risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido / Recibido: 2/12/2013
Aceitação / Aceptación: 13/01/2014

Integración de Estándares de Gestión de TI mediante MIN-ITs

Antoni Lluís Mesquida [1], Antonia Mas [1], Tomás San Feliu [2], Magdalena Arcilla [3]

antoni.mesquida@uib.es, antonia.mas@uib.es, tomas.sanfeliu@upm.es, marcilla@issi.uned.es

[1] Universitat de les Illes Balears, Departamento de Ciencias Matemáticas e Informática, Cra. de Valldemossa, km 7.5, 07122 Palma de Mallorca, España.

[2] Universidad Politécnica de Madrid, Facultad de Informática, Campus de Montegancedo, 28660 Boadilla del Monte, Madrid, España.

[3] Universidad Nacional de Educación a Distancia, ETS Ingeniería Informática, C/ Juan del Rosal 16, 28040 Madrid, España.

DOI: 10.4304/risti.e1.31-45

Resumen: Las empresas de desarrollo de software han apostado por la implantación de modelos y estándares de calidad con el objetivo de ofrecer productos que se adapten a las necesidades de los clientes y aumenten su satisfacción. Además de mejorar sus procesos de desarrollo de software, estas organizaciones también desean aumentar la capacidad de los procesos de otras disciplinas, como pueden ser la gestión de servicios de Tecnologías de la Información (TI) o la gestión de la seguridad de la información. Las normas ISO que definen las mejoras prácticas de estas áreas guardan una gran cantidad de relaciones entre sus recomendaciones, directrices y requisitos. A partir del estudio de todos estos elementos y aspectos comunes, se ha desarrollado el marco MIN-ITs, un marco que facilita la implantación integrada de los diferentes estándares ISO de gestión de TI.

Palabras-clave: Integración de Estándares de Gestión de TI, ISO/IEC 15504, ISO 9001, ISO/IEC 20000, ISO/IEC 27000.

Integrating IT Management Standards through MIN_ITs

***Abstract*:** Software development companies have opted for implementing quality models and standards in order to provide products that meet customers' needs and increase their satisfaction. In addition to improving their software development processes, these organizations also wish to increase the capability of the processes related to other disciplines, such as Information Technology (IT) service management and information security management. The ISO standards that define the best practices in these areas keep a great number of relations among their recommendations, guidelines and requirements. From the study of all these common elements and aspects we have developed MIN-ITs, a framework

that facilitates the integrated implementation of different ISO IT management standards.

Keywords: Integration of IT Management standards, ISO/IEC 15504, ISO 9001, ISO/IEC 20000, ISO/IEC 27000.

1. Introducción

Las organizaciones de desarrollo de software han apostado, desde mediados de los noventa, por la implantación de estándares con el objetivo de 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 (ISO, 2008), que define un sistema de gestión de la calidad que garantiza la eficacia y la fiabilidad de los procesos de negocio de la organización (Mas & Amengual 2004; Mas, Amengual & Mesquida, 2010). Por otra parte, estas organizaciones también se interesaron por la aplicación de modelos para la evaluación y mejora de los procesos de desarrollo de software, como pueden ser CMMI (SEI, 2010) o el estándar internacional ISO/IEC 15504 (ISO, 2003; ISO, 2004).

En la actualidad, las empresas de este sector, además de seguir reconociendo la importancia de mejorar sus procesos de desarrollo de software, parecen haber puesto una especial atención también hacia nuevos dominios de interés, como pueden ser la gestión de servicios de Tecnologías de la Información (TI) o la gestión de la seguridad de la información.

