la Evaluación de Conocimientos" (Publicación en CISTI 2011)

The long way to maturity: a road map to success	
Lugar de publicación:	EuroSPI technical proceedings. European Systems & Software Process Improvement and Innovation (EUROSPI^2 2012). Viena (Austria). 25-27 de Junio de 2012.
Fecha:	Junio de 2012.
Resumen:	This paper describes the experience of E1, a Spanish software company which, in order to achieve its business objectives and meet the needs and expectations of its customers, strongly bet on quality as the way to progress towards maturity. We present the continuous evolution suffered by both the management and the production processes through the implementation of quality standards. The knowledge reuse strategy deployed by the company has enabled an important effort reduction when implementing a new standard by taking advantage of the knowledge gained in previous improvement efforts. The most significant results and lessons learned during the improvement path are presented.
Palabras clave:	Software Process Improvement, ISO 9001, EFQM Excellence Model, ISO 14001, ISO/IEC 15504 (SPICE), ISO/IEC 27001
Relación con la investigación:	En esta publicación se muestran las lecciones aprendidas por una empresa de desarrollo de software en la que se ha aplicado el nuevo Modelo Integrado de Estándares de Gestión de TI durante su camino hacia la excelencia en su apuesta continua por la calidad.

Tabla 7.11. "*The long way to maturity: a road map to success*" (Publicación en EuroSPI 2012)

Capítulo 8. Referencias bibliográficas

Bibliografía referenciada

(Aboulnaga 1998) ABOULNAGA, I.A. Integrating quality and environmental management as competitive business strategy for 21st century, *Environmental Management and Health*, Vol. 9, 2, 65-71, 1998.

(Amengual and Mas 2003) AMENGUAL, E. and MAS, A. A New Method of ISO/IEC TR 15504 and ISO 9001:2000 Simultaneous Application on Software SMEs. *Proceedings of the Joint ESA – 3rd International SPICE Conference on Process Assessment and Improvement (SPICE),* Marzo 2003, pp. 87-92.

(Amengual and Mas 2007) AMENGUAL, E. and MAS, A. Software Process Improvement in Small Companies: An Experience. *Proceedings of the European Software Process Improvement Conference (EuroSPI),* Septiembre 2007.

(Abrahamsson et al. 2010) ABRAHAMSSON, S.; ISAKSSON, R. and HANSSON, J. Integrated Management Systems: advantages, problems and possibilities. *Proceedings of the 13th Toulon-Verona Conference: Organizational Excellence in Service 2010*, 2-4 September 2010, Coimbra, Portugal.

(Asif et al. 2008) ASIF, M.; DE BRUIJIN, E.J. and FISSCHER, O. Corporate motivation for integrated management system implementation. Why do firms engage in integration of management systems: a literature review & research agenda. *16th Annual High Technology Small Firms Conference*, HTSF 2008, 21-23 May 2008, Enschede, The Netherlands, 2008.

(Asif et al. 2010) ASIF, M.; FISSCHER, O; DE BRUIJIN, E.J. and PAGELL M. Integration of management systems: A methodology for operational excellence and strategic flexibility, *Operations Management Research*, vol 3, 3-4, 146-160, 2010.

(AENOR 2005) ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR). UNE 66177 Sistemas de gestión - Guía para la integración de los sistemas de gestión, 2005.

(Barafort and Rousseau 2009) BARAFORT, B. and ROUSSEAU, A. Sustainable Service Innovation Model: A Standardized IT Service Management Process Assessment Framework, Software Process Improvement: EuroSPI 2009. *Communications in Computer and Information Science*, vol. 42, pp. 69–80, Springer-Verlag, Heidelberg, 2009.

(Barafort et al. 2002) BARAFORT, B.; DI RENZO, B. and MERLAN, O. Benefits resulting from the combined use of ISO/IEC 15504 with the Information Technology Infrastructure Library (ITIL), International Conference on Product Focused Software Process Improvement (PROFES 2002). *Lecture Notes in Computer Science*, vol. 2559, pp. 314–325, Springer-Verlag, 2002.

(Barafort et al. 2005) BARAFORT, B.; DI RENZO, B.; LEJEUNE, V.; PRIME, S. and SIMON, J.-M. ITIL Based Service Management measurement and ISO/IEC 15504 process assessment: a win–win opportunity, *Proceedings of the 5th International SPICE Conference on Process Assessment and Improvement (SPICE 2005)*, Klagenfurt, Austria, 2005.

(Barafort et al. 2006) BARAFORT, B.; HUMBET, J-P. and POGGI, S. Information Security Management and ISO/IEC 15504: the link opportunity between Security and Quality. *International SPICE Conference on Process Assessment and Improvement*. Luxembourg, 2006.

(Barafort et al. 2008a) BARAFORT, B.; JEZEK, D.; MÄKINEN, T.; STOLFA, S.; VARKOI, T. and VONDRAK. Modeling and Assessment in IT Service Process Improvement, Software Process Improvement: EuroSPI 2008. *Communications in Computer and Information Science*, vol. 16, pp. 117–128, Springer-Verlag, 2008.

(Barafort et al. 2008b) BARAFORT, B.; RENAULT, A.; PICARD, M. and CORTINA, S. A transformation process for building PRMs and PAMs based on a collection of requirements - Example with ISO/IEC 20000, *Proceedings of the International SPICE Conference on Process Improvement and Capability dEtermination (SPICE 2008)*, Nuremberg, Germany, 2008.

(Bernardo et al. 2009) BERNARDO, M.; CASADESUS, M.; KARAPETROVIC S. and HERAS, I. How Integrated are Environmental, Quality and Other Standardized Management Systems: An Empirical Study, *Journal of Cleaner Production*, vol. 17, 8, 742-750, 2009.

(Biolchini et al. 2005) BIOLCHINI, J.; GOMES, P.; CRUZ, A. C. and HORTA G. Systematic Review in Software Engineering, Systems Engineering and Computer Science Department, COPPE/UFRJ, *Technical Report RT-ES679/05*, Rio de Janeiro, Brazil, May 2005.

(BSI 2006) BRITISH STANDARDS INSTITUTION (BSI). PAS 99:2006 Specification of common management system requirements as a framework for integration, 2006.

(Cass et al. 2002) CASS, A.; VÖLCKER, C.; SUTTER, P.; DORLING, A. and STIENEN, H. SPiCE in Action - Experiences in Tailoring and Extension, *Proceedings of the 28th Euromicro Conference (EUROMICRO 2002)*, Dortmund, Germany, 2002.

(Cater-Steel 2007) CATER-STEEL A. Integration of service management with CMMI and SPICE, *5th Annual SEPG Australia Conference*, Gold Coast, Australia, August 2007.

(Cater-Steel 2009) CATER-STEEL A. IT Service Departments Struggle to Adopt a Service-Oriented Philosophy, *International Journal of Information Systems in the Service Sector*, vol. 1, issue 2, pp. 69–77, 2009.

(Cruzes et al. 2007) CRUZES, D.; MENDONÇA, M.; BASILI, V.; SHULL, F. and JINO, M. Extracting Information from Experimental Software Engineering Papers, *Proceedings of the XXVI International Conference of the Chilean Society of Computer Science (SCCC 2007)*, pp. 105-114, 2007.

(Di Renzo and Feltus 2003) DI RENZO, B. and FELTUS, C. Process assessment for use in very small enterprise: the NOEMI assessment methodology, *Proceedings of the European Software Process Improvement Conference (EuroSPI 2003)*, Graz, Austria, December 2003.

(Di Renzo et al. 2004) DI RENZO, B.; FELTUS, C. and PRIME, S. Collaborative management for ICT process improvement in SME: experience report, *Proceedings of the European Software Process Improvement Conference (EuroSPI 2004)*, Trondheim, Norway, November 2004.

(Djapic and Lukic 2008) DJAPIC, M. and LUKIC, L. Integrated management systems - Requirement of contemporary business practices, *Mechanics Transport Communications*, issue 3, 2008.

(Fresner and Engelhardt 2004) FRESNER, J. and ENGELHARDT G. Experiences with integrated management systems for two small companies in Austria, *Journal of Cleaner Production*, vol. 12, 623-631, 2004.

(Goldschmidt et al. 2009) GOLDSCHMIDT, T.; DITTRICH, A. and MALEK, M. Quantifying Criticality of Dependability-Related IT Organization Processes in CobiT, *IEEE Proceedings of 15th Pacific Rim International Symposium on Dependable Computing (PRDC 2009)*, Shanghai, China, 2009.

(Grandry et al. 2008) GRANDRY, E.; DUBOIS, E.; PICARD, M. and RIFAUT, A. Managing the Alignment between Business and Software Services Requirements from a Capability Model Perspective, Towards a Service-Based Internet (ServiceWave 2008), *Lecture Notes In Computer Science*, vol. 5377, pp. 171–182, 2008.

(Griffith and Bhutto 2008) GRIFFITH, A. and BHUTTO K. Improving environmental performance through integrated management systems (IMS) in the UK, *Management of Environmental Quality: An International Journal*, vol 19, 5, 565-578, 2008.

(Hilbert and Renault 2007) HILBERT, R. and RENAULT A. Assessing IT Service Management Processes with AIDA - Experience Feedback, *Proceedings of the European Systems & Software Process Improvement and Innovation Conference (EuroSPI 2007)*, Potsdam, Germany, September 2007.

(Irving 2008) IRVING, D. TickIT Plus - the Future of TickIT!, *TickIT International*, issue 2Q08, pp. 3–7, 2008.

(ISO9001 2008) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO 9001:2008. Quality management systems – Requirements, 2008.

(ISO90003 2004) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 90003:2004. Software engineering – Guidelines for the application of ISO 9001:2000 to computer software, 2004.

(ISO90005 2008) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC TR 90005:2008. Systems engineering – Guidelines for the application of ISO 9001 to system life cycle processes, 2008.

(ISO12207 2002) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 12207:1995/Amd 1:2002 Information technology – Software life cycle processes, 2002.

(ISO12207 2004) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 12207:1995/Amd 2:2004 Information technology – Software life cycle processes, 2004.

(ISO12207 2008) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 12207:2008 Systems and software engineering – Software life cycle processes, 2008.

(ISO15504 2004a) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 15504-1:2004. Information Technology – Process Assessment – Part 1: Concepts and Vocabulary, 2004.

(ISO15504 2003) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 15504-2: 2003. Information Technology – Process assessment – Part 2: Performing an assessment, 2003.

(ISO15504 2004b) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 15504-3:2004. Information Technology – Process Assessment – Part 3: Guidance on performing an assessment, 2004.

(ISO15504 2004c) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 15504-4:2004. Information Technology – Process Assessment – Part 4: Guidance on use for process improvement and process capability determination, 2004.

(ISO15504 2006) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 15504-5: 2006. Information Technology – Process Assessment – Part 5: An exemplar Process Assessment Model, 2006.

(ISO15504 2012) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 15504-5:2012 Information technology – Process assessment – Part 5: An exemplar software life cycle process assessment model, 2012.

(ISO15504 2008a) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC TR 15504-6: 2008. Information Technology – Process Assessment – Part 6: An exemplar system life cycle process assessment model, 2008.

(ISO15504 2008b) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC TR 15504-7: 2008. Information Technology – Process Assessment – Part 7: Assessment of organizational maturity, 2008.

(ISO15504 2011a) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC TS 15504-9:2011 Information technology – Process assessment – Part 9: Target process profiles, 2011.

(ISO15504 2011b) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC TS 15504-10:2011 Information technology – Process assessment – Part 10: Safety extension, 2011.

(ISO20000 2011) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 20000-1:2011 Information technology – Service management – Part 1: Service management system requirements, 2011.

(ISO20000 2012) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 20000-2:2012. Information Technology – Service Management – Part 2: Guidance on the application of service management systems, 2012

(ISO20000 2009) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC TR 20000-3:2009. Information technology – Service Management – Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1, 2009.

(ISO20000 2010a) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC TR 20000-4:2010. Information technology – Service Management – Part 4: Process reference model, 2010.

(ISO20000 2010b) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC TR 20000-5:2010 Information technology – Service management – Part 5: Exemplar implementation plan for ISO/IEC 20000-1, 2010.

(ISO27000 2005a) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements, 2005.

(ISO27000 2005b) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management, 2005.

(ISO 2008) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. The integrated use of management system standards, 2008.

(ISOG72 2001) INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO Guide 72:2001 Guidelines for the justification and development of management system standards, 2001.

(Karapetrovic and Willborn 1998) KARAPETROVIC S. and WILLBORN W. Integration of quality and environmental management systems, *TQM Magazine*, vol. 10, 3, 204-213, 1998.

(Karapetrovic 2002) KARAPETROVIC S. Strategies for the integration of management systems and standards, *The TQM Magazine*, vol. 14, 1, 61-67, 2002.

(Karapetrovic and Jonker 2003) KARAPETROVIC, S. and JONKER, J. Integration of Standardized Management Systems: Searching for a Recipe and Ingredients, *Total Quality Management and Business Excellence*, vol 14, 4, 451-459, 2003.

(Karapetrovic and Casadesús 2009) KARAPETROVIC S. and CASADESUS, M. Implementing Environmental with Other Standardized Management Systems: Scope, Sequence, Time and Integration, *Journal of Cleaner Production*, vol 17, 5, 533-540, 2009.

(Kitchenham et al. 2002) KITCHENHAM, B.A.; PFLEEGER, S. L.; PICKARD, L. M.; JONES, P. W.; HOAGLIN, D. C.; EL EMAM, K. and ROSENBERG, J. Preliminary Guidelines for Empirical Research in Software Engineering, *IEEE Transactions on Software Engineering*, vol. 28, no. 8, pp 721-734, August 2002.

(Kitchenham 2007) KITCHENHAM, B. Guidelines for Performing Systematic Literature Reviews in Software Engineering Version 2.3, *Technical Report EBSE-2007-01*, Software Engineering Group, School of Computer Science and Mathematics, Keele University, and Department of Computer Science, University of Durham, July 2007.

(Kramer 2008) KRAMER, A. ISO/IEC 15504 and ITIL, *International SPICE Days 2008*, Prague, Czech Republic, June 2008.

(Labodová 2004) LABODOVÁ, A. Implementing integrated management systems using a risk analysis based approach, *Journal of Cleaner Production*, vol 12, 571-580, 2004.

(Majstorovic and Marinkovic 2011) MAJSTOROVIC, V.D. and MARINKOVIC, V. The Development of Business Standardization and Integrated Management Systems, *Journal of Medical Biochemistry* 30, 334-345, 2011.

(Malzhan 2007) MALZAHN, D. A service extension for SPICE?, *Proceedings of the International SPICE Conference on Process Assessment and Improvement (SPICE 2007)*, Seoul, South Korea, May 2007.

(Malzhan 2009) MALZAHN, D. Assessing - learning - improving, an integrated approach for self assessment and process improvement systems, *Proceedings of the fourth International Conference on Systems (ICONS 2009)*, pp. 126–130, Cancun, Mexico, March 2009.

(Mas and Amengual 2003) MAS, A and AMENGUAL, E. ISO/IEC 15504 Adaptation for Software Process Assessment in SMEs. *Proceedings of the International Conference on Software Engineering Research and Practice*, Junio 2003, pp. 693-697.

(Mas and Amengual 2004) MAS, A. and AMENGUAL, E. A Method for the Implementation of a Quality Management System in Software SMEs. *Software Quality Management XII. New Approaches to Software Quality*, The British Computer Society, 2004, pp.61-74.

(Mas and Amengual 2005) MAS, A. and AMENGUAL, E. La mejora de procesos de software en las pequeñas y medianas empresas. Un nuevo modelo y su aplicación a un caso real. *REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software*, vol. 1, nº 2, Diciembre 2005, pp.7-30.

(Mas et al. 2009) MAS, A.; FLUXÀ, B. and AMENGUAL, E. Lessons learned from an ISO/IEC 15504 SPI programme in a company. *Proceedings of the EuroSPI 2009*. Alcalá de Henares, Spain, September 2009.

(Nehfort 2007) NEHFORT, A. SPICE Assessments for IT Service Management according to ISO/IEC 20000–1, *International SPICE Days 2007*, Frankfurt, Germany, June 2007.

(Nevalainen and Johansson 2008) NEVALAINEN R. and JOHANSSON, M. Comparison of CMMI-SVC and ISO20000 – A Case Study, *Proceedings of the European Systems & Software Process Improvement and Innovation Conference (EuroSPI 2008)*, Dublin, Ireland, September 2008.

(Niessink and Van Vliet 1998) NIESSINK, F and VAN VLIET, H. Towards Mature IT Services, *Software Process - Improvement and Practice*, vol. 4, issue 2, pp. 55–71, June 1998.

(Novák 2005) NOVÁK, L. Integrated Information Management Systems, *Proceedings of the Security and Protection of Information Conference 2005*, 3-5 May 2005, Brno, Czech Republic, 2005.

(OGC 2007a) OFFICE OF GOVERNMENT COMMERCE. ITIL V3 Service Strategy, 2007.

(OGC 2007b) OFFICE OF GOVERNMENT COMMERCE. ITIL V3 Service Design, 2007.

(OGC 2007c) OFFICE OF GOVERNMENT COMMERCE. ITIL V3 Service Transition, 2007.

(OGC 2007d) OFFICE OF GOVERNMENT COMMERCE. ITIL V3 Service Operation, 2007.

(OGC 2007e) OFFICE OF GOVERNMENT COMMERCE. ITIL V3 Continual Service Improvement, 2007.

(Picard et al. 2010) PICARD, M.; RENAULT, A. and CORTINA, S. How to Improve Process Models for Better ISO/IEC 15504 Process Assessment, *Systems, Software and Services Process Improvement (EuroSPI 2010)*, CCIS 99, pp. 130–141, 2010.

(Pojasek 2006) POJASEK, R.B. Is your integrated management system really integrated?, *Environmental Quality Management*, vol. 16, 2, 89-97, 2006.

(Henry Tudor 2009) PUBLIC RESEARCH CENTRE HENRI TUDOR: Barafort, B.; Betry, V.; Cortina, S.; Picard, M.; St-Jean, M.; Renault, A. and Valdés, O. ITSM Process Assessment Supporting ITIL, Van Haren Publishing, Zaltbommel, December 2009.

(Rajkovic and Aleksic 2009) RAJKOVIC, D. and ALEKSIC M. Corporative Motives on Implementation of Integrated Management System (IMS), *International Journal for Quality research*, vol.3, 3, 2009.

(Renault and Barafort 2011) RENAULT, A and BARAFORT, B. TIPA: 7 years experience with SPICE for IT Service Management, *Proceedings of the European System & Software Process Improvement and Innovation Conference (EuroSPI 2011)*, Roskilde, Denmark, June 2011.

(Rifaut 2005) RIFAUT, A. Goal-Driven Requirements Engineering for Supporting the ISO 15504 Assessment Process, Software Process Improvement: EuroSPI 2005. *Lecture Notes in Computer Science*, vol. 3792, pp. 151–162, Springer-Verlag, 2005.

(Salomone 2008) SALOMONE, R. Integrated management systems: experiences in Italian organizations, *Journal of Cleaner Production*, vol 16, 1786-1806, 2008.

(Scheuing et al. 2000) SCHEUING, Q.; FRÜHAUF K. and SCHWARZ, W. Maturity model for IT operations (MITO), *Proceeding of the 2nd World Congress on Software Quality*, Yokohama, Japan, September 2000.

(SEI 2010a) SOFTWARE ENGINEERING INSTITUTE. CMMI® for Development, Version 1.3. CMMI-DEV, V1.3, November 2010.

(SEI 2010b) SOFTWARE ENGINEERING INSTITUTE. CMMI® for Services, Version 1.3. CMMI-SVC, V1.3, November 2010.

(SEI 2010c) SOFTWARE ENGINEERING INSTITUTE. CMMI® for Acquisition, Version 1.3. CMMI-ACQ, V1.3, November 2010.

(SPICEUG 2009) SPICE USER GROUP. http://www.spiceusergroup.org.

(AS/NZS 1999) STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND (AS/NZS). AS/NZS 4581:1999 Management system integration - Guidance to business, government and community organizations, 1999.

(St-Jean 2009) ST-JEAN, M. TIPA to keep ITIL going and going, *Proceedings of the European Systems & Software Process Improvement and Innovation Conference (EuroSPI 2009)*, Alcalá de Henares, Spain, September 2009.

(St-Jean and Mention 2009) ST-JEAN, M. and MENTION, A.-L. How to evaluate benefits of Tudor's ITSM Process Assessment?, *Proceedings of the International SPICE Conference on Process Improvement and Capability dEtermination (SPICE 2009)*, Turku, Finland, June 2009.

(Valdevit et al. 2009) VALDEVIT, T.; MAYER, N. and BARAFORT, B. Tailoring 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings. Proceedings of the EuroSPI 2009, *Communications in Computer and Information Science* 42, pp. 201-212. Springer-Verlag Berlin Heidelberg, 2009.

(Varkoi and Makinen 2008) VARKOI, T. and MAKINEN, T. Proactive elicitation of software process improvements, *Proceedings of the Portland International Conference on Management of Engineering & Technology (PICMET 2008)*, pp. 1576–1579, Cape Town, South Africa, July 2008.

(Wang and Tsai 2009) WANG, C-H. and TSAI, D-R. Integrated installing ISO 9000 and ISO 27000 management systems on an organization, *43rd Annual 2009 International Carnahan Conference on Security Technology*, 5-8 October 2009, 265-267, 2009.

(Zeng et al. 2007) ZENG, S.X.; SHIB, J. Shib and LOU, G.X. A synergetic model for implementing an integrated management system: an empirical study in China", *Journal of Cleaner Production*, vol 15, 18, 1760-1767, 2007.

Anexos

ANEXO A. Protocolo de revisión sistemática

ANEXO B. Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5

ANEXO C. Mapa de relaciones entre los controles de seguridad de la norma ISO/IEC 27002 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5

ANEXO D. MiProJOC: el juego de mejora de procesos

ANEXO E. Guías para la implantación de sistemas de gestión integrados a partir de la norma ISO 9001

ANEXO A. Protocolo de revisión sistemática

El proceso utilizado en esta investigación para realizar revisiones sistemáticas de la literatura se basa en las directrices y guías propuestas por Kitchenham (Kitchenham et al. 2002; Kitchenham 2007) y en el protocolo de revisión desarrollado por (Biolchini et al. 2005) que describe cada una de las fases del proceso de revisión sistemática.