Para las empresas de desarrollo de software es fundamental que sus clientes se formen una opinión positiva sobre los servicios que reciben, y que éstos satisfagan todas sus necesidades y expectativas (Mesquida, Mas, Amengual & Calvo-Manzano, 2012). Es por esta razón que también desean cubrir los procesos de gestión de servicios de TI y adoptar las mejores prácticas propuestas por los estándares más conocidos de esta disciplina, como son ITIL (TSO, 2011) e ISO/IEC 20000 (ISO, 2010a). Además, en estas organizaciones, 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 se ha interesado por la implantación de la norma ISO/IEC 27001 (ISO, 2005a) como estándar de seguridad de la información y, más concretamente, por la implantación de controles de seguridad definidos en la norma ISO/IEC 27002 (ISO, 2005b) para 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.

Después de años de relaciones y de trabajo continuado con empresas del sector TIC de nuestro entorno más próximo (Mas, Fluxà & Amengual, 2012; Mesquida, Mas & Amengual, 2011), se ha podido observar que, en la mayoría de casos, cuando una empresa decide implantar una norma relativa a la gestión de servicios de TI o a la gestión de la seguridad de la información, ya ha tenido otras experiencias de calidad previas, principalmente, la implantación de la norma ISO 9001 (ISO, 2008) y el despliegue de procesos según ISO/IEC 15504 (ISO, 2006) o CMMI-DEV (SEI, 2010).

La implantación de nuevos estándares de diferentes disciplinas genera 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 las buenas prácticas desplegadas anteriormente.

Dado que todos los estándares ISO anteriores se basan en un enfoque orientado a procesos, existen ciertos elementos comunes en todos ellos. Además, las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001 definen sistemas de gestión que, aunque sean específicos para ámbitos diferentes, pueden ser integrados con otros sistemas de gestión externos. Así pues, una implantación integrada de estas normas 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 una optimización de las tareas relacionadas con la implementación de procesos y buenas prácticas, y el mantenimiento de los sistemas de gestión que definen.

Este artículo presenta un marco integrado para facilitar la implantación de los estándares ISO de gestión de TI, entendiendo como tales los estándares de mejora de procesos de software, de gestión de servicios de TI y de gestión de la seguridad de la información. Este marco combina las mejores prácticas de estas disciplinas y facilita la adopción de las normas relacionadas con ellas, reduciendo los esfuerzos necesarios para su implantación, evitando duplicidades, reutilizando conocimientos y experiencias, y aprovechando las lecciones aprendidas y las metas ya conseguidas en iniciativas de calidad emprendidas con anterioridad. Más concretamente, la solución presentada pretende facilitar:

- La implantación de las normas ISO/IEC 20000 y/o ISO/IEC 27001 en organizaciones que ya hayan iniciado un programa de mejora de procesos de software según la norma ISO/IEC 15504 y que hayan obtenido la certificación ISO 9001 o
- La implantación de manera integrada de 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.

2. MIN-ITs: Marco INtegrado de Estándares de gestión de TI

La Figura 1 presenta el marco MIN-ITs (Marco INtegrado de Estándares de gestión de TI) desarrollado. Este marco está formado 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 con los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y con los controles de seguridad de la información de la norma ISO/IEC 27002.

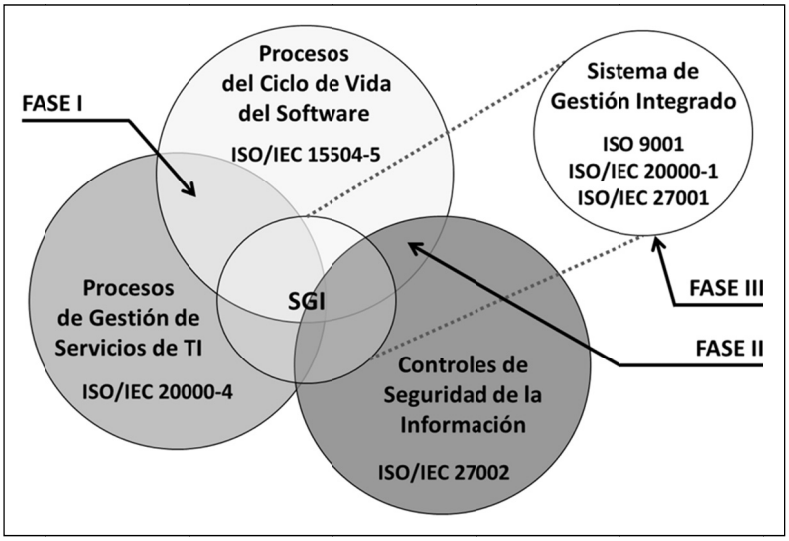

Figura 1 – MIN-ITS: Marco INtegrado de Estándares de gestión de TI

Las intersecciones entre los elementos de la Figura 1 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 las normas ISO/IEC 20000-1 e ISO/IEC 27001.

3. Construcción de MIN-ITs

El marco MIN-ITs es el resultado de un proceso de construcción formado por tres fases consecutivas y que se describen a continuación.

3.1. Fase I: Estudio de las relaciones entre las normas ISO/IEC 15504 e ISO/IEC 20000

Durante la primera fase de la construcción de MIN-ITs, se llevó a cabo un estudio exhaustivo de todas las relaciones y elementos comunes entre los resultados de los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 (ISO, 2010) y las prácticas básicas de los procesos del ciclo de vida del software que define la norma ISO/IEC 15504-5 (ISO, 2006).

La Figura 2 muestra el procedimiento seguido para realizar el estudio de relaciones entre las dos normas. Este estudio fue llevado a cabo siguiendo una estrategia iterativa en la que, para cada uno de los 26 procesos de la norma ISO/IEC 20000-4, se analizaron en profundidad sus resultados y se seleccionaron las prácticas básicas de la norma ISO/IEC 15504-5 relacionadas.

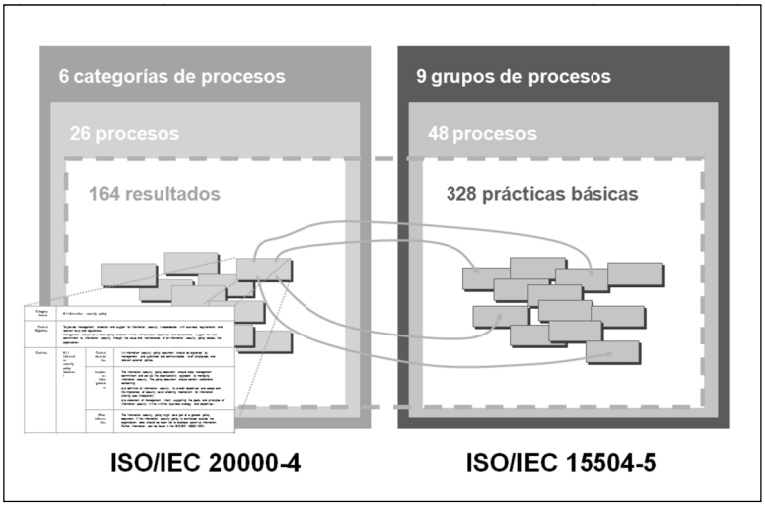

Figura 2 - Procedimiento seguido para el estudio de las relaciones de las normas ISO/IEC 20000-4 e ISO/IEC 15504-5

La versión final de la comparativa entre estos dos estándares es el resultado de un proceso de refinamiento sucesivo en tres etapas que se describen a continuación. Con el objetivo de compartir el conocimiento y de contrastar los diferentes puntos de vista de los autores, durante la primera etapa, las relaciones entre los dos estándares fueron analizadas en grupo. Se necesitaron varias sesiones de trabajo para obtener una versión preliminar de la comparativa. 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, para confirmar las decisiones alcanzadas o, por el contrario, hacer modificaciones sobre la versión preliminar. Finalmente, durante la etapa de revisión conjunta, las propuestas de cada uno de los autores fueron discutidas detenidamente, hasta llegar a un consenso general para aceptar o rechazar cada propuesta.