El protocolo utilizado para la revisión sistemática consta de cinco etapas: formulación de la pregunta, selección de las fuentes, selección de los estudios, extracción de la información y resumen de los resultados. En las siguientes secciones se abordan cada una de estas etapas.

A.1. Formulación de la pregunta

Durante la primera fase se debe definir el objetivo y el contexto de la revisión sistemática. Para determinar con precisión el contexto de aplicación de la revisión sistemática, el protocolo propone definir los siguientes elementos: Problema, Pregunta, Palabras clave y sinónimos, Intervención, Control, Efecto, Métrica de salida, Población, Aplicación, Diseño experimental.

A.2. Selección de las fuentes

Para realizar la selección de las fuentes donde se ejecutarán las búsquedas de estudios primarios, el protocolo de revisión sistemática sugiere definir los siguientes elementos: criterios de selección de fuentes, idiomas de los estudios, proceso de identificación de fuentes y cadenas de búsqueda.

Referente a los criterios de selección de fuentes, se definieron los criterios que se muestran a continuación. Las fuentes seleccionadas debían cumplir uno o más de los siguientes criterios:

- Editoriales o sitios web sugeridos por expertos.
- Publicaciones con un índice de impacto elevado.
- Disponibilidad de mecanismos de búsqueda mediante palabras clave.
- Invariabilidad en los resultados de la búsqueda usando el mismo conjunto de palabras clave.
- Disponibilidad en Internet.

Referente a los idiomas de los estudios, los estudios primarios obtenidos debían estar escritos en inglés o en español.

Las fuentes fueron identificadas según el juicio de los miembros de nuestro grupo de investigación. La lista de fuentes incluye *journals* relevantes del área de mejora de procesos de software, tales como *ACM SIGSOFT Software Engineering Notes*, *IEEE Software*, *IEEE Transactions on Software Engineering*, *Information and Software Technology*, *Journal of Service Research*, *Journal of Systems and Software*, *Software Process: Improvement and Practice* y *Software Quality Journal*, entre otros. Además, también fueron considerados los artículos publicados en las actas de diferentes congresos tales como EuroSPI, foro de discusión e intercambio de buenas prácticas para expertos en la mejora de procesos de software, y SPICE, uno de los eventos más importantes relacionados con el estándar ISO/IEC 15504.

A partir de la combinación de las palabras clave definidas en la etapa anterior, y haciendo combinaciones con los conectores lógicos "AND" y "OR", se deben obtener las cadenas de búsqueda. Para llevar a cabo las búsquedas, estas cadenas deben ser adaptadas a cada mecanismo de búsqueda de las fuentes seleccionadas.

Después de tomar en consideración todos los criterios de selección de fuentes definidos, la lista inicial de fuentes obtenida es la que se muestra en la tabla A.1.

Fuente	Sitio web
ACM Portal (Digital Library & Guide)	http://portal.acm.org/portal.cfm
CiteSeerX	http://citeseerx.ist.psu.edu
EuroSPI (Proceedings of) (desde 2004)	http://www.eurospi.net
Google Scholar	http://scholar.google.com
IEEE Computer Society Digital Library	http://www.computer.org/portal/web/csdl
IEEE Xplore	http://ieeexplore.ieee.org
IET Digital Library	http://www.ietdl.org
ISI Web of Knowledge	http://www.isiknowledge.com
SAGE Journals	http://online.sagepub.com
ScienceDirect	http://www.sciencedirect.com
SPICE (Proceedings of) (desde 2003)	http://www.spiceconference.com
Springer Link	http://www.springerlink.com
Wiley InterScience	http://www.interscience.wiley.com

Tabla A.1. Lista de fuentes utilizadas por el protocolo de revisión sistemática.

A.3. Selección de los estudios

Una vez definidas las fuentes donde se realizarán las búsquedas, es necesario describir el proceso y los criterios para la selección y evaluación de los estudios.

Los criterios mediante los cuales los estudios deben ser evaluados para decidir si son seleccionados o no en el contexto de la revisión sistemática se deben definir teniendo en cuenta las propuestas de Kitchenham (Kitchenham et al. 2002; Kitchenham 2007). Estos Criterios de Inclusión (CI) y Criterios de Exclusión (CE) se deben adaptar a cada revisión sistemática.

La figura A.1 ilustra, mediante un diagrama de flujo, el proceso llevado a cabo para obtener y evaluar los estudios primarios de acuerdo a los criterios de inclusión y exclusión definidos. Este diagrama de flujo muestra dos grupos de actividades principales. El objetivo del primer grupo es seleccionar los estudios primarios, mientras que el segundo grupo de actividades se centra en la extracción de la información de los estudios primarios seleccionados. El proceso de extracción de la información se presenta más adelante.

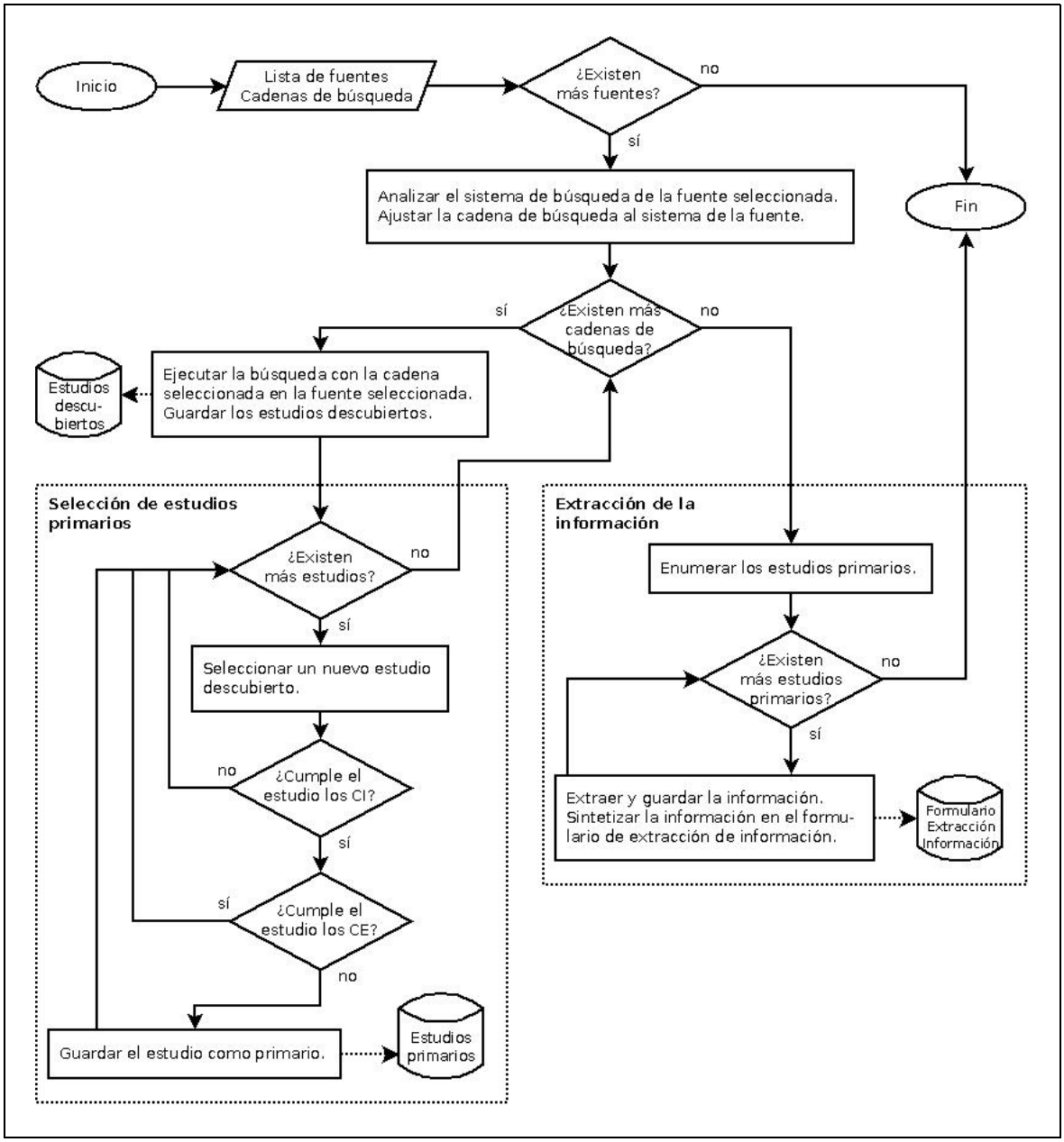

Figura A.1. Procedimiento para la ejecución de la revisión sistemática

Después de aplicar los criterios de inclusión y exclusión, se deben seleccionar los estudios primarios.

A.4. Extracción de la información

Una vez seleccionados los estudios primarios, se deben definir los Criterios de Inclusión de la información (CI_{inf}) mediante los cuales evaluar la información obtenida en los estudios primarios para decidir si debe ser tomada en consideración o descartada.

Para facilitar el análisis de los datos presentados en los estudios primarios seleccionados y para estandarizar el registro de los comentarios, las impresiones y las ideas más importantes de cada uno de estos estudios, se diseñó un formulario de extracción de datos. Este formulario, que se muestra en la tabla A.2, basa su estructura y contenidos en el formato propuesto en (Cruzes et al. 2007). Los contenidos se agrupan en dos categorías: resultados objetivos y resultados subjetivos. Los resultados objetivos se presentan en las cuatro primeras secciones del formulario:

- Identificación del estudio: la primera sección contiene los datos principales para identificar el estudio primario: un número consecutivo, el título de la publicación, sus autores, datos de contacto con los autores, el *journal* o congreso en que fue publicado, la fecha de publicación y la fuente de la que fue obtenido.
- Metodología del estudio: la segunda sección contiene el tipo de estudio, el país en el que fue desarrollado o aplicado, los objetivos fijados y otros campos específicos del tema de estudio de la revisión sistemática.
- Resultados del estudio: la tercera sección contiene información sobre los factores clave y las conclusiones extraídas de cada estudio.
- Problemas del estudio: la cuarta sección contiene las limitaciones del estudio y las desviaciones entre los resultados esperados y los obtenidos.

La última sección del formulario contiene los resultados subjetivos: impresiones generales y conclusiones sobre los resultados del estudio (salidas del estudio), contribución a la consecución de los objetivos propuestos en la investigación (contribución del estudio) y comentarios adicionales (otros aspectos).

Identificación del estudio	Número consecutivo:	
	Título de la publicación:	
	Autores:	
	Información de contacto:	
	Journal/Congreso:	
	Fecha:	
	Fuente:	

Metodología del estudio	Tipo de estudio:	
	País:	
	Objetivos:	
Resultados del estudio	Factores clave:	
	Conclusiones:	
Problemas del estudio	Limitaciones:	
	Desviación entre los resultados esperados y los obtenidos:	
Extracción de resultados	Salidas del estudio:	
	Contribución del estudio:	
	Otros aspectos:	

Tabla A.2. Formulario para la extracción de información de los estudios primarios

Después de una lectura detallada de cada uno de los estudios primarios y de una evaluación completa de la información contenida en ellos, los resultados extraídos deben ser registrados en el formulario.

A.5. Resumen de los resultados

La última etapa del protocolo de revisión sistemática tiene como objetivo presentar los datos resultantes del análisis de los estudios primarios. A continuación se detallan los elementos que define este protocolo para tal efecto:

- Cálculo estadístico de resultados.
- Presentación de los resultados en tablas.
- Comentarios finales: número de estudios, selección de estudios o extracción de la información, variaciones entre revisores, aplicación de los resultados y recomendaciones.

ANEXO B. Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5

A partir de un análisis por filas a un nivel mucho más detallado de la tabla 3.11, los siguientes apartados muestran todas las relaciones detectadas entre los resultados de los procesos de cada una de las seis categorías de procesos de la norma 20000-4 y las prácticas básicas de la norma ISO/IEC 15504-5.

B.1. Relaciones de los procesos generales del SGS

La tabla B.1 muestra todas las relaciones de los procesos de la categoría Procesos generales del SGS de la norma ISO/IEC 20000-4 con los procesos de la norma ISO/IEC 15504-5.

Procesos generales del SGS	**Grupos de Procesos de ISO/IEC 15504-5**								
	ACQ	SPL	ENG	OPE	MAN	PIM	RIN	REU	SUP
Auditoría									SUP.5
Gestión de recursos humanos							RIN.1 RIN.2		
Mejora						PIM.3			
Gestión de la información									SUP.7
Revisión de la dirección									SUP.4
Medición					MAN.6				
Gestión organizativa	ACQ.5	SPL.1 SPL.2	ENG.1		MAN.1 MAN.2 MAN.3 MAN.5				SUP.4
Gestión de riesgos					MAN.5				
Establecimiento y mantenimiento del SGS						PIM.1 PIM.3			

Tabla B.1. Relaciones entre los procesos generales del SGS de la norma ISO/IEC 20000-4 y los procesos de la norma ISO/IEC 15504-5

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los resultados obtenidos por los nueve procesos de esta categoría de procesos de la norma ISO/IEC 20000-4.

B.1.1. Relaciones del proceso de auditoría

El propósito del proceso de auditoría es determinar por separado la conformidad de los servicios, productos y procesos seleccionados con los requisitos, planes y acuerdos. Este proceso evalúa si se ha establecido y se mantiene el SGS y si los servicios se ajustan a los requisitos establecidos por el proveedor.

La tabla B.2 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Todos los resultados de este proceso quedan completamente cubiertos por prácticas básicas del proceso SUP.5 Auditoría. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de auditoría de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
1. Se define y se acuerda el alcance y el propósito de cada auditoría.	**SUP.5.BP1: Desarrollar e implementar una estrategia de auditoría**. Se implementa una estrategia de auditoría que define el propósito, el alcance, los hitos, los criterios de auditoría y el equipo de auditoría.
2. Se asegura la objetividad e imparcialidad en la realización de auditorías y en la selección de auditores.	**SUP.5.BP2: Seleccionar auditores**. Se seleccionan auditores independientes, imparciales y objetivos.
3. Se determina la conformidad de los servicios, productos y procesos seleccionados con los requisitos, planes y acuerdos.	**SUP.5.BP3: Auditar la conformidad con los requisitos**. Se auditan los productos, servicios o procesos seleccionados para determinar su conformidad con sus requisitos y disposiciones previstos. Se registran las no conformidades.
4. Se registran las no conformidades.	**SUP.5.BP3: Auditar la conformidad con los requisitos**. Se auditan los productos, servicios o procesos seleccionados para determinar su conformidad con sus requisitos y disposiciones previstos. Se registran las no conformidades.
5. Se comunican las no conformidades a los responsables de las acciones correctivas y de su resolución.	**SUP.5.BP4: Preparar y distribuir un informe de auditoría**. El auditor elabora y distribuye un informe de auditoría. **SUP.5.BP5: Tomar acciones correctivas**. La persona responsable asignada toma las acciones correctivas para hacer frente a las no conformidades. Las acciones correctivas pueden conllevar acciones inmediatas para resolver la no conformidad. También pueden conllevar otras acciones correctivas después de haber realizado un análisis de causas raíz.
6. Se verifican las acciones correctivas sobre las no conformidades.	**SUP.5.BP6: Seguir la resolución**. Se siguen las acciones correctivas hasta la resolución. El auditor puede revisar la resolución de las no conformidades y sus resultados.

Tabla B.2. Relaciones entre los resultados del proceso de auditoría y la norma ISO/IEC 15504-5

B.1.2. Relaciones del proceso de gestión de recursos humanos

El propósito del proceso de gestión de recursos humanos es proporcionar a la organización los recursos humanos necesarios y mantener sus competencias, de acuerdo con las necesidades del negocio y los requisitos del servicio. Este proceso se limita a identificar y desarrollar las competencias de las personas en relación con sus actividades de gestión de servicios.

La tabla B.3 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Casi todos los resultados de este proceso quedan cubiertos por prácticas básicas de los procesos RIN.1 Gestión de recursos humanos y RIN.2 Formación. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de recursos humanos de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se identifican las competencias requeridas por la organización para la provisión de servicios.	**RIN.1.BP1: Identificar las habilidades y las competencias necesarias**. Identificar y evaluar las habilidades y competencias que necesita la organización para lograr sus objetivos.
2. Se llena el vacío de competencias identificados mediante formación o contratación.	**RIN.2.BP2: Identificar las necesidades de formación**. Identificar las necesidades de formación. Identificar y evaluar las habilidades y competencias que deben facilitarse o mejorarse a través de la formación.
3. Se monitorizan las competencias individuales y su desarrollo.	**RIN.1.BP2: Definir los criterios de evaluación**. Definir unos criterios objetivos que se pueden utilizar para evaluar a los candidatos y evaluar el desempeño del personal. **RIN.1.BP8: Evaluar el rendimiento del personal**. Evaluar el rendimiento del personal, con respecto a su contribución a los objetivos de la organización como un todo. Garantizar que la retroalimentación se trata con el personal.
4. Cada individuo demuestra la comprensión de su papel en la consecución de los objetivos de la gestión de servicios.	

Tabla B.3. Relaciones entre los resultados del proceso de gestión de recursos humanos y la norma ISO/IEC 15504-5

B.1.3. Relaciones del proceso de mejora

El propósito del proceso de mejora es mejorar continuamente el SGS, los servicios y los procesos. Este proceso permite a un proveedor de servicios identificar oportunidades de mejora durante la operación de los procesos de gestión de servicios. Incluye la identificación, evaluación, aprobación, gestión, medición y revisión de las mejoras.

La tabla B.4 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Casi todos los resultados de este proceso quedan cubiertos por prácticas básicas del proceso PIM.3 Mejora de procesos. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de recursos humanos de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se identifican y registran las oportunidades de mejora.	**PIM.3.BP2: Identificar acciones**. Se identifican oportunidades de mejora derivadas del ambiente interno/externo de la organización y las razones justificadas para el cambio.
2. Se evalúan las oportunidades de mejora para su aprobación según los criterios acordados.	
3. Se priorizan las mejoras aprobadas y se planifican las acciones.	**PIM.3.BP4: Priorizar las mejoras**. Se priorizan los objetivos de mejora. **PIM.3.BP5: Planificar los cambios en el proceso**. Se definen y planifican los cambios en el proceso.
4. Se implementan y confirman las mejoras aprobadas.	**PIM.3.BP6: Implementar los cambios en el proceso**. Se implementan las mejoras en el proceso. **PIM.3.BP7: Confirmar la mejora del proceso**. Se monitorizan, miden y confirman los efectos de la implementación en el proceso según los objetivos de mejora definidos.
5. Se presentan y comunican los resultados de las acciones de mejora a las partes interesadas.	**PIM.3.BP8: Comunicar los resultados de la mejora**. Se comunica el conocimiento adquirido de las mejoras fuera del proyecto de mejora a través de las partes pertinentes de la organización.

Tabla B.4. Relaciones entre los resultados del proceso de mejora y la norma ISO/IEC 15504-5

B.1.4. Relaciones del proceso de gestión de la información

El propósito del proceso de gestión de la información es desarrollar y mantener registrada la información producida por un proceso. Este proceso tiene que ver con la producción, el almacenamiento, la difusión y la integridad de la información utilizada en el SGS.

La tabla B.5 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Casi todos los resultados de este proceso quedan completamente cubiertos por prácticas básicas del proceso SUP.7 Documentación. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de la información de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se produce la información de acuerdo con los criterios definidos.	**SUP.7.BP1: Desarrollar una estrategia de gestión de la documentación**. Determinar la estrategia de gestión de la documentación que cubra todo lo que debería ser documentado en cada área de la organización, para cada fase del ciclo de vida del producto/servicio. **SUP.7.BP2: Establecer estándares para los documentos**. Establecer estándares para desarrollar, modificar y mantener los documentos. **SUP.7.BP3: Especificar los requisitos de los documentos**. Especificar los requisitos de los documentos tales como formato, título, fecha, identificación, historial de versiones, autor/es, responsable de la revisión, responsable de la autorización, resumen de contenidos, finalidad y lista de distribución.
2. Se controla y se hace pública la información de acuerdo con los criterios definidos.	**SUP.7.BP6: Revisar los documentos**. Revisar los documentos antes de su distribución, y autorizarlos antes de su distribución o difusión.
3. Se comunica la información a las partes interesadas.	**SUP.7.BP7: Distribuir los documentos**. Para proveer documentos, distribuir los documentos según los modos de distribución determinados, a través de los medios de comunicación apropiados para audiencias específicas, y confirmar la entrega de los documentos cuando sea necesario.
4. Se mantiene la información de acuerdo con las disposiciones previstas.	**SUP.7.BP8: Mantener los documentos**. Mantener los documentos de acuerdo con la estrategia de documentación establecida.
5. Se garantiza la integridad de la información.	

Tabla B.5. Relaciones entre los resultados del proceso de gestión de la información y la norma ISO/IEC 15504-5

B.1.5. Relaciones con el proceso de revisión de la dirección

El propósito del proceso de revisión de la dirección es evaluar el rendimiento del SGS e identificar posibles mejoras. Este proceso revisa el SGS a intervalos planificados, para asegurar su conveniencia, adecuación y eficacia. Para ello, tiene en cuenta los resultados

de las auditorías, el rendimiento de los servicios, los informes de servicio, las incidencias, los errores conocidos, los riesgos y las sugerencias y comentarios de todas las partes interesadas.