La Tabla 1 muestra 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.

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

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

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 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					

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 ISO/IEC 15504-5, se establecieron cuatro tipos distintos de relaciones:

1. Relación total. Un total de doce procesos de la norma ISO/IEC 20000-4 (Auditoría, Gestión de cambios, Gestión de la configuración, Gestión de recursos humanos, Mejora, Gestión de incidentes y cumplimiento de peticiones, Gestión de la información, Revisión de la dirección, Medición, Gestión de riesgos, Planificación y monitorización del servicio, y Generación de informes del servicio) quedan totalmente cubiertos por prácticas básicas de la norma ISO/IEC 15504-5. Todos estos procesos, 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: (1) Nueve de estos doce procesos 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. (2) 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. (3) 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. (4) 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.

2. Relación fuerte. Otros siete procesos de la norma ISO/IEC 20000-4 quedan ampliamente cubiertos por prácticas básicas de la norma ISO/IEC 15504-5: Elaboración del presupuesto y contabilidad de los servicios de TI, Gestión de la seguridad de la información, Gestión organizativa, Gestión de problemas, Requisitos del servicio, Establecimiento y mantenimiento del SGS, y Gestión de suministradores. 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: (1) 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. (2) 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. (3) 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. (4) Los propósitos de los procesos ENG.1 Captura de requisitos y SUP.3 Validación pueden ampliarse para definir y validar los Requisitos del servicio. (5) 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. (6) 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.

3. Relación parcial. 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.

4. Inexistencia de relación. 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.

3.2. 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, durante la segunda fase de MIN-ITs se examinaron las relaciones existentes entre los

controles de seguridad de la información que define la norma ISO/IEC 27002 (ISO, 2005b) y las prácticas básicas de la norma ISO/IEC 15504-5 (ISO, 2006), con el objetivo de facilitar la implantación de la norma ISO/IEC 27000 en una empresa que ya tiene un determinado nivel de capacidad en algunos procesos según la norma ISO/IEC 15504 o facilitar la implantación conjunta de ambos estándares.

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, para cada uno de los 133 controles de seguridad de la información de la norma ISO/IEC 27002, que se agrupan en once cláusulas, se seleccionó un conjunto de prácticas básicas de la norma ISO/IEC 15504-5 relacionadas con el resultado en cuestión.

La Tabla 2 muestra, a alto nivel, un resumen de las relaciones detectadas entre las once cláusulas de la norma ISO/IEC 270002 y los nueve grupos de procesos de la norma ISO/IEC 15504-5. Como resultado de esta segunda fase, pudimos observar que 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.

Tabla 2 - Relaciones entre las cláusulas de la norma ISO/IEC 27002 y los grupos de procesos de la norma ISO/IEC 15504-5

	Grupos de procesos de ISO/IEC 15504-5								
Cláusulas de ISO/IEC 27002	**ACQ**	**SPL**	**ENG**	**OPE**	**MAN**	**PIM**	**RIN**	**REU**	**SUP**
Política de seguridad					x		x		
Aspectos organizativos de la seguridad de la información	x	x			x		x		x
Gestión de activos							x		
Seguridad ligada a recursos humanos					x		x		
Seguridad física y ambiental							x		
Gestión de comunicaciones y operaciones	x	x	x				x		x
Control de acceso							x		
Adquisición, desarrollo y mantenimiento de los sistemas de información	x		x		x		x		x
Gestión de incidentes de seguridad de la información					x		x		x
Gestión de la continuidad del negocio					x		x		
Cumplimiento	x	x	x				x		x

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 cuatro 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.

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: (1) 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 o (2) 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. 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.

3.3. Fase III: Definición de un Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001

Durante la tercera fase se construyó el núcleo de MIN-ITs, es decir, un sistema de gestión integrado que amplía los requisitos del sistema de gestión de calidad de la norma ISO 9001 (ISO, 2008), con los requisitos específicos del Sistema de Gestión de Servicios de TI (SGSTI) de la norma ISO/IEC 20000-1 (ISO, 2011) y del Sistema de Gestión de Seguridad de la Información (SGSI) de la norma ISO/IEC 27001 (ISO, 2005a).

El primer paso de la investigación realizada en esta fase consistió en realizar un estudio en profundidad de los diferentes sistemas de gestión para determinar las posibilidades de integración. Después de observar que las tres normas se refieren explícitamente a la compatibilidad con otros sistemas de gestión, llevamos a cabo un estudio exhaustivo para interpretar los requisitos de los tres sistemas de gestión anteriores y analizar las relaciones entre ellos. Este estudio fue llevado 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 sistema de gestión de calidad de la norma ISO 9001 y, de manera análoga, cada uno de los requisitos del SGSI de la norma ISO/IEC 27001 fue comparado con todos los requisitos del sistema de gestión de calidad de la norma ISO 9001.

Para asegurar una buena trazabilidad entre las diferentes normas, este proceso iterativo se llevó a cabo también en la dirección opuesta, es decir, comparando cada uno de los requisitos del sistema de gestión de calidad 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 Tabla 3 muestra el nuevo sistema de gestión integrado obtenido. La primera columna muestra los requisitos del sistema de gestión de calidad de la norma ISO 9001. La segunda y la tercera columnas muestran, respectivamente, las ampliaciones sobre los requisitos del sistema de gestión de calidad de la norma ISO 9001 con los aspectos propios de la gestión de servicios de TI de la norma ISO/IEC 20000-1 o de la gestión de la seguridad de la información de la norma ISO/IEC 27001.

Tabla 3 - Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001

ISO/IEC 9001:2008	ISO/IEC 20000-1:2011	ISO/IEC 27001:2005
0.2 Enfoque basado en procesos	4.5 Establecer y mejorar el SGS	0 Enfoque por proceso
1 Objeto y campo de aplicación	1 Objeto y campo de aplicación	
1.1 Generalidades	1.1 Generalidades	
1.2 Aplicación	1.2 Aplicación	
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
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
5.4.1 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	
5.5.2 Representante de la dirección	4.1.4 Representante de la dirección	
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	

ISO/IEC 9001:2008	ISO/IEC 20000-1:2011	ISO/IEC 27001:2005
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
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)	
8.1 Generalidades		4.2.4 Mantenimiento y mejora del SGSI
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)	
8.5 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

4. Activos de soporte a la utilización de MIN-ITs

Con el objetivo de facilitar la aplicación de MIN-ITs en empresas de desarrollo de software, a partir de los resultados obtenidos en cada una de las tres fases, se desarrollaron un conjunto de activos de soporte a su implantación.

El activo resultante de la primera fase fue 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 de relaciones 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.

A partir de las relaciones detectadas en la segunda fase entre los controles de seguridad de la norma ISO/IEC 27002 y los procesos de la norma ISO/IEC 15504-5, se construyó la *ISO/IEC 15504 Security Extension*, una extensión que 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. Para cada uno de los controles de seguridad de la norma ISO/IEC 27002, la *ISO/IEC 15504 Security Extension* detalla los cambios que son necesarios realizar sobre los procesos de la norma ISO/IEC 15504-5 con el fin de hacerlos compatibles con los requisitos de seguridad del control de la norma ISO/IEC 27002 en cuestión. Las modificaciones y

ampliaciones que propone realizar la *ISO/IEC 15504 Security Extension* sobre los procesos de la norma ISO/IEC 15504-5, pueden afectar a diferentes componentes de los procesos: propósito, prácticas básicas y/o productos de trabajo.