La tabla B.6 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Todos los resultados de este proceso quedan completamente cubiertos por prácticas básicas del proceso SUP.4 Revisión conjunta. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de revisión de la dirección de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se establecen los objetivos de la revisión.	**SUP.4.BP1: Identificar las revisiones**. Identificar el calendario, el alcance y los participantes de las revisiones de gestión y técnicas, según las necesidades del proyecto.
2. Se evalúa el estado y el rendimiento de una actividad o proceso.	**SUP.4.BP3: Llevar a cabo revisiones conjuntas**. Llevar a cabo las revisiones conjuntas de gestión y técnicas. Registrar los resultados de las revisiones según lo previsto.
3. Se identifican y registran los riesgos, problemas y oportunidades de mejora.	**SUP.4.BP5: Determinar las acciones para los resultados de la revisión**. Analizar el informe de la revisión, identificar y registrar los problemas, proponer soluciones a los resultados de la revisión, determinar la prioridad de las acciones.
4. Se comunican los resultados de la revisión a las partes interesadas.	**SUP.4.BP4: Comunicar los resultados**. Los resultados de la revisión deben ser puestos a disposición de todas las partes afectadas.
5. Se realiza un seguimiento de las acciones resultantes de la revisión hasta su cierre.	**SUP.4.BP6: Realizar el seguimiento de las acciones para los resultados de la revisión**. Realizar el seguimiento de las acciones para la resolución de los problemas identificados en la revisión. Informar y documentar los cambios en los productos de trabajo y procesos.

Tabla B.6. Relaciones entre los resultados del proceso de revisión de la dirección y la norma ISO/IEC 15504-5

B.1.6. Relaciones del proceso de medición

El propósito del proceso de medición es identificar, recopilar, analizar y presentar los datos relativos a los servicios prestados y a los procesos implementados para dar soporte a la gestión eficaz de los procesos, y para demostrar objetivamente la calidad de los servicios

prestados. Este proceso permite identificar, desarrollar y utilizar un conjunto de medidas que proporcionan información cuantitativa para demostrar una provisión de servicios eficaz y detectar oportunidades de mejora.

La tabla B.7 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Todos los resultados de este proceso quedan completamente cubiertos por prácticas básicas del proceso MAN.6 Medición. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de medición de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se identifican las necesidades de información prioritarias relacionadas con los servicios prestados y los procesos implementados.	**MAN.6.BP3: Identificar las necesidades de medición de información**. Identificar las necesidades de medición de información de los procesos organizativos y de gestión.
2. Se identifica y/o se desarrolla un conjunto adecuado de medidas, impulsadas por las necesidades de información.	**MAN.6.BP4: Especificar las medidas**. Identificar y desarrollar un conjunto adecuado de medidas basadas en las necesidades de medición de información.
3. Se recogen y se verifican los datos necesarios.	**MAN.6.BP5: Recoger y almacenar datos de la medición**. Identificar, recoger y almacenar los datos de la medición, incluyendo la información de contexto necesaria para verificar, comprender o evaluar los datos.
4. Se analizan los datos necesarios e interpretan los resultados.	**MAN.6.BP6: Analizar los datos de la medición**. Analizar e interpretar los datos de la medición y desarrollar productos de información.
5. Se utiliza la información del proceso de medición para dar soporte a las decisiones y proporcionar una base objetiva para la comunicación.	**MAN.6.BP7: Utilizar los productos de información de la medición para la toma de decisiones**. Poner los productos de información de la medición precisos y actualizados a disposición de los procesos de toma de decisiones para los que pueden ser relevantes.

Tabla B.7. Relaciones entre los resultados del proceso de medición y la norma ISO/IEC 15504-5

B.1.7. Relaciones del proceso de gestión organizativa

El propósito del proceso de gestión organizativa es establecer los objetivos de la gestión de servicios de TI, identificar y proporcionar los recursos necesarios, y monitorizar el rendimiento de los servicios proveídos, con el fin de satisfacer las necesidades de los clientes y de todas las partes interesadas.

La tabla B.8 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. La mayoría de los aspectos indicados por los resultados de este proceso quedan cubiertos por prácticas básicas de los procesos ACQ.5 Aceptación del cliente, SPL.1 Oferta del proveedor, SPL.2 Entrega del producto, ENG.1 Captura de requisitos, MAN.1 Alineación de la organización, MAN.2 Gestión de la organización, MAN.3 Gestión de proyectos, MAN.5 Gestión de riesgos y SUP.4 Revisión conjunta. Por tanto, existe una relación fuerte entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión organizativa de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se establecen los requisitos del servicio en respuesta a las necesidades del negocio, los requisitos del cliente y las peticiones de los clientes.	**SPL.1.BP8: Preparar la propuesta de proveedor o la respuesta de licitación**. Se prepara una propuesta de proveedor o de licitación como respuesta a la petición del cliente. **ENG.1.BP1: Obtener los requisitos y las peticiones del cliente**. Obtener y definir los requisitos y las peticiones del cliente a través de la solicitud directa y continua de información a los clientes y usuarios.
2. Se identifican y se establecen los objetivos y los requisitos de gestión de servicios para satisfacer las necesidades del negocio, los procesos financieros del proveedor de servicios y los requisitos reglamentarios, contractuales y legales.	**ENG.1.BP1: Obtener los requisitos y las peticiones del cliente**. Obtener y definir los requisitos y las peticiones del cliente a través de la solicitud directa y continua de información a los clientes y usuarios.
3. La estructura de la organización permite la provisión de los servicios.	**MAN.1.BP1: Desarrollar una visión estratégica**. Desarrollar una visión estratégica de la organización identificando sus objetivos de negocio y la relación de las funciones de ingeniería de sistemas y del software con las actividades básicas de la organización.
4. Se planifica y ejecuta la gestión de servicios con la intención de lograr los objetivos de gestión de servicios y la satisfacción de los clientes.	
5. Se identifican roles, competencias, facultades y responsabilidades para permitir la provisión de los servicios.	**MAN.2.BP1: Identificar la infraestructura de gestión**. Identificar la infraestructura de gestión adecuada para llevar a cabo prácticas de gestión de software que sean compatibles con los objetivos empresariales de la organización. NOTA: La infraestructura de gestión puede incluir funciones y responsabilidades organizativas, el sistema de toma de decisiones, mecanismos de comunicación y la planificación y el control de las operaciones de negocio.

Resultados del proceso de gestión organizativa de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
6. Se designan las personas con las competencias adecuadas para las funciones necesarias para llevar a cabo actividades de gestión de servicios.	**SPL.1.BP6: Identificar y designar al personal**. Identificar y designar al personal con las competencias apropiadas para la tarea.
7. Se determinan y proporcionan los recursos y la infraestructura.	**MAN.2.BP1: Identificar la infraestructura de gestión**. Identificar la infraestructura de gestión adecuada para llevar a cabo prácticas de gestión de software que sean compatibles con los objetivos empresariales de la organización. NOTA: La infraestructura de gestión puede incluir funciones y responsabilidades organizativas, el sistema de toma de decisiones, mecanismos de comunicación y la planificación y el control de las operaciones de negocio. **MAN.2.BP2: Proporcionar la infraestructura de gestión**. Proporcionar la infraestructura de gestión identificada, adecuada en el ámbito más amplio de la organización.
8. Se desarrollan servicios que cumplan con los requisitos acordados.	
9. Se prestan servicios de acuerdo con los requisitos acordados.	**SPL.2.BP11: Entregar el producto al cliente**. Entregar el producto al cliente, con confirmación positiva de recepción.
10. Se gestionan los servicios suministrados por otras partes para cumplir con los requisitos de servicio.	**ACQ.5.BP1: Evaluar el producto entregado**. Llevar a cabo la evaluación del producto/servicio usando los criterios de aceptación definidos. **ACQ.5.BP2: Cumplimiento del acuerdo.** Resolver cualquier problema de aceptación, de conformidad con los procedimientos establecidos en el acuerdo y confirmar que el producto o servicio entregado cumple con el acuerdo.
11. Se monitoriza el rendimiento y el progreso según las disposiciones previstas.	**MAN.3.BP12: Monitorizar los atributos del proyecto**. Monitorizar el ámbito, el presupuesto, el coste, los recursos y otros atributos necesarios y documentar las desviaciones significativas de estos atributos frente a la línea de base. **MAN.3.BP13: Revisar el progreso del proyecto**. Reportar regularmente y revisar el estado de la realización del proyecto frente al plan del proyecto.
12. Se realiza un seguimiento hasta su cierre de las cuestiones derivadas de las revisiones del SGS y los proveedores.	**SUP.4.BP6: Realizar el seguimiento de las acciones para los resultados de la revisión**. Realizar el seguimiento de las acciones para la resolución de los problemas identificados en la revisión. Informar y documentar los cambios en los productos de trabajo y procesos.

Resultados del proceso de gestión organizativa de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
13. Se identifican, analizan, tratan y controlan continuamente los riesgos de la organización.	**MAN.5.BP3: Identificar los riesgos del proyecto**. Identificar los riesgos del proyecto, tanto inicialmente en la estrategia del proyecto, como cuando surjan durante el desarrollo del mismo. **MAN.5.BP4: Analizar los riesgos del proyecto**. Analizar los riesgos y aplicar medidas de riesgos para determinar la prioridad con la que se aplicarán los recursos para monitorizar los riesgos. **MAN.5.BP5: Definir y realizar acciones de tratamiento de riesgos**. Para cada riesgo (o conjunto de riesgos) definir y realizar las acciones apropiadas para reducir los riesgos a un nivel aceptable. **MAN.5.BP6: Monitorizar los riesgos**. Monitorizar el estado actual de cada riesgo, identificar los cambios en el estado de los riesgos y evaluar la efectividad de las acciones de tratamiento de riesgos.
14. Se toman medidas para mejorar la eficacia y eficiencia del SGS para cumplir los objetivos y los requisitos de gestión de servicios.	

Tabla B.8. Relaciones entre los resultados del proceso de gestión organizativa y la norma ISO/IEC 15504-5

B.1.8. Relaciones del proceso de gestión de riesgos

El propósito del proceso de gestión de riesgos es identificar, analizar, evaluar, tratar y monitorizar continuamente los riesgos relacionados con la provisión de servicios a los clientes. Se puede aplicar a los riesgos relacionados con otros procesos de gestión de servicios, como puede ser el de gestión de la seguridad de la información, el de gestión de la continuidad y la disponibilidad del servicio o el de gestión del cambio, entre otros.

La tabla B.9 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Casi todos los resultados de este proceso quedan completamente cubiertos por prácticas básicas del proceso MAN.5 Gestión de riesgos. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de riesgos de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se identifican los riesgos a medida que ocurren.	**MAN.5.BP3: Identificar los riesgos**. Identificar los riesgos del proyecto, tanto inicialmente durante la planificación del proyecto como a medida que se desarrollen durante la ejecución del proyecto. NOTA: Ejemplos de riesgos incluyen el coste, el calendario, el esfuerzo, los recursos y los riesgos técnicos, entre otros.
2. Se clasifican y evalúan los riesgos identificados y se determina la prioridad en la que aplicar recursos para el tratamiento de estos riesgos.	**MAN.5.BP4: Analizar los riesgos**. Analizar los riesgos y aplicar medidas de riesgos para determinar la prioridad en la que aplicar los recursos para controlar los riesgos. NOTA: Los temas a considerar en el análisis de riesgos incluyen la probabilidad y el impacto de la ocurrencia de cada riesgo identificado.
3. Se comunican los riesgos y su tratamiento propuesto a las partes interesadas.	
4. Se monitorizan los riesgos evaluados.	**MAN.5.BP6: Monitorizar riesgos**. Monitorizar el estado actual de cada riesgo, determinar los cambios en la situación del riesgo y evaluar la eficacia de las acciones de tratamiento del riesgo.
5. Se realiza el tratamiento apropiado para corregir o evitar riesgos inaceptables.	**MAN.5.BP5: Definir y realizar acciones de tratamiento de riesgos**. Para cada riesgo (o conjunto de riesgos) definir y realizar las acciones adecuadas para reducir los riesgos a un nivel aceptable.

Tabla B.9. Relaciones entre los resultados del proceso de gestión de riesgos y la norma ISO/IEC 15504-5

B.1.9. Relaciones del proceso de establecimiento y mantenimiento del SGS

El propósito del proceso de establecimiento y mantenimiento del SGS es proporcionar los procesos de gestión de servicios que permiten una efectiva implementación y gestión de todos los servicios de TI. El alcance de este proceso incluye la creación de todas las políticas, procedimientos y planes requeridos por los procesos organizacionales y operativos del SGS. Este proceso también identifica los roles y responsabilidades asociadas con la supervisión de los procesos de gestión de servicios.

La tabla B.10 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. La mayoría de los aspectos indicados por los resultados de este proceso quedan cubiertos por prácticas básicas de los procesos PIM.1 Establecimiento de procesos y PIM.3 Mejora de procesos. Por tanto, existe una relación fuerte entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de establecimiento y mantenimiento del SGS de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
1. Se establecen los procesos del SGS para dar soporte a los objetivos de la gestión de servicios.	**PIM.1.BP1: Definir la arquitectura de procesos**. Definir un conjunto estándar de procesos, el propósito de cada proceso y las interacciones entre ellos. **PIM.1.BP2: Dar soporte al despliegue de los procesos**. Dar soporte al uso en toda la organización de los procesos estándar de acuerdo con el propósito de cada proceso. **PIM.1.BP3: Definir los procesos estándar**. Definir y mantener una descripción de cada proceso estándar de acuerdo con las necesidades de establecer procesos de la organización.
2. Se definen los roles y las responsabilidades necesarias para dar soporte a los procesos del SGS.	
3. Se mejora continuamente la eficacia y eficiencia de los procesos del SGS en línea con los objetivos del SGS.	**PIM.3.BP3: Establecer objetivos de mejora de procesos**. Se lleva a cabo un análisis de la situación actual de los procesos existentes, centrándose en aquellos procesos de los que surgen estímulos de mejora y/o el riesgo es reducido, dando lugar al establecimiento de objetivos de mejora para el proceso. **PIM.3.BP6: Implementar cambios en el proceso**. Se implementan las mejoras en el proceso.

Tabla B.10. Relaciones entre los resultados del proceso de establecimiento y mantenimiento del SGS y la norma ISO/IEC 15504-5

B.2. Relaciones de los procesos de diseño y transición de nuevos servicios o servicios modificados

La tabla B.11 muestra todas las relaciones de los procesos de la categoría Procesos de diseño y transición de nuevos servicios o servicios modificados de la norma ISO/IEC 20000-4 con los procesos de la norma ISO/IEC 15504-5.

Procesos de diseño y transición de nuevos servicios o servicios modificados	Grupos de Procesos de ISO/IEC 15504-5								
	ACQ	SPL	ENG	OPE	MAN	PIM	RIN	REU	SUP
Diseño del servicio									

Procesos de diseño y transición de nuevos servicios o servicios modificados	**Grupos de Procesos de ISO/IEC 15504-5**								
	ACQ	SPL	ENG	OPE	MAN	PIM	RIN	REU	SUP
Planificación y monitorización del servicio					MAN.3				
Requisitos del servicio			ENG.1						SUP.3
Transición del servicio		SPL.2		OPE.1					

Tabla B.11. Relaciones entre los procesos de diseño y transición de nuevos servicios o servicios modificados de la norma ISO/IEC 20000-4 y los procesos de la norma ISO/IEC 15504-5

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los resultados obtenidos por los cuatro procesos de esta categoría de procesos de la norma ISO/IEC 20000-4.

B.2.1. Relaciones del proceso de diseño del servicio

El propósito del proceso de diseño del servicio es diseñar y desarrollar servicios nuevos o modificados. Este proceso toma los requisitos de servicios nuevos y/o los de servicios modificados, e identifica las actividades necesarias para el diseño de una solución consensuada.

La tabla B.12 muestra los resultados de este proceso. Estos resultados no están relacionados con ninguna práctica básica de la norma ISO/IEC 15504-5. Por tanto, no existe ninguna relación entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de diseño del servicio de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se diseñan servicios nuevos o modificados para satisfacer las necesidades del negocio acordadas y los requisitos de los clientes.	
2. Se prepara una especificación del servicio que define los atributos de los servicios nuevos o modificados.	
3. Se especifica la infraestructura y los componentes del servicio para dar soporte al servicio diseñado.	

Resultados del proceso de diseño del servicio de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
4. Se desarrollan servicios nuevos o modificados que satisfacen los criterios indicados en la especificación del servicio.	

Tabla B.12. Relaciones entre los resultados del proceso de diseño del servicio y la norma ISO/IEC 15504-5

B.2.2. Relaciones del proceso de planificación y monitorización del servicio

El propósito del proceso de planificación y monitorización del servicio es planificar y supervisar la provisión de un servicio nuevo o modificado. La planificación se encarga de traducir las decisiones estratégicas en servicios y garantiza que las propuestas de servicios nuevos o modificados tengan en cuenta todas las implicaciones económicas, organizacionales, procedimentales, técnicas y comerciales de los cambios de los servicios. La monitorización se encarga de realizar el seguimiento del progreso de acuerdo con el tiempo, coste y restricciones de calidad estimados.

La tabla B.13 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Todos los resultados de este proceso quedan cubiertos por prácticas básicas del proceso MAN.3 Gestión de proyectos. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de planificación y monitorización del servicio de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
1. Se define el alcance del trabajo necesario para la provisión de servicios nuevos o modificados.	**MAN.3.BP1: Definir el ámbito de trabajo**. Identificar los objetivos, la motivación y los límites del proyecto y definir el trabajo a realizar.
2. Se evalúa la viabilidad de alcanzar los requisitos del servicio nuevo o modificado con los recursos disponibles y las restricciones.	**MAN.3.BP3: Evaluar la viabilidad del proyecto**. Evaluar la viabilidad de satisfacer los objetivos del proyecto con los recursos disponibles y considerando las restricciones.
3. Se clasifican y estiman las tareas y los recursos necesarios para completar el trabajo.	**MAN.3.BP5: Definir las actividades y tareas**. Identificar las actividades y las tareas del proyecto de acuerdo con el ciclo de vida definido y definir las dependencias entre ellas.
4. Se identifican las interfaces entre las unidades organizacionales y las partes externas.	**MAN.3.BP8: Identificar y monitorizar las interfaces del proyecto**. Identificar y acordar las interfaces del proyecto con otros proyectos, unidades organizativas y otras partes afectadas. Monitorizar los acuerdos realizados.

Resultados del proceso de planificación y monitorización del servicio de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
5. Se desarrollan planes para la provisión de los servicios nuevos o modificados.	**MAN.3.BP10: Establecer el plan del proyecto**. Definir y mantener el plan del proyecto y otros planes relevantes para cubrir el ámbito, los objetivos, los recursos, la infraestructura, las interfaces y los mecanismos de comunicación del proyecto.
6. Se activan los planes para la ejecución de la provisión de los servicios nuevos o modificados.	**MAN.3.BP11: Llevar a cabo el plan del proyecto**. Llevar a cabo las actividades planificadas del proyecto, registrar el estado del progreso y darlo a conocer a todas las partes afectadas.
7. Se supervisa e informa del progreso de la provisión del servicio nuevo o modificado.	**MAN.3.BP12: Monitorizar los atributos del proyecto**. Monitorizar el ámbito, el presupuesto, el coste, los recursos y otros atributos necesarios y documentar las desviaciones significativas de estos atributos frente a la línea de base. **MAN.3.BP13: Revisar el progreso del proyecto**. Reportar regularmente y revisar el estado de la realización del proyecto frente al plan del proyecto.
8. Se ejecutan acciones para corregir las desviaciones del plan cuando no se logran los objetivos.	**MAN.3.BP14: Actuar para corregir desviaciones**. Emprender acciones cuando los objetivos del proyecto no se cumplan, para corregir las desviaciones del plan y para prevenir la recurrencia de los problemas identificados en el proyecto. Actualizar los planes del proyecto adecuadamente.

Tabla B.13. Relaciones entre los resultados del proceso de planificación y monitorización del servicio y la norma ISO/IEC 15504-5

B.2.3. Relaciones del proceso de requisitos del servicio

El propósito del proceso de requisitos del servicio es establecer y acordar los requisitos del servicio, que puede tener su origen dentro del propio proveedor de servicios (creación del catálogo de servicios) o surgir de las peticiones de los clientes (construcción a medida).

La tabla B.14 muestra los resultados de este proceso y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. La mayoría de los aspectos indicados por los resultados de este proceso quedan cubiertos por prácticas básicas de los procesos ENG.1 Captura de requisitos y SUP.3 Validación. Por tanto, existe una relación fuerte entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de requisitos del servicio de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
1. Se identifican y registran las características requeridas y el contexto de uso de los servicios nuevos o modificados.	**ENG.1.BP1: Obtener peticiones y requisitos del cliente**. Obtener y definir las peticiones y los requisitos del cliente mediante la solicitud directa y continua de información de los clientes y usuarios.
2. Se definen las restricciones de las soluciones de servicio.	**ENG.1.BP1: Obtener peticiones y requisitos del cliente**. Obtener y definir las peticiones y los requisitos del cliente mediante la solicitud directa y continua de información de los clientes y usuarios.
3. Se definen los requisitos del servicio nuevo o modificado.	**ENG.1.BP4: Establecer la línea de base de los requisitos del cliente**. Formalizar los requisitos del cliente y establecer una línea de base para utilizar en el proyecto y para poder realizar el seguimiento de las necesidades del cliente.
4. Se definen los requisitos para la validación del servicio nuevo o modificado.	**SUP.3.BP1: Desarrollar una estrategia de validación**. Desarrollar e implementar una estrategia de validación que incluya las actividades de validación con los métodos, técnicas y herramientas asociados, los productos de trabajo o procesos a validar, los grados de independencia para la validación y el cronograma para la realización de estas actividades.
5. Se negocian y acuerdan los requisitos del servicio nuevo o modificado.	**ENG.1.BP3: Acordar los requisitos**. Obtener un acuerdo entre los equipos acerca de los requisitos del cliente disponiendo de las firmas de los representantes de todos los equipos y de todas las partes contractualmente sujetas a trabajar con estos requisitos.

Tabla B.14. Relaciones entre los resultados del proceso de requisitos del servicio y la norma ISO/IEC 15504-5

B.2.4. Relaciones del proceso de transición del servicio

El propósito del proceso de transición del servicio incluye las actividades de construcción, pruebas, verificación y validación que permiten al proveedor de servicios aceptar un servicio nuevo o modificado de acuerdo con los criterios de aceptación definidos. Este proceso prepara y coordina los recursos y las personas necesarios para poner con éxito un servicio en producción de acuerdo con el tiempo, coste y limitaciones de calidad estimados.

La tabla B.15 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Algunos de los aspectos indicados por los resultados de este proceso quedan parcialmente cubiertos por prácticas básicas de los procesos SPL.2 Entrega del producto y OPE.1 Uso operacional. Por tanto, existe una relación parcial entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de transición del servicio de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se determinan y acuerdan los requisitos para la transición de los servicios.	
2. Se identifican, acuerdan, adquieren y asignan habilidades y experiencia nuevas o modificadas.	
3. Se identifican, acuerdan y realizan las actividades de transición que deben llevar a cabo el proveedor de servicios o el cliente.	**OPE.1.BP3: Poner el producto en funcionamiento**. Poner el producto en funcionamiento en el entorno específico y del modo indicado.
4. Se identifican métodos, procedimientos y medidas nuevos o modificados para los servicios nuevos y los servicios modificados.	**OPE.1.BP4: Desarrollar criterios para el uso operativo**. Se desarrollan los criterios para el uso operativo que puedan demostrar el cumplimiento con los requisitos acordados.
5. Se identifican autoridades y responsabilidades nuevas o modificadas para los servicios nuevos y los servicios modificados.	
6. Se identifican e implementan contratos y acuerdos formales nuevos o modificados con los grupos internos y con los proveedores para ajustarse a los cambios en los requisitos.	
7. Se identifican e implementan planes nuevos o modificados para la disponibilidad, la continuidad del servicio, la capacidad y seguridad de la información.	
8. Se identifican y proporcionan recursos para la provisión de los servicios nuevos o modificados.	
9. Se implementa y prueba el servicio nuevo o modificado de acuerdo con la especificación del servicio.	**OPE.1.BP2: Realizar pruebas de funcionamiento**. Realizar pruebas de funcionamiento de cada entrega del producto, evaluando la satisfacción con los criterios especificados.
10. Se acepta el servicio nuevo o modificado de acuerdo con los criterios de aceptación del servicio.	**SPL.2.BP10: Asegurar la aprobación de la entrega del producto antes de realizarla**. Asegurar que se satisfacen los criterios de la entrega del producto antes de realizar las tareas propias de la entrega.

Resultados del proceso de transición del servicio de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
11. Se comunica a las partes interesadas la información sobre el resultado de la transición del servicio nuevo o modificado.	**SPL.2.BP6: Comunicar el tipo, el nivel y la duración del soporte para la entrega**. Identificar y comunicar el tipo, el nivel y la duración de la entrega.

Tabla B.15. Relaciones entre los resultados del proceso de transición del servicio y la norma ISO/IEC 15504-5

B.3. Relaciones de los procesos de provisión del servicio

La tabla B.16 muestra todas las relaciones de los procesos de la categoría Procesos de provisión del servicio de la norma ISO/IEC 20000-4 con los procesos de la norma ISO/IEC 15504-5.

Procesos de provisión del servicio	Grupos de Procesos de ISO/IEC 15504-5								
	ACQ	SPL	ENG	OPE	MAN	PIM	RIN	REU	SUP
Elaboración del presupuesto y contabilidad de los servicios de TI					MAN.3				
Gestión de la capacidad									
Gestión de la seguridad de la información					MAN.5		RIN.4		
Gestión de la continuidad y disponibilidad del servicio									
Gestión del nivel de servicio				OPE.2					
Generación de informes del servicio									SUP.7

Tabla B.16. Relaciones entre los procesos de provisión del servicio de la norma ISO/IEC 20000-4 y los procesos de la norma ISO/IEC 15504-5

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los resultados obtenidos por los seis procesos de esta categoría de procesos de la norma ISO/IEC 20000-4.

B.3.1. Relaciones del proceso de elaboración del presupuesto y contabilidad de los servicios de TI

El propósito del proceso de elaboración del presupuesto y contabilidad de los servicios de TI es presupuestar y llevar las contabilidad de la provisión de los servicios. La parte de presupuesto cubre la predicción y el control de los gastos y la supervisión y ajuste de los presupuestos. La parte de contabilidad se encarga de calcular los costes de entrega de los servicios de TI, de compararlos con los costes presupuestados y de gestionar las variaciones en el presupuesto.

La tabla B.17 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. La mayoría de los aspectos indicados por los resultados de este proceso quedan cubiertos por prácticas básicas del proceso MAN.3 Gestión de proyectos. Por tanto, existe una relación fuerte entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de elaboración del presupuesto y contabilidad de los servicios de TI de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se estiman los costes de la provisión del servicio.	
2. Se elaboran presupuestos mediante estimaciones de costes.	**MAN.3.BP4: Determinar y mantener estimaciones de los atributos del proyecto**. Definir y mantener líneas de base de los atributos del proyecto. NOTA: Los atributos del proyecto pueden incluir 1) objetivos de calidad y objetivos de negocio del proyecto, 2) tamaño y complejidad y 3) esfuerzo, planificación y presupuesto del proyecto.
3. Se controlan las desviaciones del presupuesto y los costes.	**MAN.3.BP12: Monitorizar los atributos del proyecto**. Monitorizar el ámbito, el presupuesto, el coste, los recursos y otros atributos necesarios y documentar las desviaciones significativas de estos atributos frente a la línea de base.
4. Se resuelven las desviaciones del presupuesto.	**MAN.3.BP14: Actuar para corregir desviaciones**. Emprender acciones cuando los objetivos del proyecto no se cumplan, para corregir las desviaciones del plan y para prevenir la recurrencia de los problemas identificados en el proyecto. Actualizar los planes del proyecto adecuadamente.
5. Se comunican a las partes interesadas las desviaciones del presupuesto y los costes.	

Tabla B.17. Relaciones entre los resultados del proceso de elaboración del presupuesto y contabilidad de los servicios de TI y la norma ISO/IEC 15504-5

B.3.2. Relaciones con del proceso de gestión de la capacidad

El propósito del proceso de gestión de la capacidad es asegurar que el proveedor de servicios dispone de recursos y capacidad suficientes durante todo el servicio para satisfacer los requisitos actuales y futuros acordados de forma rentable y oportuna, y cumplir con los objetivos de nivel de servicio.

La tabla B.18 muestra los resultados de este proceso. Estos resultados no están relacionados con ninguna práctica básica de la norma ISO/IEC 15504-5. Por tanto, no existe ninguna relación entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de la capacidad de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se identifican y acuerdan los requisitos de capacidad y de rendimiento actuales y futuros.	
2. Se desarrolla un plan de capacidad basado en los requisitos de capacidad y de rendimiento.	
3. Se provee la capacidad necesaria para satisfacer los requisitos actuales de capacidad y de rendimiento.	
4. Se monitoriza y analiza el uso de la capacidad y se ajusta el rendimiento.	
5. Se prepara la capacidad necesaria para satisfacer las necesidades futuras de capacidad y de rendimiento.	
6. Se reflejan en el plan de capacidad los cambios de capacidad y de rendimiento.	

Tabla B.18. Relaciones entre los resultados del proceso de gestión de la capacidad y la norma ISO/IEC 15504-5

B.3.3. Relaciones del proceso de gestión de la seguridad de la información

El propósito del proceso de gestión de la seguridad de la información es gestionar la seguridad de la información a un nivel de seguridad acordado en todas las actividades de gestión de servicios. Este proceso asegura que los controles de seguridad necesarios para realizar las actividades de gestión de servicios protegen adecuadamente los activos de información.

La tabla B.19 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. La mayoría de los aspectos indicados por los resultados de este proceso quedan cubiertos por prácticas básicas de los procesos RIN.4 Infraestructura y MAN.5 Gestión de riesgos. Por tanto, existe una relación fuerte entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de la seguridad de la información de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se identifican y acuerdan los requisitos de seguridad de la información.	**RIN.4.BP2: Definir los requisitos de infraestructura.** Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. NOTA: Los requisitos del proceso de infraestructura pueden incluir los de seguridad.
2. Se identifican los criterios para evaluar los riesgos de seguridad de la información y el nivel aceptable de riesgo.	**MAN.5.BP1: Establecer el ámbito de la gestión de riesgos**. Determinar el ámbito de la gestión de riesgos a realizar. **MAN.5.BP2: Definir las estrategias de gestión de riesgos**. Definir estrategias y medidas de gestión de riesgos apropiadas para identificar, analizar, tratar y monitorizar cada riesgo o conjunto de riesgos, tanto a nivel de proyecto como a nivel de organización.
3. Se identifican los riesgos de seguridad de la información.	**MAN.5.BP3: Identificar los riesgos**. Identificar los riesgos del proyecto, tanto inicialmente en la estrategia del proyecto, como cuando surjan durante el desarrollo del mismo. NOTA: Los riesgos podrían estar relacionados con las siguientes áreas: coste, planificación, esfuerzo, recursos y riesgos técnicos.
4. Se evalúan los riesgos de seguridad de la información.	**MAN.5.BP4: Analizar los riesgos**. Analizar los riesgos y aplicar medidas de riesgos para determinar la prioridad con la que se aplicarán los recursos para monitorizar los riesgos. NOTA: Los aspectos a ser considerados en el análisis de riesgos pueden ser la probabilidad y el impacto de cada uno de los riesgos identificados.
5. Se definen medidas y controles de riesgos de seguridad de la información.	**MAN.5.BP5: Definir y realizar acciones de tratamiento de riesgos**. Para cada riesgo (o conjunto de riesgos) definir y realizar las acciones apropiadas para reducir los riesgos a un nivel aceptable. **MAN.5.BP6: Monitorizar los riesgos**. Monitorizar el estado actual de cada riesgo, identificar los cambios en el estado de los riesgos y evaluar la efectividad de las acciones de tratamiento de riesgos .

Resultados del proceso de gestión de la seguridad de la información de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
6. Se implementan medidas y controles de riesgos de seguridad de la información.	**MAN.5.BP5: Definir y realizar acciones de tratamiento de riesgos**. Para cada riesgo (o conjunto de riesgos) definir y realizar las acciones apropiadas para reducir los riesgos a un nivel aceptable. **MAN.5.BP7: Llevar a cabo acciones preventivas o correctivas**. Cuando no se consiga mitigar el riesgo según lo previsto, llevar a cabo acciones preventivas para reducir o evitar el impacto cada riesgo. Cuando la mitigación del riesgo no pueda reducir o evitar el riesgo, planificar acciones correctoras para resolver el problema derivado del riesgo.
7. Se cuantifican y registran los incidentes de seguridad.	
8. Se comunican los asuntos relacionados con la seguridad de la información a las partes interesadas.	
9. Se analiza y reporta el impacto de los cambios en seguridad de la información.	

Tabla B.19. Relaciones entre los resultados del proceso de gestión de la seguridad de la información y la norma ISO/IEC 15504-5

B.3.4. Relaciones del proceso de gestión de la continuidad y disponibilidad del servicio

El propósito del proceso de gestión de la continuidad y disponibilidad del servicio es asegurar que se podrán cumplir los niveles de servicio acordados en circunstancias previsibles. Este proceso incluye la definición, análisis, planificación, medición y mejora de todos los aspectos relacionados con la continuidad y la disponibilidad del servicio, con el objetivo de reducir los riesgos a un nivel aceptable y planificar la recuperación del servicio en caso de que se produzca una interrupción.

La tabla B.20 muestra los resultados de este proceso. Estos resultados no están relacionados con ninguna práctica básica de la norma ISO/IEC 15504-5. Por tanto, no existe ninguna relación entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de la continuidad y disponibilidad del servicio de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
1. Se identifican los requisitos de continuidad y disponibilidad del servicio.	

Resultados del proceso de gestión de la continuidad y disponibilidad del servicio de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
2. Se desarrolla un plan de continuidad del servicio a partir de los requisitos de continuidad del servicio.	
3. Se desarrolla un plan de disponibilidad del servicio a partir de los requisitos de disponibilidad del servicio.	
4. Se prueba la continuidad del servicio contra los requisitos de continuidad del servicio para validar el plan.	
5. Se prueba la disponibilidad del servicio contra los requisitos de disponibilidad del servicio para validar el plan.	
6. Se monitoriza la disponibilidad del servicio.	
7. Se identifican y analizan las causas subyacentes de las no disponibilidades del servicio no planificadas.	
8. Se llevan a cabo acciones correctivas para solucionar las causas subyacentes identificadas.	
9. Se reflejan los cambios en los requisitos de continuidad del servicio en el plan de continuidad del servicio.	
10. Se reflejan los cambios en los requisitos de disponibilidad del servicio en el plan de disponibilidad del servicio.	

Tabla B.20. Relaciones entre los resultados del proceso de gestión de la continuidad y disponibilidad del servicio y la norma ISO/IEC 15504-5

B.3.5. Relaciones del proceso de gestión del nivel de servicio

El propósito del proceso de gestión del nivel de servicio es asegurar que se cumplen los objetivos de nivel de servicio acordados con cada cliente. Las características de la carga de trabajo soportada y los objetivos de nivel de servicio se definen, para cada servicio, en un Acuerdo de Nivel de Servicio, ANS, (también conocido como *Service Level Agreement*, SLA). Este proceso se encarga de monitorizar y de elaborar informes sobre los niveles de servicio logrados.

La tabla B.21 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Algunos de los aspectos indicados por los resultados de este proceso quedan parcialmente cubiertos por prácticas básicas del proceso OPE.2 Soporte al cliente. Por tanto, existe una relación parcial entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión del nivel de servicio de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
1. Se identifican los servicios y sus dependencias.	
2. Se definen en Acuerdos de Nivel de Servicio (ANS) los objetivos de nivel de servicio y las características de la carga de trabajo de los servicios.	
3. Se monitorizan los servicios según los Acuerdos de Nivel de Servicio (ANS).	**OPE.2.BP3: Monitorizar el renidmiento**. Monitorizar el rendimiento operacional del producto con el fin de ser conscientes de los problemas que puedan afectar al nivel de servicio.
4. Se comunica a las partes interesadas el rendimiento del nivel de servicio respecto a los objetivos de nivel de servicio.	**OPE.2.BP6: Comunicar la satisfacción del cliente**. Comunicar los datos de satisfacción del cliente en toda la organización proveedora de forma adecuada al personal involucrado y a la naturaleza de los hallazgos, y comunicar al cliente.
5. Se reflejan en los ANS los cambios en los requisitos del servicio.	

Tabla B.21. Relaciones entre los resultados del proceso de gestión del nivel de servicio y la norma ISO/IEC 15504-5

B.3.6. Relaciones con el proceso de generación de informes del servicio

El propósito del proceso de generación de informes del servicio es producir informes del servicio precisos para dar soporte a una comunicación eficaz y a la toma de decisiones. Estos informes deben satisfacer los requisitos de información del proveedor de servicios, de los clientes y del resto de partes interesadas.

La tabla B.22 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Todos los resultados de este proceso quedan cubiertos por prácticas básicas del proceso SUP.7 Documentación. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de generación de informes del servicio de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se identifican las necesidades de información de los servicios.	**SUP.7.BP4: Identificar los documentos a elaborar**. Identificar los documentos a elaborar para cualquier ciclo de vida.
2. Se definen los contenidos del informe del servicio en función de las necesidades de información de los servicios y los requisitos identificados.	**SUP.7.BP2: Establecer estándares para los documentos**. Establecer estándares para elaborar, modificar y mantener los documentos. **SUP.7.BP3: Especificar los requisitos de los documentos**. Especificar los requisitos de los documentos tales como formato, título, fecha, identificación, historial de versiones, autor/es, responsable de la revisión, responsable de la autorización, el resumen de contenidos, la finalidad y la lista de distribución.
3. Se producen los informes del servicio de acuerdo a los requisitos del informe del servicio.	**SUP.7.BP5: Elaborar los documentos**. Elaborar los documentos en los puntos del proceso en que se haya determinado de acuerdo con los estándares y la política establecidos.
4. Se comunican los informes del servicio a las partes interesadas.	**SUP.7.BP7: Distribuir los documentos**. Con el objetivo de hacer que los documentos estén disponibles, distribuirlos de acuerdo con los modos de distribución acordados, a través de los medios apropiados y a las audiencias especificadas, confirmando la entrega de los documentos cuando sea necesario.

Tabla B.22. Relaciones entre los resultados del proceso de generación de informes del servicio y la norma ISO/IEC 15504-5

B.4. Relaciones de los procesos de control

La tabla B.23 muestra todas las relaciones de los procesos de la categoría Procesos de control de la norma ISO/IEC 20000-4 con los procesos de la norma ISO/IEC 15504-5.

Procesos de control	**Grupos de Procesos de ISO/IEC 15504-5**								
	ACQ	SPL	ENG	OPE	MAN	PIM	RIN	REU	SUP
Gestión de cambios									SUP.10
Gestión de la configuración									SUP.8
Gestión de la entrega y del despliegue		SPL.2							

Tabla B.23. Relaciones entre los procesos de control de la norma ISO/IEC 20000-4 y los procesos de la norma ISO/IEC 15504-5

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los resultados obtenidos por los tres procesos de esta categoría de procesos de la norma ISO/IEC 20000-4.

B.4.1. Relaciones del proceso de gestión de cambios

El propósito del proceso de gestión de cambios es asegurar que todos los cambios son evaluados, aprobados, implementados y revisados de forma controlada. Este proceso planifica y controla los cambios en los servicios, sus aplicaciones e infraestructura para garantizar la puntualidad sin interrupciones innecesarias. Se solucionan los efectos no intencionados de los cambios.

La tabla B.24 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Todos los resultados de este proceso quedan cubiertos por prácticas básicas del proceso SUP.10 Gestión de las peticiones de cambios. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de cambios de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
1. Se registran y clasifican las peticiones de cambio.	**SUP.10.BP1: Desarrollar una estrategia para la gestión de cambios**. Establecer y llevar a cabo una estrategia para la gestión de cambios que asegure que los cambios se pueden describir, registrar, analizar y llevar a cabo. **SUP.10.BP2: Registrar las peticiones de cambio**. Identificar cada petición de cambio de manera única y registrarla.
2. Se evalúan las peticiones de cambio usando los criterios definidos.	**SUP.10.BP5: Evaluar el impacto del cambio**. Evaluar el impacto, los recursos, los riesgos y los beneficios potenciales de las peticiones de cambio y establecer criterios para su realización.
3. Se aprueban las peticiones de cambio antes de que los cambios se realicen y desplieguen.	**SUP.10.BP7: Aprobar los cambios**. Todos los cambios son aprobados antes de realizarse.
4. Se establece un programa de cambios y versiones y se comunica a las partes interesadas.	**SUP.10.BP8: Implementar los cambios**. Los cambios aprobados son implementados. NOTA: Los cambios planificados deben ser incorporados en entregas objetivo. Una entrega empaquetada debe incorporar cambios correctivos y adaptativos.
5. Se realizan y prueban los cambios aprobados.	**SUP.10.BP9: Revisar los cambios implementados**. Todos los cambios implementados deben ser revisados antes del cierre para asegurar que han tenido el efecto deseado y que satisfacen sus objetivos.

Resultados del proceso de gestión de cambios de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
6. Se revierten o remedian los cambios infructuosos.	

Tabla B.24. Relaciones entre los resultados del proceso de gestión de cambios y la norma ISO/IEC 15504-5

B.4.2. Relaciones con el proceso de gestión de la configuración

El propósito del proceso de gestión de la configuración es establecer y mantener la integridad de todos los componentes del servicio identificados.

La tabla B.25 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Todos los resultados de este proceso quedan cubiertos por prácticas básicas del proceso SUP.8 Gestión de la configuración. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de la configuración de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
1. Se identifican los elementos de la configuración que requieren ser gestionados.	**SUP.8.BP2: Identificar los elementos de la configuración**. Identificar los elementos de la configuración que necesitan ser identificados, almacenados, probados, revisados, utilizados, cambiados, entregados y/o mantenidos de manera independiente. NOTA: Para proporcionar un mecanismo eficiente para almacenar y acceder a las entidades requeridas, se puede establecer jerarquías y estructuras de ficheros y directorios.
2. Se registra y reporta el estado de los elementos de la configuración y las modificaciones.	**SUP.8.BP8: Notificar el estado de la configuración**. Notificar el estado de cada elemento de la configuración y su relación en la integración actual del sistema.
3. Se controlan los cambios a los elementos bajo gestión de la configuración.	**SUP.8.BP6: Controlar las modificaciones y las entregas**. Establecer un mecanismo para acceder, emitir y entregar los elementos.
4. Se asegura la integridad de los sistemas, servicios y componentes del servicio.	**SUP.8.BP10: Gestionar las copias de seguridad, el almacenaje, la gestión y la entrega de elementos configurados**. Asegurar la integridad y la consistencia de los elementos configurados a través de la planificación apropiada y de los recursos necesarios para copias de seguridad y almacenaje. Controlar la gestión y la entrega de elementos configurados.

Resultados del proceso de gestión de la configuración de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
5. Se controla la configuración de los elementos entregados.	

Tabla B.25. Relaciones entre los resultados del proceso de gestión de la configuración y la norma ISO/IEC 15504-5

B.4.3. Relaciones del proceso de gestión de la entrega y del despliegue

El propósito del proceso de gestión de la entrega y del despliegue es implementar entregas en el entorno real de un modo controlado. Este proceso es el responsable de planificar, programar y controlar el paso de las entregas a través del ciclo de vida del servicio. Asegura que la integridad del entorno real está protegido y que se liberan los componentes correctos.

La tabla B.26 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Algunos de los aspectos indicados por los resultados de este proceso quedan cubiertos por prácticas básicas del proceso SPL.2 Entrega del producto. Por tanto, existe una relación parcial entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de la entrega y del despliegue de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
1. Se establecen y acuerdan con las partes interesadas los requisitos de las entregas.	**SPL.2.BP10: Asegurar la aprobación de la entrega del producto antes de realizar la entrega**. Asegurar que se satisfacen los criterios de la entrega del producto antes de realizar las tareas propias de la entrega.
2. Se planifican las entregas de servicios y de componentes de servicios.	
3. Se diseñan las entregas.	**SPL.2.BP1: Definir los productos de la entrega**. Se definen los productos asociados con la entrega sobre las bases del acuerdo o la estrategia de desarrollo. NOTA: La entrega del producto software puede incluir herramientas de programación.
4. Se prueban las entregas antes de su liberación.	
5. Se despliegan las entregas aprobadas.	**SPL.2.BP11: Llevar a cabo la entrega al cliente**. Entregar el producto al cliente y recibir confirmación de la misma.