Finalmente, a partir de las relaciones entre los sistemas de gestión de las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001 extraídas durante la tercera fase y, con el objetivo de ofrecer una aproximación incremental con directrices para la alineación y/o integración de estos tres sistemas de gestión, se elaboraron dos guías de soporte a la implantación efectiva de sistemas de gestión integrados:

- *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*. Fue diseñada con el objetivo de implantar el SGSTI que propone la norma ISO/IEC 20000-1 de forma integrada con el sistema de gestión de calidad de la norma ISO 9001.
- *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 sistema de gestión de calidad de la norma ISO 9001.

5. Conclusiones

En este artículo se ha presentado MIN-ITs, un nuevo marco integrado de estándares de gestión de TI compuesto, por una parte, por un modelo de referencia de procesos 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 resultados y controles de las normas ISO/IEC 20000-4 e ISO/IEC 27002 y, por otra parte, por 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.

Este marco es el resultado de un trabajo de investigación en tres fases cuyos resultados han permitido, en primer lugar, 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. En segundo lugar, 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 y el mantenimiento de un sistema de gestión de seguridad de la información según la norma ISO/IEC 27001. La *ISO/IEC 15504 Security Extension* desarrollada ofrece a estas empresas directrices para facilitar el despliegue de los controles de seguridad sobre los procesos de la norma ISO/IEC 15504-5, reduciendo los esfuerzos para implantar ambos estándares que se deberían dedicar si se llevara a cabo su implantación por separado.

Finalmente, debido al gran número de elementos comunes entre los tres sistemas de gestión de las normas ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001, el esfuerzo necesario para implantar el sistema de gestión integrado propuesto, sería mucho menor que el esfuerzo que supondría implantar los tres sistemas de gestión de manera

independiente. La implantación de este sistema de gestión integrado permite a las organizaciones reducir los recursos humanos, presupuesto y tiempo necesarios para planificar, implementar y mantener los diferentes sistemas de gestión.

Referencias bibliográficas

ISO (2003). ISO/IEC 15504-2:2003 Information technology -- Process assessment -- Part 2: Performing an assessment.

ISO (2004). ISO/IEC 15504-1:2004 Information technology -- Process assessment -- Part 1: Concepts and vocabulary.

ISO (2005a). ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standarization.

ISO (2005b). ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management, International Organization for Standarization.

ISO (2006). ISO/IEC 15504-5:2006 Information Technology – Process Assessment – Part 5: An exemplar Process Assessment Model, International Organization for Standarization.

ISO (2008). ISO 9001:2008 Quality management systems – Requirements, International Organization for Standarization.

ISO (2010). ISO/IEC TR 20000-4:2010 Information technology – Service Management – Part 4: Process reference model, International Organization for Standarization.

ISO (2011). ISO/IEC 20000-1:2011 Information technology – Service management – Part 1: Service management system requirements, International Organization for Standarization.

Mas, A. & Amengual, E. (2004). A Method for the Implementation of a Quality Management System in Software SMEs. *Proc. 12th International Conference on Software Quality Management. British Computer Society*, March 2004, 61-74.

Mas, A., Amengual, E. & Mesquida, A. L. (2010). Application of ISO/IEC 15504 in Very Small Enterprises. *Systems, Software and Services Process Improvement, Communications in Computer and Information Science* 99, Springer-Verlag, 290-301.

Mas, A., Fluxà, B. & Amengual E. (2012). Lessons learned from an ISO/IEC 15504 SPI Programme in a Company. *Journal of Software: Evolution and Process*. 24, 5, 493-500.

Mesquida, A. L., Mas, A. & Amengual, E. (2011). An ISO/IEC 15504 Security Extension. *Communications in Computer and Information Science* 155, Springer-Verlag, 64-72.

Mesquida, A. L., Mas, A., Amengual, E. & Calvo-Manzano, J. A. (2012). IT Service Management Process Improvement based on ISO/IEC 15504: A systematic review. *Information and Software Technology*, 54, 3, 239-247.

SEI (2010). CMMI® for Development, Version 1.3, Software Engineering Institute.

TSO (2011). ITIL® Lifecycle Publication Suite – Books. The Stationery Office.