Resultados del proceso de gestión de la entrega y del despliegue de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
6. Se asegura la integridad del hardware, software y otros componentes del servicio durante el despliegue de la entrega.	
7. Se revierten o remedian las entregas desplegadas sin éxito.	
8. Se comunica la información de la entrega a las partes interesadas.	**SPL.2.BP6: Se comunica el tipo, el nivel y la duración del soporte para la entrega**. Identificar y comunicar el tipo, el nivel y la duración de la entrega.

Tabla B.26. Relaciones entre los resultados del proceso de gestión de la entrega y del despliegue y la norma ISO/IEC 15504-5

B.5. Relaciones de los procesos de resolución

La tabla B.27 muestra todas las relaciones de los procesos de la categoría Procesos de resolución de la norma ISO/IEC 20000-4 con los procesos de la norma ISO/IEC 15504-5.

Procesos de resolución	**Grupos de Procesos de ISO/IEC 15504-5**								
	ACQ	SPL	ENG	OPE	MAN	PIM	RIN	REU	SUP
Gestión de incidentes y cumplimiento de peticiones									SUP.9
Gestión de problemas					MAN.5				SUP.9

Tabla B.27. Relaciones entre los procesos de resolución de la norma ISO/IEC 20000-4 y los procesos de la norma ISO/IEC 15504-5

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los resultados obtenidos por los dos procesos de esta categoría de procesos de la norma ISO/IEC 20000-4.

B.5.1. Relaciones del proceso de gestión de incidentes y cumplimiento de peticiones

El propósito del proceso de gestión de incidentes y cumplimiento de peticiones es restaurar el servicio acordado y cumplir con las peticiones de servicio dentro de los niveles de servicio acordados. Este proceso se centra en la reducción de la duración y las consecuencias de la interrupción del servicio desde una perspectiva empresarial y de atención al cliente, y no en encontrar la causa raíz del incidente.

La tabla B.28 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Todos los resultados de este proceso quedan cubiertos por prácticas básicas del proceso SUP.9 Gestión de la resolución de problemas. Por tanto, existe una relación total entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de incidentes y cumplimiento de peticiones de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se registran y clasifican los incidentes y las peticiones de servicio.	**SUP.9.BP1: Desarrollar una estrategia para la resolución de problemas**. Determinar una estrategia para la resolución de problemas que asegure que los problemas son descritos, registrados, analizados y corregidos. **SUP.9.BP2: Identificar y registrar el problema**. Identificar y registrar cada problema de manera única.
2. Se priorizan y analizan los incidentes y las peticiones de servicio.	**SUP.9.BP3: Proporcionar soporte inicial y clasificar el problema**. Proporcionar soporte inicial, retroalimentar los problemas reportados y clasificarlos según su severidad. NOTA: La clasificación de los problemas se puede realizar en términos de criticidad, urgencia, relevancia, etc. **SUP.9.BP5: Evaluar el impacto del problema para determinar la solución**. Evaluar el impacto del problema para determinar las acciones apropiadas y acordar una solución.
3. Se resuelven y cierran los incidentes y las peticiones de servicio.	**SUP.9.BP6: Ejecutar acciones urgentes para la resolución del problema cuando sea necesario**. Si el problema requiere una resolución inmediata que depende de un cambio, obtener autorización para una solución inmediata. **SUP.9.BP8: Llevar a cabo la resolución del problema**. Poner en marcha las acciones para la resolución del problema y revisar la implantación de dichas acciones.
4. Se escalan los incidentes y las peticiones de servicio que no progresan según los niveles de servicio acordados.	

Resultados del proceso de gestión de incidentes y cumplimiento de peticiones de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
5. Se comunica a las partes interesadas la información sobre el estado y el progreso de los incidentes o de las peticiones de servicio reportados.	**SUP.9.BP7: Comunicar las notificaciones de alerta, cuando sea necesario**. Si el problema tiene una severidad importante e impacta a otros sistemas o usuarios, puede ser necesario enviar notificaciones de alerta mientras se espera reparar el problema. **SUP.9.BP10: Realizar el seguimiento del estado de los problemas**. Realizar el seguimiento del estado de los problemas identificados hasta su total resolución.

Tabla B.28. Relaciones entre los resultados del proceso de gestión de incidentes y cumplimiento de peticiones y la norma ISO/IEC 15504-5

B.5.2. Relaciones del proceso de gestión de problemas

El propósito del proceso de gestión de problemas es reducir al mínimo la interrupción del servicio. Este proceso investiga la causa raíz de los incidentes que tienen un impacto sobre los servicios y los niveles de servicio.

La tabla B.29 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. La mayoría de los aspectos indicados por los resultados de este proceso quedan cubiertos por prácticas básicas de los procesos SUP.9 Gestión de la resolución de problemas y MAN.5 Gestión de riesgos. Por tanto, existe una relación fuerte entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de problemas de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se identifican, registran y clasifican los problemas.	**MAN.5.BP2: Definir las estrategias de gestión de riesgos**. Definir estrategias y medidas de gestión de riesgos apropiadas para identificar, analizar, tratar y monitorizar cada riesgo o conjunto de riesgos, tanto a nivel de proyecto como a nivel de organización. **MAN.5.BP3: Identificar los riesgos**. Identificar los riesgos del proyecto, tanto inicialmente en la estrategia del proyecto, como cuando surjan durante el desarrollo del mismo. NOTA: Los riesgos podrían estar relacionados con las siguientes áreas: coste, planificación, esfuerzo, recursos y riesgos técnicos.

Resultados del proceso de gestión de problemas de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
2. Se priorizan y analizan los problemas.	**SUP.9.BP4: Investigar y diagnosticar la causa del problema**. Analizar los problemas para identificar la causa del problema. NOTA: Un problema puede ser un error conocido o puede impactar una aplicación en múltiples plataformas. **SUP.9.BP5: Evaluar el impacto del problema para determinar la solución**. Evaluar el impacto del problema para determinar las acciones apropiadas y acordar una solución. **MAN.5.BP4: Analizar los riesgos**. Analizar los riesgos y aplicar medidas de riesgos para determinar la prioridad con la que se aplicarán los recursos para monitorizar los riesgos. NOTA: Los aspectos a ser considerados en el análisis de riesgos pueden ser la probabilidad y el impacto de cada uno de los riesgos identificados.
3. Se resuelven y cierran los problemas.	**MAN.5.BP5: Definir y realizar acciones de tratamiento de riesgos**. Para cada riesgo (o conjunto de riesgos) definir y realizar las acciones apropiadas para reducir los riesgos a un nivel aceptable. **SUP.9.BP8: Llevar a cabo la resolución del problema**. Poner en marcha las acciones para la resolución del problema y revisar la implantación de dichas acciones.
4. Se escalan los problemas que no progresan según los niveles de servicio acordados.	**MAN.5.BP7: Llevar a cabo acciones preventivas o correctivas**. Cuando no se consiga mitigar el riesgo según lo previsto, llevar a cabo acciones preventivas para reducir o evitar el impacto cada riesgo. Cuando la mitigación del riesgo no pueda reducir o evitar el riesgo, planificar acciones correctoras para resolver el problema derivado del riesgo. NOTA: Las acciones preventivas pueden incluir el desarrollo y la implantación de nuevas estrategias de tratamiento o el reajuste de las estrategias existentes.
5. Se minimiza el efecto de los problemas no resueltos.	
6. Se comunica a las partes interesadas el estado y el progreso de la resolución de los problemas.	

Tabla B.29. Relaciones entre los resultados del proceso de gestión de problemas y la norma ISO/IEC 15504-5

B.6. Relaciones de los procesos de relaciones

La tabla B.30 muestra todas las relaciones de los procesos de la categoría Procesos de relaciones de la norma ISO/IEC 20000-4 con los procesos de la norma ISO/IEC 15504-5.

Procesos de relaciones	**Grupos de Procesos de ISO/IEC 15504-5**								
	ACQ	SPL	ENG	OPE	MAN	PIM	RIN	REU	SUP
Gestión de las relaciones con el negocio				OPE.2					
Gestión de suministradores	ACQ.2 ACQ.4								

Tabla B.30. Relaciones entre los procesos de resolución de la norma ISO/IEC 20000-4 y los procesos de la norma ISO/IEC 15504-5

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los resultados obtenidos por los dos procesos de esta categoría de procesos de la norma ISO/IEC 20000-4.

B.6.1. Relaciones del proceso de gestión de las relaciones con el negocio

El propósito del proceso de gestión de las relaciones con el negocio es identificar y gestionar las necesidades y expectativas de los clientes y partes interesadas. Este proceso permite a un proveedor de servicios construir una buena relación con sus clientes al entender el entorno empresarial en el que operan los servicios.

La tabla B.31 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. Algunos de los aspectos indicados por los resultados de este proceso quedan cubiertos por prácticas básicas del proceso OPE.2 Soporte al cliente. Por tanto, existe una relación parcial entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de las relaciones con el negocio de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se identifican los clientes y las partes interesadas.	
2. Se identifican y monitorizan las necesidades y las expectativas de los clientes.	

Resultados del proceso de gestión de las relaciones con el negocio de la norma ISO/IEC 20000-4	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
3. Se planifican y se implementan las comunicaciones con el cliente.	**OPE.2.BP1: Establecer un soporte del producto**. Establecer un servicio por el cual el cliente puede plantear problemas y preguntas surgidos por el uso del producto y recibir ayuda en la solución de ellos.
4. Se monitoriza el rendimiento del servicio.	**OPE.2.BP3: Monitorizar el rendimiento**. Supervisar el rendimiento operativo del producto con el fin de ser conscientes de los problemas que puedan afectar al nivel de servicio.
5. Se identifican los cambios en el alcance de los servicios, de los Acuerdos de Nivel de Servicio (ANS) y de los contratos.	
6. Se registran las quejas del servicio y se gestionan a través del ciclo de vida hasta el cierre.	
7. Se intensifican las quejas del servicio que no se resuelven a través de los canales normales.	
8. Se mide y analiza la satisfacción del cliente.	**OPE.2.BP5: Determinar la satisfacción del servicio del cliente**. Determinar el nivel de satisfacción del cliente con los servicios recibidos.
9. Se comunican a las partes interesadas los resultados del análisis de la satisfacción de los clientes.	**OPE.2.BP6: Comunicar la satisfacción del cliente**. Comunicar los datos de satisfacción del cliente en toda la organización proveedora, de una forma adecuada para el personal involucrado y la naturaleza de los hallazgos, y comunicarlos al cliente.

Tabla B.31. Relaciones entre los resultados del proceso de gestión de las relaciones con el negocio y la norma ISO/IEC 15504-5

B.6.2. Relaciones del proceso de gestión de suministradores

El propósito del proceso de gestión de gestión de sumnistradores es garantizar que los servicios de los suministradores se integran en los servicios de la organización para cumplir con los requisitos acordados. Este proceso garantiza que la organización proveedora de servicios puede administrar sus suministradores subcontratados para cumplir con sus obligaciones y los requisitos contractuales.

La tabla B.32 muestra los resultados de este proceso, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5. La mayoría de los aspectos indicados por los resultados de este proceso quedan cubiertos por prácticas básicas de los procesos ACQ.2 Selección del proveedor y ACQ.4 Monitorización del proveedor. Por tanto, existe una relación fuerte entre este proceso y la norma ISO/IEC 15504-5.

Resultados del proceso de gestión de suministradores de la norma ISO/IEC 20000-4	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
1. Se gestionan las relaciones entre el proveedor de servicios y los suministradores.	**ACQ.4.BP1: Establecer y mantener el enlace de comunicaciones**. Establecer y mantener el enlace de comunicaciones entre cliente y proveedor (es decir, definir las interfaces, calendario, agenda, mensajes, documentos, reuniones, revisiones conjuntas).
2. Se negocian con cada suministrador los servicios a ser provistos.	**ACQ.2.BP3: Preparar y negociar un acuerdo**. Negociar un acuerdo de proveedor que exprese claramente las expectativas de los clientes y las responsabilidades del proveedor y el cliente.
3. Se determinan los roles y las relaciones entre los suministradores.	
4. Se confirma la capacidad de los suministradores subcontratados para cumplir con sus obligaciones.	**ACQ.2.BP1: Evaluar la capacidad declarada o percibida del proveedor**. Evaluar la capacidad declarada o percibida del proveedor contra los requisitos indicados, de acuerdo con los criterios de selección de proveedores.
5. Se monitorizan las obligaciones del suministrador para satisfacer los requisitos del servicio.	**ACQ.4.BP4: Monitorizar la adquisición**. Monitorizar la adquisición según la documentación de adquisición acordada, analizando la información de las revisiones con el proveedor, para que el progreso pueda ser evaluado y así asegurar que las restricciones específicas tales como el coste, horario y calidad se cumplen.
6. Se monitoriza el rendimiento del suministrador contra los criterios acordados.	**ACQ.4.BP3: Revisar el rendimiento de los proveedores**. Examinar los aspectos de rendimiento del proveedor (técnicos, calidad, costes y plazos) de forma regular, según los requisitos acordados. **ACQ.4.BP2: Intercambiar información sobre el progreso técnico**. Utilizar el enlace de comunicaciones para intercambiar información sobre el avance técnico de la provisión, incluyendo los riesgos para la finalización con éxito.

Tabla B.32. Relaciones entre los resultados del proceso de gestión de suministradores y la norma ISO/IEC 15504-5

ANEXO C. Mapa de relaciones entre los controles de seguridad de la norma ISO/IEC 27002 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5

A partir de un análisis por filas a un nivel mucho más detallado de la tabla 4.1, los siguientes apartados muestran todas las relaciones detectadas entre los controles de cada una de las once cláusulas de la norma ISO/IEC 27002 y las prácticas básicas de la norma ISO/IEC 15504-5. En el caso de que el control en cuestión esté relacionado con todas las prácticas básicas del proceso, únicamente se indica el nombre del proceso.

C.1. Relaciones de la cláusula 5 Política de seguridad

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de la única categoría de esta cláusula de la norma ISO/IEC 27002.

C.1.1. Relaciones de la categoría 5.1 Política de seguridad de la información

El objetivo de la categoría 5.1 Política de seguridad de la información es proporcionar indicaciones para la gestión y soporte de la seguridad de la información de acuerdo con los requisitos empresariales y con la legislación y las normativas aplicables. La tabla C.1 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 5.1 Política de seguridad de la información de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
5.1.1 Documento de política de seguridad de la información. La Dirección debe aprobar un documento de política de seguridad de la información, publicarlo y distribuirlo a todos los empleados y terceros afectados.	**MAN.1.BP1: Desarrollar una visión estratégica**. Desarrollar una visión estratégica de la organización identificando sus objetivos de negocio y la relación de las funciones de ingeniería de sistemas y del software con las actividades básicas de la organización. **MAN.1.BP3: Definir una estrategia para el despliegue de procesos**. Definir una estrategia para el despliegue, implantación y mejora de procesos en la unidad organizativa. **MAN.1.BP4: Proporcionar compromiso de la dirección**. Proporcionar soporte de la dirección al despliegue, implantación y mejora de los procesos para permitir el logro de los objetivos de negocio. **MAN.1.BP5: Comunicar la visión y las metas**. Explicar la visión estratégica y las metas de la organización a todas las personas que trabajan para la organización, usando la gestión y los mecanismos de comunicación adecuados.
5.1.2 Revisión de la política de seguridad de la información. La política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	Proceso **MAN.1 Alineación de la organización**. Nivel de capacidad 2.

Tabla C.1. Relaciones entre los controles de la categoría 5.1 Política de seguridad de la información y la norma ISO/IEC 15504-5

C.2. Relaciones de la cláusula 6 Aspectos organizativos de la seguridad de la información

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de las dos categorías de esta cláusula de la norma ISO/IEC 27002.

C.2.1. Relaciones de la categoría 6.1 Organización interna

El objetivo de la categoría 6.1 Organización interna es gestionar la seguridad de la información dentro de la organización. La tabla C.2 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 6.1 Organización interna de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
6.1.1 Comité de gestión de seguridad de la información. La Dirección debe prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explícitas y el reconocimiento de las responsabilidades de seguridad de la información.	Proceso **MAN.2 Gestión de la organización**. Nivel de capacidad 2, GP 2.1.2: Planificar y monitorizar el rendimiento del proceso para cumplir con los objetivos identificados.
6.1.2 Coordinación de seguridad de la información. Las actividades relativas a la seguridad de la información deben ser coordinadas entre los representantes de las diferentes partes de la organización con sus correspondientes roles y funciones de trabajo.	**MAN.2.BP1: Identificar la infraestructura de gestión**. Nivel de capacidad 2, GP 2.1.5: Identificar y hacer que los recursos estén disponibles para llevar a cabo el proceso según el plan. **MAN.2.BP2: Proporcionar la infraestructura de gestión**. Nivel de capacidad 2, GP 2.1.5: Identificar y hacer que los recursos estén disponibles para llevar a cabo el proceso según el plan.
6.1.3 Asignación de responsabilidades relativas a la seguridad de la información. Deben definirse claramente todas las responsabilidades relativas a la seguridad de la información.	Proceso **MAN.2 Gestión de la organización**. Nivel de capacidad 2, GP 2.1.4: Definir responsabilidades y autoridades para realizar el proceso.
6.1.4 Proceso de autorización de recursos para el procesado de la información. Para cada nuevo recurso de procesado de la información, debe definirse e implantarse un proceso de autorización por parte de la Dirección.	**Todos los procesos**. Nivel de capacidad 2, GP 2.1.5: Identificar y hacer que los recursos estén disponibles para llevar a cabo el proceso según el plan.
6.1.5 Acuerdos de confidencialidad. Debe determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información.	**RIN.1.BP1: Identificar las habilidades y las competencias necesarias**. Identificar y evaluar las habilidades y competencias que necesita la organización para lograr sus objetivos.
6.1.6 Contacto con las autoridades. Deben mantenerse los contactos adecuados con las autoridades competentes.	**RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura.** Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.

Controles de la categoría 6.1 Organización interna de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
6.1.7 Contacto con grupos de especial interés. Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros, y asociaciones profesionales especializados en seguridad.	**RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura.** Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
6.1.8 Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.	**SUP.5.BP1: Desarrollar e implementar una estrategia de auditoría**. Se implementa una estrategia de auditoría que define el propósito, el alcance, los hitos, los criterios de auditoría y el equipo de auditoría. **SUP.5.BP2: Seleccionar auditores**. Se seleccionan auditores independientes, imparciales y objetivos. **SUP.5.BP3: Auditar la conformidad con los requisitos**. Se auditan los productos, servicios o procesos seleccionados para determinar su conformidad con sus requisitos y disposiciones previstos. Se registran las no conformidades.

Tabla C.2. Relaciones entre los controles de la categoría 6.1 Organización interna y la norma ISO/IEC 15504-5

C.2.2. Relaciones de la categoría 6.2 Terceros

El objetivo de la categoría 6.2 Terceros es mantener la seguridad de la información de la organización y de los dispositivos de procesado de la información que son objeto de acceso, tratamiento, comunicación o gestión por terceros. La tabla C.3 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 6.2 Terceros de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
6.2.1 Identificación de los riesgos derivados del acceso de terceros. Deben identificarse los riesgos para la información y para los dispositivos de procesado de la información de la organización derivados de los procesos de negocio que requieran de terceros, e implantar los controles apropiados antes de otorgar el acceso.	**ACQ.1.BP4: Desarrollar la estrategia de adquisiciones**. Desarrollar una estrategia para la adquisición del producto de acuerdo con las necesidades de adquisición. **ACQ.1.BP5: Definir los criterios de selección**. Establecer y acordar los criterios de selección de proveedores y los medios de evaluación a ser utilizados. **ACQ.2.BP1: Evaluar la capacidad declarada o percibida del proveedor**. Evaluar la capacidad declarada o percibida del proveedor contra los requisitos indicados, de acuerdo con los criterios de selección de proveedores. **ACQ.3.BP4: Revisar el contrato para las acciones de mitigación de riesgos**. Revisar y evaluar un mecanismo de para la mitigación de los riesgos identificados en las condiciones del contrato. **ACQ.4.BP4: Monitorizar la adquisición**. Monitorizar la adquisición según la documentación de adquisición acordada, analizando la información de las revisiones con el proveedor, para que el progreso pueda ser evaluado y así asegurar que las restricciones específicas tales como el coste, horario y calidad se cumplen. **MAN.5.BP1: Establecer el ámbito de la gestión de riesgos**. Determinar el ámbito de la gestión de riesgos a realizar. **MAN.5.BP3: Identificar los riesgos**. Identificar los riesgos del proyecto, tanto inicialmente durante la planificación del proyecto como a medida que se desarrollen durante la ejecución del proyecto.
6.2.2 Tratamiento de la seguridad en la relación con los clientes. Antes de otorgar acceso a los clientes a los activos o a la información de la organización, deben tratarse todos los requisitos de seguridad identificados.	**SPL.1.BP9: Negociar el contrato/acuerdo con el adquiriente**. Negociar todos los aspectos relevantes del contrato/acuerdo con el adquiriente.
6.2.3 Tratamiento de la seguridad en contratos con terceros. Los acuerdos con terceros que conlleven acceso, tratamiento, comunicación o gestión, bien de la información de la organización, o de los recursos de tratamiento de la información, o bien la incorporación de productos o servicios a los recursos de tratamiento de la información, deben cubrir todos los requisitos de seguridad pertinentes.	**ACQ.2.BP3: Preparar y negociar un acuerdo.** Negociar un acuerdo de proveedor que exprese claramente las expectativas de los clientes y las responsabilidades del proveedor y el cliente. **ACQ.3.BP1: Negociar el contrato/acuerdo**. Negociar todos los aspectos del contrato/acuerdo con el proveedor.

Tabla C.3. Relaciones entre los controles de la categoría 6.2 Terceros y la norma ISO/IEC 15504-5

C.3. Relaciones de la cláusula 7 Gestión de activos

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de las dos categorías de esta cláusula de la norma ISO/IEC 27002.

C.3.1. Relaciones de la categoría 7.1 Responsabilidad sobre los activos

El objetivo de la categoría 7.1 Responsabilidad sobre los activos es conseguir y mantener una protección adecuada de los activos de la organización. La tabla C.4 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 7.1 Responsabilidad sobre los activos de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
7.1.1 Inventario de activos. Todos los activos deben estar claramente identificados y debe elaborarse y mantenerse un inventario de todos los activos importantes.	
7.1.2 Propiedad de los activos. Toda la información y activos asociados con los recursos para el tratamiento de la información deben tener un propietario que forme parte de la organización y haya sido designado como propietario	**RIN.4.BP2: Definir los requisitos de infraestructura.** Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
7.1.3 Uso aceptable de los activos. Se deben identificar, documentar e implantar las reglas para el uso aceptable de la información y los activos asociados con los recursos para el procesado de la información.	**RIN.2.BP2: Identificar las necesidades de formación**. Identificar las necesidades de formación. Identificar y evaluar las habilidades y competencias que deben facilitarse o mejorarse a través de la formación. **RIN.2.BP3: Desarrollar o adquirir formación**. Desarrollar o adquirir formación que cubra las necesidades comunes de formación. **RIN.2.BP4: Preparar la ejecución de la formación**. Identificar y preparar la ejecución de las sesiones de formación, incluyendo la disponibilidad de los materiales de capacitación y la disponibilidad del personal a ser entrenado. **RIN.2.BP5: Formar al personal**. Capacitar al personal de los conocimientos y habilidades necesarias para desempeñar sus funciones. **RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los estándares, procedimientos, herramientas y técnicas que el proceso de infraestructura debería apoyar.

Tabla C.4. Relaciones entre los controles de la categoría 7.1 Responsabilidad sobre los activos y la norma ISO/IEC 15504-5

C.3.2. Relaciones de la categoría 7.2 Clasificación de la información

El objetivo de la categoría 7.2 Clasificación de la información es asegurar que la información recibe un nivel adecuado de protección. La tabla C.5 muestra los controles de seguridad de esta categoría. Estos controles no tienen relación con ninguna de las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 7.2 Clasificación de la información de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
7.2.1 Directrices de clasificación. La información debe ser clasificada según su valor, los requisitos legales, la sensibilidad y la criticidad para la organización.	
7.2.2 Etiquetado y manipulado de la información. Se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	

Tabla C.5. Relaciones entre los controles de la categoría 7.2 Clasificación de la información y la norma ISO/IEC 15504-5

C.4. Relaciones de la cláusula 8 Seguridad ligada a los recursos humanos

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de las tres categorías de esta cláusula de la norma ISO/IEC 27002.

C.4.1. Relaciones de la categoría 8.1 Antes del empleo

El objetivo de la categoría 8.1 Antes del empleo es asegurar que los empleados, los contratistas y los terceros entienden sus responsabilidades, y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos. La tabla C.6 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 8.1 Antes del empleo de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
8.1.1 Funciones y responsabilidades. Las funciones y responsabilidades de seguridad de los empleados, contratistas y terceros se deben definir y documentar de acuerdo con la política de seguridad de la información de la organización.	Proceso **MAN.1 Alineación de la organización**. Proceso **RIN.1 Gestión de recursos humanos**.
8.1.2 Investigación de antecedentes. La comprobación de los antecedentes de todos los candidatos al puesto de trabajo, de los contratistas o de los terceros, se debe llevar a cabo de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación y de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos considerados.	Proceso **RIN.1 Gestión de recursos humanos**.
8.1.3 Términos y condiciones de contratación. Como parte de sus obligaciones contractuales, los empleados, los contratistas y los terceros deben aceptar y firmar los términos y condiciones de su contrato de trabajo, que debe establecer sus responsabilidades y las de la organización en lo relativo a seguridad de la información.	Proceso **RIN.1 Gestión de recursos humanos**.

Tabla C.6. Relaciones entre los controles de la categoría 8.1 Antes del empleo y la norma ISO/IEC 15504-5

C.4.2. Relaciones de la categoría 8.2 Durante el empleo

El objetivo de la categoría 8.2 Durante el empleo es asegurar que todos los empleados, contratistas y terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización, en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano. La tabla C.7 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 8.2 Durante el empleo de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
8.2.1 Responsabilidades de la dirección. La Dirección debe exigir a los empleados, contratistas y terceros, que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización.	Proceso **MAN.1 Alineación de la organización**. **RIN.1.BP2: Definir los criterios de evaluación**. Definir unos criterios objetivos que se pueden utilizar para evaluar a los candidatos y evaluar el desempeño del personal.
8.2.2 Concienciación, formación y capacitación en seguridad de la información. Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deben recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.	**RIN.1.BP4: Desarrollar las habilidades y competencias del personal**. Definir y proporcionar oportunidades para el desarrollo de las habilidades y competencias del personal. Proceso **RIN.2 Formación**.
8.2.3 Proceso disciplinario. Debe existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad.	

Tabla C.7. Relaciones entre los controles de la categoría 8.2 Durante el empleo y la norma ISO/IEC 15504-5

C.4.3. Relaciones de la categoría 8.3 Cese del empleo o cambio de puesto de trabajo

El objetivo de la categoría 8.3 Cese del empleo o cambio de puesto de trabajo es asegurar que los empleados, contratistas y terceros abandonan la organización o cambian de puesto de trabajo de una manera ordenada. La tabla C.8 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 8.3 Cese del empleo o cambio de puesto de trabajo de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
8.3.1 Responsabilidad del cese o cambio. Las responsabilidades para proceder al cese en el empleo o al cambio de puesto de trabajo deben estar claramente definidas y asignadas.	
8.3.2 Devolución de activos. Todos los empleados, contratistas y terceros deben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	**RIN.4.BP2: Definir los requisitos de infraestructura.** Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.

Controles de la categoría 8.3 Cese del empleo o cambio de puesto de trabajo de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
8.3.3 Retirada de los derechos de acceso. Los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los empleados, contratistas y terceros deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o bien deben ser adaptados a los cambios producidos.	**RIN.4.BP2: Definir los requisitos de infraestructura.** Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.

Tabla C.8. Relaciones entre los controles de la categoría 8.3 Cese del empleo o cambio de puesto de trabajo y la norma ISO/IEC 15504-5

C.5. Relaciones de la cláusula 9 Seguridad física y ambiental

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de las dos categorías de esta cláusula de la norma ISO/IEC 27002.

C.5.1. Relaciones de la categoría 9.1 Áreas seguras

El objetivo de la categoría 9.1 Áreas seguras es prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la organización. La tabla C.9 muestra los controles de seguridad de esta categoría. Estos controles no tienen relación con ninguna de las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 9.1 Áreas seguras de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
9.1.1 Perímetro de seguridad física. Se deben utilizar perímetros de seguridad (barreras, muros, puertas de entrada con control a través de tarjeta, o puestos de control) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.	
9.1.2 Controles físicos de entrada. Las áreas seguras deben estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	
9.1.3 Seguridad de oficinas, despachos e instalaciones. Se deben diseñar y aplicar las medidas de seguridad física para las oficinas, despachos e instalaciones.	

Controles de la categoría 9.1 Áreas seguras de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
9.1.4 Protección contra las amenazas externas y de origen ambiental. Se debe diseñar y aplicar una protección física contra el daño causado por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre.	
9.1.5 Trabajo en áreas seguras. Se deben diseñar e implantar una protección física y una serie de directrices para trabajar en las áreas seguras.	
9.1.6 Áreas de acceso público y de carga y descarga. Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, a través de los que personal no autorizado puede acceder a las instalaciones, y si es posible, dichos puntos se deben aislar de los recursos de tratamiento de la información para evitar los accesos no autorizados.	

Tabla C.9. Relaciones entre los controles de la categoría 9.1 Áreas seguras y la norma ISO/IEC 15504-5

C.5.2. Relaciones de la categoría 9.2 Seguridad de los equipos

El objetivo de la categoría 9.2 Seguridad de los equipos es evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización. La tabla C.10 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 9.2 Seguridad de los equipos de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
9.2.1 Emplazamiento y protección de equipos. Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental así como las ocasiones de que se produzcan accesos no autorizados.	Proceso **RIN.4 Infraestructura**.
9.2.2 Instalaciones de suministro. Los equipos deben estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro.	Proceso **RIN.4 Infraestructura**.
9.2.3 Seguridad del cableado. El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debe estar protegido frente a interceptaciones o daños.	Proceso **RIN.4 Infraestructura**.

Controles de la categoría 9.2 Seguridad de los equipos de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
9.2.4 Mantenimiento de los equipos. Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad.	**RIN.4.BP6: Mantener la infraestructura**. Realizar el mantenimiento del proceso de infraestructura con el fin de corregir defectos y mejorar el rendimiento.
9.2.5 Seguridad de los equipos fuera de las instalaciones. Teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización, deben aplicarse medidas de seguridad a los equipos situados fuera dichas instalaciones.	**RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura.** Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
9.2.6 Reutilización o retirada segura de equipos. Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado o bien se han recargado de manera segura, antes de su retirada.	**RIN.4.BP2: Definir los requisitos de infraestructura.** Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
9.2.7 Retirada de materiales propiedad de la empresa. Los equipos, la información o el software no deben sacarse de las instalaciones, sin una autorización previa.	Proceso **RIN.4 Infraestructura**.

Tabla C.10. Relaciones entre los controles de la categoría 9.2 Seguridad de los equipos y la norma ISO/IEC 15504-5

C.6. Relaciones de la cláusula 10 Gestión de comunicaciones y operaciones

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de las diez categorías de esta cláusula de la norma ISO/IEC 27002.

C.6.1. Relaciones de la categoría 10.1 Responsabilidades y procedimientos de operación

El objetivo de la categoría 10.1 Responsabilidades y procedimientos de operación es asegurar el funcionamiento correcto y seguro de los recursos de procesamiento de la información. La tabla C.11 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 10.1 Responsabilidades y procedimientos de operación de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
10.1.1 Documentación de los procedimientos de operación. Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.	**SUP.7.BP1: Desarrollar una estrategia de gestión de la documentación**. Determinar la estrategia de gestión de la documentación que cubra todo lo que debería ser documentado en cada área de la organización, para cada fase del ciclo de vida del producto/servicio. **SUP.7.BP7: Distribuir los documentos**. Para proveer documentos, distribuir los documentos según los modos de distribución determinados, a través de los medios de comunicación apropiados para audiencias específicas, y confirmar la entrega de los documentos cuando sea necesario. **SUP.7.BP8: Mantener los documentos**. Mantener los documentos de acuerdo con la estrategia de documentación determinada.
10.1.2 Gestión de cambios. Deben controlarse los cambios en los recursos y los sistemas de tratamiento de la información.	Proceso **SUP.10 Gestión de las peticiones de cambio**.
10.1.3 Segregación de tareas. Las tareas y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.	**RIN.4.BP2: Definir los requisitos de infraestructura.** Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
10.1.4 Separación de los recursos de desarrollo, prueba y operación. Deben separarse los recursos de desarrollo, de pruebas y de operación, para reducir los riesgos de acceso no autorizado o los cambios en el sistema operativo.	Proceso **ENG.7 Integración del software**. Proceso **ENG.8 Pruebas del software**. Proceso **ENG.9 Integración del sistema**. Proceso **ENG.10 Pruebas del sistema**.

Tabla C.11. Relaciones entre los controles de la categoría 10.1 Responsabilidades y procedimientos de operación y la norma ISO/IEC 15504-5

C.6.2. Relaciones de la categoría 10.2 Gestión de la provisión de servicios por terceros

El objetivo de la categoría 10.2 Gestión de la provisión de servicios por terceros es implantar y mantener el nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros. La tabla C.12 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 10.2 Gestión de la provisión de servicios por terceros de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
10.2.1 Provisión de servicios. Se debe comprobar que los controles de seguridad, las definiciones de los servicios y los niveles de provisión, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero.	**ACQ.3.BP1: Negociar el contrato/acuerdo**. Negociar todos los aspectos del contrato/acuerdo con el proveedor. **ACQ.3.BP3: Revisar el contrato para la monitorización de la capacidad del proveedor**. Revisar y considerar un mecanismo para monitorizar la capacidad y el rendimiento del proveedor en las condiciones del contrato.
10.2.2 Supervisión y revisión de los servicios prestados por terceros. Los servicios, informes y registros proporcionados por un tercero deben ser objeto de supervisión y revisión periódicas, y también deben llevarse a cabo auditorias periódicas.	**ACQ.4.BP3: Revisar el rendimiento de los proveedores**. Examinar los aspectos de rendimiento del proveedor (técnicos, calidad, costes y plazos) de forma regular, según los requisitos acordados. **ACQ.4.BP4: Monitorizar la adquisición**. Monitorizar la adquisición según la documentación de adquisición acordada, analizando la información de las revisiones con el proveedor, para que el progreso pueda ser evaluado y así asegurar que las restricciones específicas tales como el coste, horario y calidad se cumplen.
10.2.3 Gestión de cambios en los servicios prestados por terceros. Se deben gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos.	**ACQ.4.BP5: Acordar los cambios**. Se negocian los cambios propuestos por cualquiera de las partes y se documentan los resultados en el acuerdo. Proceso **SUP.10 Gestión de las peticiones de cambio**.

Tabla C.12. Relaciones entre los controles de la categoría 10.2 Gestión de la provisión de servicios por terceros y la norma ISO/IEC 15504-5

C.6.3. Relaciones de la categoría 10.3 Planificación y aceptación del sistema

El objetivo de la categoría 10.3 Planificación y aceptación del sistema es minimizar el riesgo de fallos de los sistemas. La tabla C.13 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 10.3 Planificación y aceptación del sistema de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
10.3.1 Gestión de capacidades. La utilización de los recursos se debe supervisar y ajustar así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el comportamiento requerido del sistema.	
10.3.2 Aceptación del sistema. Se deben establecer los criterios para la aceptación de nuevos sistemas de información, de las actualizaciones y de nuevas versiones de los mismos, y se deben llevar a cabo pruebas adecuadas de los sistemas durante el desarrollo y previamente a la aceptación.	**ACQ.5.BP3: Aceptar el producto**. Aceptar el producto o servicio entregado y comunicar la aceptación al proveedor.

Tabla C.13. Relaciones entre los controles de la categoría 10.3 Planificación y aceptación del sistema y la norma ISO/IEC 15504-5

C.6.4. Relaciones de la categoría 10.4 Protección contra código malicioso y descargable

El objetivo de la categoría 10.4 Protección contra código malicioso y descargable es proteger la integridad del software y de la información. La tabla C.14 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 10.4 Protección contra código malicioso y descargable de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
10.4.1 Controles contra el código malicioso. Se deben implantar los controles de detección, prevención y recuperación que sirvan como protección contra código malicioso y se deben implantar procedimientos adecuados de concienciación del usuario.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
10.4.2 Controles contra el código descargado en el cliente. Cuando se autorice el uso de código descargado en el cliente, (JavaScript, VBScript, applets de Java applets, controles ActiveX, etc..), la configuración debe garantizar que dicho código autorizado funciona de acuerdo con una política de seguridad claramente definida, y se debe evitar que se ejecute el código no autorizado.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.

Tabla C.14. Relaciones entre los controles de la categoría 10.4 Protección contra código malicioso y descargable y la norma ISO/IEC 15504-5

C.6.5. Relaciones de la categoría 10.5 Copias de seguridad

El objetivo de la categoría 10.5 Copias de seguridad es Mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información. La tabla C.15 muestra el único control de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 10.5 Copias de seguridad de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
10.5.1 Copias de seguridad de la información. Se deben realizar copias de seguridad de la información y del software, y se deben probar periódicamente con conforme a la política de copias de seguridad acordada.	**SUP.8.BP10: Gestionar las copias de seguridad, el almacenaje, la gestión y la entrega de elementos configurados**. Asegurar la integridad y la consistencia de los elementos configurados a través de la planificación apropiada y de los recursos necesarios para copias de seguridad y almacenaje. Controlar la gestión y la entrega de elementos configurados. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.

Tabla C.15. Relaciones entre los controles de la categoría 10.5 Copias de seguridad y la norma ISO/IEC 15504-5

C.6.6. Relaciones de la categoría 10.6 Gestión de la seguridad de las redes

El objetivo de la categoría 10.6 Gestión de la seguridad de las redes es asegurar la protección de la información en las redes y la protección de la infraestructura de soporte. La tabla C.16 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 10.6 Gestión de la seguridad de las redes de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
10.6.1 Controles de red. Las redes deben estar adecuadamente gestionadas y controladas, para que estén protegidas frente a posibles amenazas y para mantener la seguridad de los sistemas y de las aplicaciones que utilizan estas redes, incluyendo la información en tránsito.	**RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización. **RIN.4.BP6: Mantener la infraestructura**. Realizar el mantenimiento del proceso de infraestructura con el fin de corregir defectos y mejorar el rendimiento.

Controles de la categoría 10.6 Gestión de la seguridad de las redes de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
10.6.2 Seguridad de los servicios de red. Se deben identificar las características de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en todo acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	**ACQ.3.BP1: Negociar el contrato/acuerdo**. Negociar todos los aspectos del contrato/acuerdo con el proveedor.

Tabla C.16. Relaciones entre los controles de la categoría 10.6 Gestión de la seguridad de las redes y la norma ISO/IEC 15504-5

C.6.7. Relaciones de la categoría 10.7 Manipulación de los soportes

El objetivo de la categoría 10.7 Manipulación de los soportes es evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización. La tabla C.17 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 10.7 Manipulación de los soportes de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
10.7.1 Gestión de soportes extraíbles. Se deben establecer procedimientos para la gestión de los soportes extraíbles.	**RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
10.7.2 Retirada de soportes. Los soportes deben ser retirados de forma segura cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos.	

Controles de la categoría 10.7 Manipulación de los soportes de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
10.7.3 Procedimientos de manipulación de la información. Deben establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **SUP.8.BP10: Gestionar las copias de seguridad, el almacenaje, la gestión y la entrega de elementos configurados**. Asegurar la integridad y la consistencia de los elementos configurados a través de la planificación apropiada y de los recursos necesarios para copias de seguridad y almacenaje. Controlar la gestión y la entrega de elementos configurados.
10.7.4 Seguridad de la documentación del sistema. La documentación del sistema debe estar protegida contra accesos no autorizados.	**SUP.7.BP1: Desarrollar una estrategia de gestión de la documentación**. Determinar la estrategia de gestión de la documentación que cubra todo lo que debería ser documentado en cada área de la organización, para cada fase del ciclo de vida del producto/servicio. **SUP.7.BP3: Especificar los requisitos de los documentos**. Especificar los requisitos de los documentos tales como formato, título, fecha, identificación, historial de versiones, autor/es, responsable de la revisión, responsable de la autorización, el resumen de contenidos, la finalidad y la lista de distribución. **SUP.7.BP6: Revisar los documentos**. Revisar los documentos antes de su distribución, y autorizar los documentos antes de su distribución o difusión. **SUP.7.BP7: Distribuir los documentos**. Para proveer documentos, distribuir los documentos según los modos de distribución determinados, a través de los medios de comunicación apropiados para audiencias específicas, y confirmar la entrega de los documentos cuando sea necesario. **SUP.7.BP8: Mantener los documentos**. Mantener los documentos de acuerdo con la estrategia de documentación determinada. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.

Tabla C.17. Relaciones entre los controles de la categoría 10.7 Manipulación de los soportes y la norma ISO/IEC 15504-5

C.6.8. Relaciones de la categoría 10.8 Intercambio de información

El objetivo de la categoría 10.8 Intercambio de información es mantener la seguridad de la información y del software intercambiados dentro de una organización y con un tercero. La tabla C.18 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 10.8 Intercambio de información de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
10.8.1 Políticas y procedimientos de intercambio de información. Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	**RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización.
10.8.2 Acuerdos de intercambio. Deben establecerse acuerdos para el intercambio de información y del software entre la organización y los terceros.	**ACQ.3.BP1: Negociar el contrato/acuerdo**. Negociar todos los aspectos del contrato/acuerdo con el proveedor. **ACQ.3.BP2: Aprobar el contrato**. El contrato es aprobado por las partes interesadas. **SPL.1.BP9: Negociar el contrato/acuerdo con el adquiriente**. Negociar todos los aspectos relevantes del contrato/acuerdo con el adquiriente. **SPL.1.BP10: Establecer la confirmación del contrato/acuerdo**. Confirmar formalmente el contrato/acuerdo para proteger los intereses de ambas partes. **RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
10.8.3 Soportes físicos en tránsito. Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	**SPL.2.BP8: Identificar el embalaje de los elementos liberados**. Se identifica el embalaje de los diferentes tipos de medios. NOTA: El embalaje de ciertos tipos de medios puede necesitar protección física o electrónica o técnicas específicas de cifrado.

Controles de la categoría 10.8 Intercambio de información de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
10.8.4 Mensajería electrónica. La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
10.8.5 Sistemas de información empresariales. Deben formularse e implantarse políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información empresariales.	**RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización.

Tabla C.18. Relaciones entre los controles de la categoría 10.8 Intercambio de información y la norma ISO/IEC 15504-5

C.6.9. Relaciones de la categoría 10.9 Servicios de comercio electrónico

El objetivo de la categoría 10.9 Servicios de comercio electrónico es garantizar la seguridad de los servicios de comercio electrónico, y el uso seguro de los mismos. La tabla C.19 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 10.9 Servicios de comercio electrónico de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
10.9.1 Comercio electrónico. La información incluida en el comercio electrónico que se transmita a través de redes públicas debe protegerse contra las actividades fraudulentas, las disputas contractuales, y la revelación o modificación no autorizada de dicha información.	Proceso **ENG.1 Captura de requisitos**. Proceso **ENG.2 Análisis de requisitos de sistema**. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
10.9.2 Transacciones en línea. La información contenida en las transacciones en línea debe estar protegida para evitar transmisiones incompletas, errores de direccionamiento, alteraciones no autorizadas de los mensajes, la revelación, la duplicación o la reproducción no autorizadas del mensaje.	Proceso **ENG.1 Captura de requisitos**. Proceso **ENG.2 Análisis de requisitos de sistema**. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.

Controles de la categoría 10.9 Servicios de comercio electrónico de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
10.9.3 Información puesta a disposición pública. La integridad de la información puesta a disposición pública se debe proteger para evitar modificaciones no autorizadas.	Proceso **ENG.1 Captura de requisitos**. Proceso **ENG.2 Análisis de requisitos de sistema**. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.

Tabla C.19. Relaciones entre los controles de la categoría 10.9 Servicios de comercio electrónico y la norma ISO/IEC 15504-5

C.6.10. Relaciones de la categoría 10.10 Supervisión

El objetivo de la categoría 10.10 Supervisión es detectar las actividades de procesamiento de la información no autorizadas. La tabla C.20 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 10.10 Supervisión de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
10.10.1 Registro de auditorías. Se deben realizar registros de auditoria de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deben mantener estos registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización.
10.10.2 Supervisión del uso del sistema. Se deben establecer procedimientos para supervisar el uso de los recursos de procesamiento de la información y se deben revisar periódicamente los resultados de las actividades de supervisión.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización. **RIN.4.BP6: Mantener la infraestructura**. Realizar el mantenimiento del proceso de infraestructura con el fin de corregir defectos y mejorar el rendimiento.
10.10.3 Protección de la información de los registros. Los dispositivos de registro y la información de los registros deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	

Controles de la categoría 10.10 Supervisión de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
10.10.4 Registros de administración y operación. Se deben registrar las actividades del administrador del sistema y de la operación del sistema.	
10.10.5 Registro de fallos. Los fallos deben ser registrados y analizados y se deben tomar las correspondientes acciones	
10.10.6 Sincronización del reloj. Los relojes de todos los sistemas de procesamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una precisión de tiempo acordada.	

Tabla C.20. Relaciones entre los controles de la categoría 10.10 Supervisión y la norma ISO/IEC 15504-5

C.7. Relaciones de la cláusula 11 Control de acceso

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de las siete categorías de esta cláusula de la norma ISO/IEC 27002.

C.7.1. Relaciones de la categoría 11.1 Requisitos de negocio para el control de acceso

El objetivo de la categoría 11.1 Requisitos de negocio para el control de acceso es controlar el acceso a la información. La tabla C.21 muestra el único control de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 11.1 Requisitos de negocio para el control de acceso de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
11.1.1 Política de control de acceso. Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos empresariales y de seguridad para el acceso.	**RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización. **RIN.4.BP6: Mantener la infraestructura**. Realizar el mantenimiento del proceso de infraestructura con el fin de corregir defectos y mejorar el rendimiento.

Tabla C.21. Relaciones entre los controles de la categoría 11.1 Requisitos de negocio para el control de acceso y la norma ISO/IEC 15504-5

C.7.2. Relaciones de la categoría 11.2 Gestión de acceso de usuario

El objetivo de la categoría 11.2 Gestión de acceso de usuario es asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas de información. La tabla C.22 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 11.2 Gestión de acceso de usuario de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
11.2.1 Registro de usuario. Debe establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.	**RIN.1.BP10: Mantener registros de personal**. Mantener registros adecuados de personal, incluyendo no sólo detalles personales, sino también información sobre capacidades, formación recibida y evaluaciones de rendimiento.
11.2.2 Gestión de privilegios. La asignación y el uso de privilegios deben estar restringidos y controlados.	**RIN.1.BP10: Mantener registros de personal**. Mantener registros adecuados de personal, incluyendo no sólo detalles personales, sino también información sobre capacidades, formación recibida y evaluaciones de rendimiento.

Controles de la categoría 11.2 Gestión de acceso de usuario de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
11.2.3 Gestión de contraseñas de usuario. La asignación de contraseñas debe ser controlada a través de un proceso de gestión formal.	**RIN.1.BP10: Mantener registros de personal**. Mantener registros adecuados de personal, incluyendo no sólo detalles personales, sino también información sobre capacidades, formación recibida y evaluaciones de rendimiento.
11.2.4 Revisión de derechos de acceso de usuario. La Dirección debe revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.	**RIN.1.BP10: Mantener registros de personal**. Mantener registros adecuados de personal, incluyendo no sólo detalles personales, sino también información sobre capacidades, formación recibida y evaluaciones de rendimiento.

Tabla C.22. Relaciones entre los controles de la categoría 11.2 Gestión de acceso de usuario y la norma ISO/IEC 15504-5

C.7.3. Relaciones de la categoría 11.3 Responsabilidades de usuario

El objetivo de la categoría 11.3 Responsabilidades de usuario es prevenir el acceso de usuarios no autorizados, así como evitar el que se comprometa o se produzca el robo de la información o de los recursos de procesamiento de la información. La tabla C.23 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 11.3 Responsabilidades de usuario de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
11.3.1 Uso de contraseña. Se debe requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y el uso de las contraseñas.	**RIN.2.BP5: Formar al personal**. Capacitar al personal de los conocimientos y habilidades necesarias para desempeñar sus funciones.
11.3.2 Equipo de usuario desatendido. Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.	**RIN.2.BP5: Formar al personal**. Capacitar al personal de los conocimientos y habilidades necesarias para desempeñar sus funciones.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia. Debe adoptarse una política de puesto de trabajo despejado de papeles y de soportes de almacenamiento extraíbles junto con una política de pantalla limpia para los recursos de procesamiento de la información.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.

Tabla C.23. Relaciones entre los controles de la categoría 11.3 Responsabilidades de usuario y la norma ISO/IEC 15504-5

C.7.4. Relaciones de la categoría 11.4 Control de acceso a la red

El objetivo de la categoría 11.4 Control de acceso a la red es prevenir el acceso no autorizado a los servicios en red. La tabla C.24 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 11.4 Control de acceso a la red de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
11.4.1 Política de uso de los servicios en red. Se debe proporcionar a los usuarios únicamente el acceso a los servicios para que los que hayan sido específicamente autorizados.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
11.4.2 Autenticación de usuario para conexiones externas. Se deben utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
11.4.3 Identificación de los equipos en las redes. La identificación automática de los equipos se debe considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
11.4.4 Diagnóstico remoto y protección de los puertos de configuración. Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
11.4.5 Segregación de las redes. Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en redes.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
11.4.6 Control de la conexión a la red. En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debe restringirse la capacidad de los usuarios para conectarse a la red, esto debe hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones del negocio.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.
11.4.7 Control de encaminamiento (*routing*) de red. Se deben implantar controles de encaminamiento (*routing*) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones empresariales.	**RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados.

Tabla C.24. Relaciones entre los controles de la categoría 11.4 Control de acceso a la red y la norma ISO/IEC 15504-5

C.7.5. Relaciones de la categoría 11.5 Control de acceso al sistema operativo

El objetivo de la categoría 11.5 Control de acceso al sistema operativo es prevenir el acceso no autorizado a los sistemas operativos. La tabla C.25 muestra los controles de seguridad de esta categoría. Estos controles no tienen relación con ninguna de las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 11.5 Control de acceso al sistema operativo de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
11.5.1 Procedimientos seguros de inicio de sesión. El acceso a los sistemas operativos se debe controlar por medio de un procedimiento seguro de inicio de sesión.	
11.5.2 Identificación y autenticación de usuario. Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal y exclusivo, y se debe elegir una técnica adecuada de autenticación para confirmar la identidad solicitada del usuario.	
11.5.3 Sistema de gestión de contraseñas. Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.	
11.5.4 Uso de los recursos del sistema. Se debe restringir y controlar rigurosamente el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	
11.5.5 Desconexión automática de sesión. Las sesiones inactivas deben cerrarse después de un periodo de inactividad definido.	
11.5.6 Limitación del tiempo de conexión. Para proporcionar seguridad adicional a las aplicaciones de alto riesgo, se deben utilizar restricciones en los tiempos de conexión.	

Tabla C.25. Relaciones entre los controles de la categoría 11.5 Control de acceso al sistema operativo y la norma ISO/IEC 15504-5

C.7.6. Relaciones de la categoría 11.6 Control de acceso a las aplicaciones y la información

El objetivo de la categoría 11.6 Control de acceso a las aplicaciones y la información es prevenir el acceso no autorizado a la información que contienen las aplicaciones. La tabla C.26 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 11.6 Control de acceso a las aplicaciones y la información de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
11.6.1 Restricción del acceso a la información. Se debe restringir el acceso a la información y a las aplicaciones a los usuarios y al personal de soporte, de acuerdo con la política de control de acceso definida.	**RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización.
11.6.2 Aislamiento de sistemas sensibles. Los sistemas sensibles deben tener un entorno de ordenadores dedicados (aislados).	

Tabla C.26. Relaciones entre los controles de la categoría 11.6 Control de acceso a las aplicaciones y la información y la norma ISO/IEC 15504-5

C.7.7. Relaciones de la categoría 11.7 Ordenadores portátiles y teletrabajo

El objetivo de la categoría 11.7 Ordenadores portátiles y teletrabajo es garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y servicios de teletrabajo. La tabla C.27 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 11.7 Ordenadores portátiles y teletrabajo de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
11.7.1 Ordenadores portátiles y comunicaciones móviles. Se debe implantar una política formal y se deben adoptar las medidas de seguridad adecuadas de protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles.	**RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización.
11.7.2 Teletrabajo. Se debe redactar e implantar, una política de actividades de teletrabajo, así como los planes y procedimientos de operación correspondientes.	**RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización.

Tabla C.27. Relaciones entre los controles de la categoría 11.7 Ordenadores portátiles y teletrabajo y la información y la norma ISO/IEC 15504-5

C.8. Relaciones de la cláusula 12 Adquisición, desarrollo y mantenimiento de los sistemas de información

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de las seis categorías de esta cláusula de la norma ISO/IEC 27002.

C.8.1. Relaciones de la categoría 12.1 Requisitos de seguridad de los sistemas de información

El objetivo de la categoría 12.1 Requisitos de seguridad de los sistemas de información es garantizar que la seguridad está integrada en los sistemas de información. La tabla C.28 muestra el único control de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 12.1 Requisitos de seguridad de los sistemas de información de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
12.1.1 Análisis y especificación de los requisitos de seguridad. En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deben especificar los requisitos de los controles de seguridad.	Proceso **ENG.1 Captura de requisitos**. Proceso **ENG.2 Análisis de requisitos del sistema**. Proceso **ENG.3 Diseño de la arquitectura del sistema**. Proceso **ENG.4 Análisis de requisitos del software**.

Tabla C.28. Relaciones entre los controles de la categoría 12.1 Requisitos de seguridad de los sistemas de información y la norma ISO/IEC 15504-5

C.8.2. Relaciones de la categoría 12.2 Tratamiento correcto de las aplicaciones

El objetivo de la categoría 12.2 Tratamiento correcto de las aplicaciones es evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones. La tabla C.29 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 12.2 Tratamiento correcto de las aplicaciones de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
12.2.1 Validación de los datos de entrada. La introducción de datos en las aplicaciones debe validarse para garantizar que dichos datos son correctos y adecuados.	**ENG.4.BP3: Desarrollar criterios para las pruebas de software**. Utilizar los requisitos del software para definir los criterios de aceptación para las pruebas de los productos software. Las pruebas de producto software deben demostrar la conformidad con los requisitos del software.
12.2.2 Control del procesamiento interno. Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deben incorporar comprobaciones de validación en las aplicaciones.	Proceso **ENG.2 Análisis de requisitos del sistema**. Proceso **ENG.4 Análisis de requisitos del software**.
12.2.3 Integridad de los mensajes. Se deben identificar los requisitos para garantizar la autenticidad y para proteger la integridad de los mensajes en las aplicaciones y se deben identificar e implantar los controles adecuados.	Proceso **ENG.2 Análisis de requisitos del sistema**. Proceso **ENG.4 Análisis de requisitos del software**.

Controles de la categoría 12.2 Tratamiento correcto de las aplicaciones de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
12.2.4 Validación de los datos de salida. Los datos de salida de una aplicación se deben validar para garantizar que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias	Proceso **ENG.4 Análisis de requisitos del software**.

Tabla C.29. Relaciones entre los controles de la categoría 12.2 Tratamiento correcto de las aplicaciones y la norma ISO/IEC 15504-5

C.8.3. Relaciones de la categoría 12.3 Controles criptográficos

El objetivo de la categoría 12.3 Controles criptográficos es proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos. La tabla C.30 muestra los controles de seguridad de esta categoría. Estos controles no tienen relación con ninguna de las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 12.3 Controles criptográficos de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
12.3.1 Política de uso de los controles criptográficos. Se debe formular e implantar una política para el uso de los controles criptográficos para proteger la información.	
12.3.2 Gestión de claves. Debe implantarse un sistema de gestión de claves para dar soporte al uso de técnicas criptográficas por parte de la organización.	

Tabla C.30. Relaciones entre los controles de la categoría 12.3 Controles criptográficos y la norma ISO/IEC 15504-5

C.8.4. Relaciones de la categoría 12.4 Seguridad de los archivos de sistema

El objetivo de la categoría 12.4 Seguridad de los archivos de sistema es garantizar la seguridad de los archivos de sistema. La tabla C.31 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 12.4 Seguridad de los archivos de sistema de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
12.4.1 Control de software en explotación. Deben estar implantados procedimientos para controlar la instalación de software en los sistemas operativos.	Proceso **ENG.11 Instalación del software**.
12.4.2 Protección de los datos de prueba del sistema. Los datos de prueba se deben seleccionar con cuidado y deben estar protegidos y controlados.	**ENG.4.BP3: Desarrollar criterios para las pruebas de software**. Utilizar los requisitos del software para definir los criterios de aceptación para las pruebas de los productos software. Las pruebas de producto software deben demostrar la conformidad con los requisitos del software.
12.4.3 Control de acceso al código fuente de los programas. Se debe restringir el acceso al código fuente de los programas.	Proceso **SUP.8 Gestión de la configuración**.

Tabla C.31. Relaciones entre los controles de la categoría 12.4 Seguridad de los archivos de sistema y la norma ISO/IEC 15504-5

C.8.5. Relaciones de la categoría 12.5 Seguridad en los procesos de desarrollo y soporte

El objetivo de la categoría 12.5 Seguridad en los procesos de desarrollo y soporte es mantener la seguridad del software y de la información de las aplicaciones. La tabla C.32 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 12.5 Seguridad en los procesos de desarrollo y soporte de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
12.5.1 Procedimientos de control de cambios. La implantación de cambios debe controlarse mediante el uso de procedimientos formales de control de cambios.	Proceso **SUP.8 Gestión de la configuración**. Proceso **SUP.10 Gestión de las peticiones de cambio**.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. Cuando se modifiquen los sistemas operativos, las aplicaciones empresariales críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o en la seguridad de la organización.	Proceso **ENG.7 Integración del software**.

Controles de la categoría 12.5 Seguridad en los procesos de desarrollo y soporte de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
12.5.3 Restricciones a los cambios en los paquetes de software. Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	Proceso **SUP.10 Gestión de las peticiones de cambio**.
12.5.4 Fugas de información. Deben evitarse las situaciones que permitan que se produzcan fugas de información.	Proceso **ENG.1 Captura de requisitos** **RIN.3.BP4: Capturar conocimiento**. Identificar y registrar cada elemento de conocimiento de acuerdo con el esquema de clasificación y los criterios de los activos.
12.5.5 Externalización del desarrollo de software. La externalización del desarrollo de software debe ser supervisada y controlada por la organización.	Proceso **ACQ.1 Preparación de la adquisición**. Proceso **ACQ.2 Selección del proveedor**. Proceso **ACQ.3 Acuerdo contractual**. Proceso **ACQ.4 Monitorización del proveedor**. Proceso **ACQ.5 Aceptación del cliente**.

Tabla C.32. Relaciones entre los controles de la categoría 12.5 Seguridad en los procesos de desarrollo y soporte y la norma ISO/IEC 15504-5

C.8.6. Relaciones de la categoría 12.6 Gestión de la vulnerabilidad técnica

El objetivo de la categoría 12.6 Gestión de la vulnerabilidad técnica es reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas. La tabla C.33 muestra el único control de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 12.6 Gestión de la vulnerabilidad técnica de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
12.6.1 Control de las vulnerabilidades técnicas. Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	Proceso **MAN.5 Gestión de riesgos**.

Tabla C.33. Relaciones entre los controles de la categoría 12.6 Gestión de la vulnerabilidad técnica y la norma ISO/IEC 15504-5

C.9. Relaciones de la cláusula 13 Gestión de incidentes de seguridad de la información

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de las dos categorías de esta cláusula de la norma ISO/IEC 27002.

C.9.1. Relaciones de la categoría 13.1 Notificación de eventos y puntos débiles de la seguridad de la información

El objetivo de la categoría 13.1 Notificación de eventos y puntos débiles de la seguridad de la información es asegurarse de que los eventos y las vulnerabilidades de la seguridad de la información, asociados con los sistemas de información, se comunican de manera que sea posible emprender las acciones correctivas oportunas. La tabla C.34 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 13.1 Notificación de eventos y puntos débiles de la seguridad de la información de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
13.1.1 Notificación de los eventos de seguridad de la información. Los eventos de seguridad de la información se deben notificar a través de los canales adecuados de gestión lo antes posible.	Proceso **SUP.9 Gestión de la resolución de problemas**. Proceso **MAN.5 Gestión de riesgos**.
13.1.2 Notificación de los puntos débiles de la seguridad. Todos los empleados, contratistas, y terceros que sean usuarios de los sistemas y servicios de información deben estar obligados a anotar y notificar cualquier punto débil que observen o que sospechen exista, en dichos sistemas o servicios.	Proceso **SUP.9 Gestión de la resolución de problemas**. Proceso **MAN.5 Gestión de riesgos**.

Tabla C.34. Relaciones entre los controles de la categoría 13.1 Notificación de eventos y puntos débiles de la seguridad de la información y la norma ISO/IEC 15504-5

C.9.2. Relaciones de la categoría 13.2 Gestión de incidentes de seguridad de la información y mejoras

El objetivo de la categoría 13.2 Gestión de incidentes de seguridad de la información y mejoras es garantizar que se aplica un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información. La tabla C.35 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 13.2 Gestión de incidentes de seguridad de la información y mejoras de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
13.2.1 Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	Proceso **SUP.9 Gestión de la resolución de problemas**. Nivel de capacidad 2. Proceso **MAN.5 Gestión de riesgos**. Nivel de capacidad 2.
13.2.2 Aprendizaje de los incidentes de seguridad de la información. Deben existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información.	Proceso **SUP.9 Gestión de la resolución de problemas**. Proceso **MAN.5 Gestión de riesgos**. **RIN.3.BP4: Capturar conocimiento**. Identificar y registrar cada elemento de conocimiento de acuerdo con el esquema de clasificación y los criterios de los activos.
13.2.3 Recopilación de evidencias. Cuando se emprenda una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique acciones legales (tanto civiles como penales), deben recopilarse las evidencias, conservarse y presentarse conforme a las normas establecidas en la jurisdicción correspondiente.	Proceso **SUP.9 Gestión de la resolución de problemas**. **RIN.3.BP4: Capturar conocimiento**. Identificar y registrar cada elemento de conocimiento de acuerdo con el esquema de clasificación y los criterios de los activos.

Tabla C.35. Relaciones entre los controles de la categoría 13.2 Gestión de incidentes de seguridad de la información y mejoras y la norma ISO/IEC 15504-5

C.10. Relaciones de la cláusula 14 Gestión de la continuidad del negocio

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de la única categoría de esta cláusula de la norma ISO/IEC 27002.

C.10.1. Relaciones de la categoría 14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

El objetivo de la categoría 14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio es contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación. La tabla C.36 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
14.1.1 Inclusión de la seguridad de la información en el procesos de gestión de la continuidad del negocio. Debe desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio.	Proceso **MAN.2 Gestión de la organización**. Proceso **RIN.4 Infraestructura**.
14.1.2 Continuidad del negocio y evaluación de riesgos. Deben identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información.	Proceso **MAN.2 Gestión de la organización**. Proceso **RIN.4 Infraestructura**.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información. Deben desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requeridos, después de una interrupción o un fallo de los procesos de negocio críticos.	Proceso **MAN.2 Gestión de la organización**. Proceso **RIN.4 Infraestructura**.
14.1.4 Marco de referencia para la planificación de la continuidad del negocio. Debe mantenerse un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes sean coherentes, para cumplir los requisitos de seguridad de la información de manera consistente y para identificar las prioridades de realización de pruebas y de mantenimiento.	Proceso **MAN.2 Gestión de la organización**. Proceso **RIN.4 Infraestructura**.

Controles de la categoría 14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
14.1.5 Pruebas, mantenimiento y re-evaluación de los planes de continuidad del negocio. Los planes de continuidad del negocio deben probarse y actualizarse periódicamente para asegurar que están al día y que son efectivos.	Proceso **MAN.2 Gestión de la organización**. Proceso **RIN.4 Infraestructura**.

Tabla C.36. Relaciones entre los controles de la categoría 14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio y la norma ISO/IEC 15504-5

C.11. Relaciones de la cláusula 15 Cumplimiento

A continuación se muestran las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con cada uno de los controles de seguridad de las tres categorías de esta cláusula de la norma ISO/IEC 27002.

C.11.1. Relaciones de la categoría 15.1 Cumplimiento de los requisitos legales

El objetivo de la categoría 15.1 Cumplimiento de los requisitos legales es evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad. La tabla C.37 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 15.1 Cumplimiento de los requisitos legales de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
15.1.1 Identificación de la legislación aplicable. Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplir dichos requisitos, deben estar definidos, documentados y mantenerse actualizados de forma explícito para cada sistema de información de la organización.	Proceso **ENG.1 Captura de requisitos**. Proceso **ENG.2 Análisis de requisitos del sistema**. Proceso **ENG.4 Análisis de requisitos del software**.

Controles de la categoría 15.1 Cumplimiento de los requisitos legales de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
15.1.2 Derechos de propiedad intelectual (DPI) [*Intellectual Property Rights* (IPR)]. Deben implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software/propietario.	**ACQ.3.BP1: Negociar el contrato/acuerdo**. Negociar todos los aspectos del contrato/acuerdo con el proveedor. **ACQ.3.BP2: Aprobar el contrato**. El contrato es aprobado por las partes interesadas. **ACQ.3.BP3: Revisar el contrato para la monitorización de la capacidad del proveedor**. Revisar y considerar un mecanismo para monitorizar la capacidad y el rendimiento del proveedor en las condiciones del contrato. **ENG.1.BP3: Acordar los requisitos**. Obtener un acuerdo entre los equipos acerca de los requisitos del cliente disponiendo de las firmas de los representantes de todos los equipos y de todas las partes contractualmente sujetas a trabajar con estos requisitos. **SPL.1.BP9: Negociar el contrato/acuerdo con el adquiriente**. Negociar todos los aspectos relevantes del contrato/acuerdo con el adquiriente. **SPL.1.BP10: Establecer la confirmación del contrato/acuerdo**. Confirmar formalmente el contrato/acuerdo para proteger los intereses de ambas partes. **PIM.1.BP3: Definir los procesos estándar**. Definir y mantener una descripción de cada proceso estándar de acuerdo con las necesidades de establecer procesos de la organización.

Controles de la categoría 15.1 Cumplimiento de los requisitos legales de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
15.1.3 Protección de los documentos de la organización. Los documentos importantes deben estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, regulatorios, contractuales y empresariales.	**SUP.7.BP1: Desarrollar una estrategia de gestión de la documentación**. Determinar la estrategia de gestión de la documentación que cubra todo lo que debería ser documentado en cada área de la organización, para cada fase del ciclo de vida del producto/servicio. **SUP.7.BP3: Especificar los requisitos de los documentos**. Especificar los requisitos de los documentos tales como formato, título, fecha, identificación, historial de versiones, autor/es, responsable de la revisión, responsable de la autorización, el resumen de contenidos, la finalidad y la lista de distribución. **SUP.7.BP6: Revisar los documentos**. Revisar los documentos antes de su distribución, y autorizar los documentos antes de su distribución o difusión. **SUP.7.BP7: Distribuir los documentos**. Para proveer documentos, distribuir los documentos según los modos de distribución determinados, a través de los medios de comunicación apropiados para audiencias específicas, y confirmar la entrega de los documentos cuando sea necesario. **SUP.7.BP8: Mantener los documentos**. Mantener los documentos de acuerdo con la estrategia de documentación determinada. **SUP.8.BP10: Gestionar las copias de seguridad, el almacenaje, la gestión y la entrega de elementos configurados**. Asegurar la integridad y la consistencia de los elementos configurados a través de la planificación apropiada y de los recursos necesarios para copias de seguridad y almacenaje. Controlar la gestión y la entrega de elementos configurados.

Controles de la categoría 15.1 Cumplimiento de los requisitos legales de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
15.1.4 Protección de datos y privacidad de la información personal. Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y las regulaciones y, en su caso, en las cláusulas contractuales pertinentes.	**ACQ.3.BP1: Negociar el contrato/acuerdo**. Negociar todos los aspectos del contrato/acuerdo con el proveedor. **ACQ.3.BP2: Aprobar el contrato**. El contrato es aprobado por las partes interesadas. **ACQ.3.BP3: Revisar el contrato para la monitorización de la capacidad del proveedor**. Revisar y considerar un mecanismo para monitorizar la capacidad y el rendimiento del proveedor en las condiciones del contrato. **ENG.1.BP3: Acordar los requisitos**. Obtener un acuerdo entre los equipos acerca de los requisitos del cliente disponiendo de las firmas de los representantes de todos los equipos y de todas las partes contractualmente sujetas a trabajar con estos requisitos. **SPL.1.BP9: Negociar el contrato/acuerdo con el adquiriente**. Negociar todos los aspectos relevantes del contrato/acuerdo con el adquiriente. **SPL.1.BP10: Establecer la confirmación del contrato/acuerdo**. Confirmar formalmente el contrato/acuerdo para proteger los intereses de ambas partes. **RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **RIN.4.BP3: Adquirir la infraestructura**. Adquirir un proceso de infraestructura que satisfaga los requisitos. **RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización.

Controles de la categoría 15.1 Cumplimiento de los requisitos legales de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
15.1.5 Prevención del uso indebido de los recursos de tratamiento de la información. Se debe impedir que los usuarios utilicen los recursos de tratamiento de la información para fines no autorizados.	**RIN.2.BP5: Formar al personal**. Capacitar al personal de los conocimientos y habilidades necesarias para desempeñar sus funciones. **RIN.4.BP1: Identificar el alcance de la infraestructura**. Identificar los procedimientos, estándares, herramientas y técnicas que el proceso de infraestructura debería apoyar. **RIN.4.BP2: Definir los requisitos de infraestructura**. Definir los requisitos de infraestructura para dar soporte a la realización de los procesos apropiados. **RIN.4.BP3: Adquirir la infraestructura**. Adquirir un proceso de infraestructura que satisfaga los requisitos. **RIN.4.BP4: Establecer la infraestructura**. Ensamblar e integrar los elementos del proceso de infraestructura, proporcionando un entorno eficaz que dé soporte a la implantación de los procesos de la organización.
15.1.6 Regulación de los controles criptográficos. Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	**ACQ.3.BP1: Negociar el contrato/acuerdo**. Negociar todos los aspectos del contrato/acuerdo con el proveedor. **ACQ.3.BP2: Aprobar el contrato**. El contrato es aprobado por las partes interesadas. **ACQ.3.BP3: Revisar el contrato para la monitorización de la capacidad del proveedor**. Revisar y considerar un mecanismo para monitorizar la capacidad y el rendimiento del proveedor en las condiciones del contrato. **ENG.1.BP3: Acordar los requisitos**. Obtener un acuerdo entre los equipos acerca de los requisitos del cliente disponiendo de las firmas de los representantes de todos los equipos y de todas las partes contractualmente sujetas a trabajar con estos requisitos. **SPL.1.BP9: Negociar el contrato/acuerdo con el adquiriente**. Negociar todos los aspectos relevantes del contrato/acuerdo con el adquiriente. **SPL.1.BP10: Establecer la confirmación del contrato/acuerdo**. Confirmar formalmente el contrato/acuerdo para proteger los intereses de ambas partes.

Tabla C.37. Relaciones entre los controles de la categoría 15.1 Cumplimiento de los requisitos legales y la norma ISO/IEC 15504-5

C.11.2. Relaciones de la categoría 15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

El objetivo de la categoría 15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico es asegurar que los sistemas cumplen las políticas y normas de seguridad de la organización. La tabla C.38 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico de la norma ISO/IEC 27002	**Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas**
15.2.1 Cumplimiento de las políticas y normas de seguridad. Los directores deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad.	Proceso **SUP.1 Aseguramiento de la calidad**.
15.2.2 Comprobación del cumplimiento técnico. Debe comprobarse periódicamente que los sistemas de información cumplen las normas de aplicación de la seguridad.	**SUP.2.BP3: Realizar la verificación**. Verificar los productos de trabajo identificados de acuerdo con la estrategia especificada. **SUP.3.BP3: Realizar actividades de validación**. Llevar a cabo actividades de validación utilizando las técnicas, procesos y casos de prueba identificados en contra de los requisitos y estándares de calidad. Registrar los resultados de las actividades de validación.

Tabla C.38. Relaciones entre los controles de la categoría 15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico y la norma ISO/IEC 15504-5

C.11.3. Relaciones de la categoría 15.3 Consideraciones sobre la auditoría de los sistemas de información

El objetivo de la categoría 15.3 Consideraciones sobre la auditoría de los sistemas de información es lograr que el proceso de auditoria de los sistemas de información alcance la máxima eficacia con las mínimas interferencias. La tabla C.39 muestra los controles de seguridad de esta categoría, y las relaciones con las prácticas básicas de la norma ISO/IEC 15504-5.

Controles de la categoría 15.3 Consideraciones sobre la auditoría de los sistemas de información de la norma ISO/IEC 27002	Prácticas básicas de la norma ISO/IEC 15504-5 relacionadas
15.3.1 Controles de auditoría de los sistemas de información. Los requisitos y las actividades de auditoria que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de empresariales.	**SUP.5.BP1: Desarrollar e implementar una estrategia de auditoría**. Se implementa una estrategia de auditoría que define el propósito, el alcance, los hitos, los criterios de auditoría y el equipo de auditoría. **SUP.5.BP2: Seleccionar auditores**. Se seleccionan auditores independientes, imparciales y objetivos. **SUP.5.BP3: Auditar la conformidad con los requisitos**. Se auditan los productos, servicios o procesos seleccionados para determinar su conformidad con sus requisitos y disposiciones previstos. Se registran las no conformidades. **SUP.5.BP4: Preparar y distribuir un informe de auditoría**. El auditor elabora y distribuye un informe de auditoría.
15.3.2 Protección de las herramientas de auditoria de los sistemas de la información. El acceso a las herramientas de auditoria de los sistemas de información debe estar protegido para evitar cualquier posible peligro o uso indebido.	

Tabla 3.39. Relaciones entre los controles de la categoría 15.3 Consideraciones sobre la auditoría de los sistemas de información y la norma ISO/IEC 15504-5

ANEXO D. MiProJOC: el juego de mejora de procesos

La combinación de métodos tradicionales de formación con mecanismos de innovación pedagógica genera un efecto positivo en el aprendizaje de cualquier materia. Como complemento de las sesiones de formación teóricas y prácticas en los estándares que integra el nuevo Modelo Integrado de Estándares de Gestión de TI, y para facilitar su aplicación en las organizaciones de desarrollo de software, se ha desarrollado un juego de preguntas y respuestas llamado MiProJOC, cuyo acrónimo proviene de *juego de mejora de procesos*, y es accesible a través de www.miprojoc.com.

Esta herramienta ha sido diseñada para ofrecer a sus usuarios un soporte automatizado para la consolidación y evaluación de conocimientos sobre diferentes campos o áreas de conocimiento, como pueden ser la mejora de procesos de software, la gestión de servicios de TI o la gestión de la seguridad de la información. La herramienta permite el mantenimiento de un repositorio de preguntas sobre las distintas áreas de conocimiento, en este caso sobre los distintos estándares integrados, definir distintas modalidades de juego y presentar los resultados estadísticos derivados de la utilización del juego.

Desde el punto de vista funcional el juego MiProJOC puede dividirse en dos grandes módulos:

- Un módulo de administración, denominado MiProJOC Adm. Este primer módulo, que será de uso exclusivo para los usuarios administradores, permitirá definir las diferentes áreas de conocimiento, mantener la batería de preguntas y respuestas para cada una de éstas áreas, configurar los diferentes modos de juego y obtener informes estadísticos.
- Un módulo de juego, denominado MiProJOC Game. Este segundo módulo agrupa todas las funciones relacionadas con la realización de juegos, tanto individuales como en equipo, y será utilizado para comprobar el grado de conocimiento de los usuarios de una determinada área de conocimiento.

En los apartados siguientes se describen las principales funcionalidades de cada uno de estos dos módulos.

D.1. Módulo de administración: MiProJOC Adm

El módulo de administración ha sido diseñado con el objetivo de dar soporte a la gestión del repositorio de preguntas, la configuración de las diferentes modalidades de juego y la visualización de estadísticas de aciertos por categorías de preguntas. A continuación, se exponen con más detalle las principales funciones que contempla este módulo.

- **Gestión del repositorio de preguntas**. La gestión del repositorio de preguntas incluye las funciones necesarias para administrar las áreas de conocimiento, las categorías en que se divide cada área y las preguntas que se generen para cada una de estas categorías.
- **Configuración de las modalidades de juego**. Este módulo ofrece el conjunto de funcionalidades necesarias para definir nuevas modalidades de juego o parametrizar las modalidades ya existentes. Estas modalidades de juego surgen de la asignación de unos determinados valores para una serie de parámetros. MiProJOC cuenta con los siguientes parámetros, que el administrador podrá ir adaptando para generar nuevas modalidades de juego:
  - Número de jugadores. Existen modalidades de juego individual (1 jugador) y modalidades de juego para varios jugadores o equipos (2-6 jugadores).
  - Tiempo máximo de partida. En caso de activar este parámetro, un contador indica en todo momento el tiempo restante de juego.
  - Tiempo máximo de respuesta. Indica el tiempo de que dispone el jugador para seleccionar la respuesta correcta.
  - Número máximo de preguntas por categoría. Indica el número máximo de preguntas de cada categoría que pueden formularse durante el juego.
  - Número máximo de aciertos por categoría. Indica el número de preguntas de una determinada categoría que deben responderse correctamente para demostrar su dominio.

  A partir de la combinación de valores para los parámetros anteriores, MiProJOC cuenta con 3 modalidades de juego predefinidas: Competición, Autoevaluación y Contrarreloj. Los posibles valores que pueden tomar los parámetros, en caso de que sean configurables se muestran en la tabla D.1.

Parámetro	**Modalidad de juego**		
	Competición	**Autoevaluación**	**Contrarreloj**
Número de jugadores	2-6	1	1
Tiempo máximo de partida	10-120 min	10-30 min	1-3 min
Tiempo máximo de respuesta	NO / 5-30 s	NO	NO
Número máximo de preguntas por categoría	NO	1-10	NO

Parámetro	Modalidad de juego		
	Competición	**Autoevaluación**	**Contrarreloj**
Número máximo de aciertos por categoría	1-5	NO	NO

Tabla D.1. Modalidades de juego de MiProJOC

- **Visualización de resultados estadísticos**. El módulo de administración también ofrece funciones de visualización de resultados estadísticos. Estos resultados muestran información sobre:
  - Pruebas de evaluación. Se indican las preguntas que han aparecido en las diferentes pruebas generadas, los porcentajes de éxito o de fracaso en cada una de las respuestas y otra información que pueda considerarse de interés.
  - Preguntas. Se permite consultar el número de veces que se ha acertado cada pregunta de entre el número de veces que se ha formulado.
  - Categorías. Ofrece la posibilidad de consultar las categorías con más preguntas acertadas o falladas.
  - Usuarios. Permite almacenar los resultados que obtiene un usuario en las diferentes pruebas de evaluación. De esta manera, una misma persona puede comprobar si va mejorando en los conocimientos de un determinado tema.
  - Equipos. Permite comparar la evolución de los distintos equipos de juego, a partir del número de partidas jugadas, de partidas ganadas, y del número de aciertos en cada categoría de preguntas.

D.2. Módulo de juego: MiProJOC Game

El módulo MiProJOC Game ofrece la posibilidad de acceder a diferentes juegos de preguntas y respuestas con objetivos y normas diferentes para cada caso.

En la primera pantalla de este módulo se presentan todas las modalidades de juego definidas en el módulo de administración. La figura D.1 muestra las modalidades de juego que inicialmente ofrece MiProJOC: dos modalidades de juego individual (Autoevaluación y Contrarreloj) y una modalidad para varios jugadores o equipos (Competición).

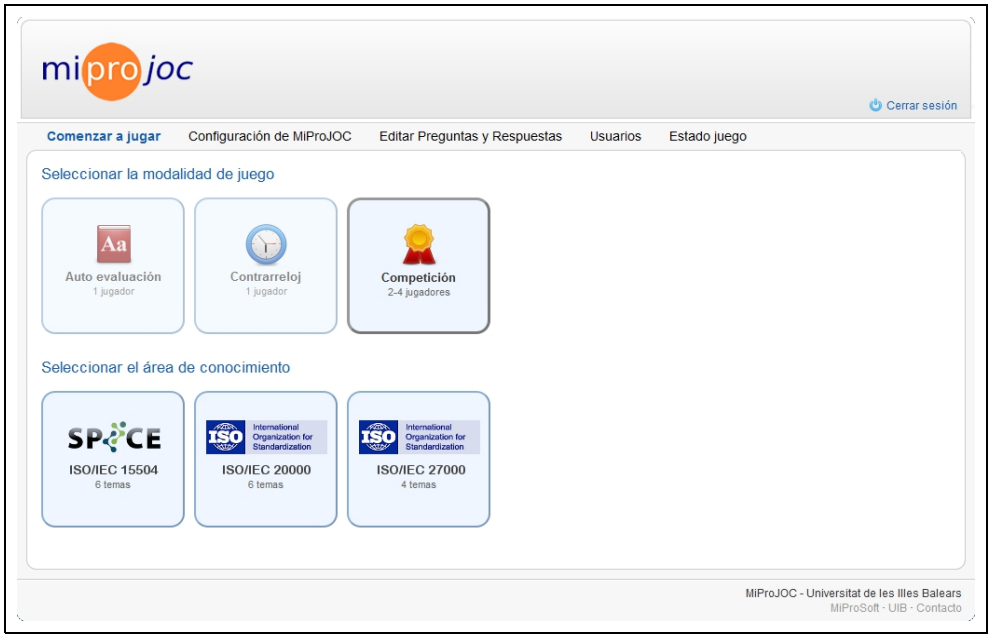

Figura D.1. Pantalla de selección de la modalidad de juego

- **Autoevaluación**. En la modalidad de Autoevaluación, el usuario, una vez registrado, deberá elegir el área de conocimiento de la que desea ser evaluado y, a continuación, las categorías sobre las que se le formularán las preguntas. Además deberá seleccionar el número de preguntas que se le formularán de cada una de estas categorías así como la modalidad de puntuación: que una respuesta incorrecta reste la parte proporcional al número de posibles respuestas de la pregunta, o que las respuestas equivocadas se traten como si fueran preguntas sin responder. Una vez finalizada la partida, se muestran los resultados obtenidos en el informe de la evaluación, que contiene: el número de preguntas formuladas, el número de respuestas acertadas, el de no acertadas y el que se han dejado sin responder. A partir de estos datos y según la modalidad de puntuación elegida, se presenta la puntuación final obtenida y el tiempo invertido en completar el test.
- **Contrarreloj**. La modalidad de juego Contrarreloj es una variante de la modalidad anterior, en la que el usuario, una vez registrado, en lugar de elegir el número de preguntas que va a responder, debe elegir el tiempo máximo para contestar correctamente el mayor número de preguntas posible. Del mismo modo que en la modalidad anterior, puede elegir si las respuestas respondidas de forma incorrecta descuentan o no sobre las respuestas acertadas. También se genera un informe con los resultados de la partida.

- **Competición**. La modalidad de juego de Competición está pensada para varios jugadores o equipos. Como en las modalidades anteriores, los jugadores deberán elegir el área de conocimiento y las categorías de las preguntas. Antes de empezar la partida, se ofrecerá la posibilidad de personalizar los siguientes aspectos: el nivel de dificultad de las preguntas, la duración máxima de la partida, el tiempo máximo de respuesta y el número máximo de aciertos por categoría. El jugador o equipo ganador será el que consiga antes reunir el número prefijado de aciertos en todas las categorías de preguntas. La figura D.2 muestra un momento de una partida en la modalidad Competición.

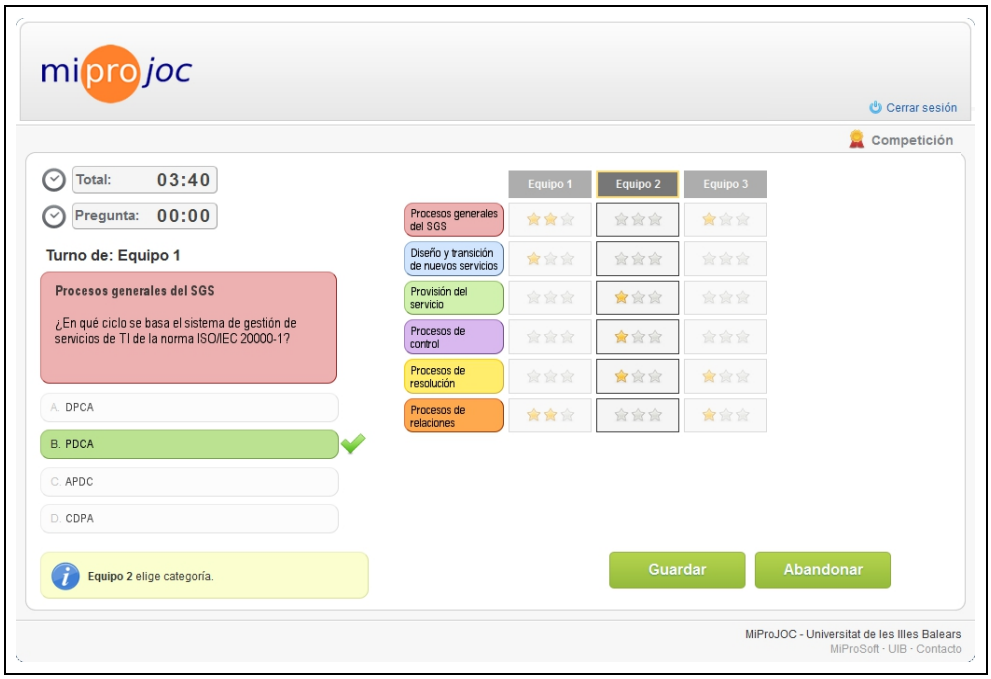

Figura D.2. Pantalla de juego en el modo Competición

ANEXO E. Guías para la implantación de sistemas de gestión integrados a partir de la norma ISO 9001

Uno de los resultados de esta tesis doctoral ha sido la elaboración de dos guías que definen directrices para facilitar la implantación de sistemas de gestión integrados según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001.

- La *Guía para la integración del Sistema de Gestión de Servicios de TI de la norma ISO/IEC 20000-1 con el Sistema de Gestión de Calidad de la norma ISO 9001* puede ser usada para facilitar la implantación del sistema de gestión de servicios de TI que propone la norma ISO/IEC 20000-1 de forma integrada con el sistema de gestión de calidad de la norma ISO 9001.
- La *Guía para la integración del Sistema de Gestión de Seguridad de la Información de la norma ISO/IEC 270001 con el Sistema de Gestión de Calidad de la norma ISO 9001* permite facilitar la implantación integrada del sistema de gestión de seguridad de la información de la norma ISO/IEC 27001 con el sistema de gestión de calidad de la norma ISO 9001.

Ambas guías pueden ser utilizadas tanto por las organizaciones interesadas en integrar sus sistemas de gestión como por consultores especializados en la implantación de las normas que se integran.

Al constituir estas guías un material inédito y con entidad propia, se han redactado y estructurado en dos documentos independientes con la intención de que puedan ser editadas en un futuro próximo. Además, el día 16 de Diciembre de 2011 se inició la tramitación del expediente de solicitud de inscripción de las dos guías en el Registro Central de la Propiedad Intelectual de Madrid.