Guía de Estándares y Modelos de Buenas Prácticas

Aplicables a la Calidad en Sistemas y Tecnologías de la Información y Comunicación (CSTIC)

Guía de ayuda para la selección de estándares o modelos de buenas prácticas más idóneos para cumplir los objetivos de negocio de las organizaciones en el área de Calidad, Desarrollo de Sistemas, Gestión de Proyectos, y Gobierno Corporativo y Gestión TI.

Grupo de trabajo del Comité CSTIC de la AEC

2016

Este informe recopila las conclusiones del Grupo de Trabajo de la Comunidad AEC de Calidad en los Sistemas y las Tecnologías de la Información y las Comunicaciones.

Esta Comunidad tiene como misión constituir un foro de encuentro que, mediante la suma de experiencia y conocimiento de sus integrantes, permita explorar, identificar y desarrollar de forma colaborativa los modelos y prácticas de éxito en la gestión de las TIC.

Entre sus objetivos está el propiciar un ámbito de encuentro y de colaboración intersectorial de expertos en el que se compartan experiencias relativas a la gestión de las TIC, mediante casos prácticos, metodologías y benchmarking. Fruto de este trabajo conjunto nace el presente documento "Guía de Estándares y Modelos de Buenas Prácticas".

La AEC promueve y colabora en la difusión de los trabajos elaborados por sus Comunidades y Comités, respetando al máximo su independencia y el criterio de sus miembros. Las opiniones y contenidos reflejan, por tanto, sus opiniones y no necesariamente el posicionamiento oficial de la AEC.

Asociación Española para la Calidad (AEC), Marzo 2016

Reconocimientos

La Comunidad AEC CSTIC (Calidad, Sistemas y Tecnologías de la Información y la Comunicación) desea reconocer la dedicación y esfuerzo a:

Coordinador del Grupo de trabajo:

Antonio Moya Catena, Miembro individual de la AEC y Vicepresidente del Comité CSTIC

Autores del estudio:

Ana Isabel González Fernández, ATOS SPAIN

Antonio Moya Catena, Miembro individual de la AEC

Beatriz Brecciaroli Fragozo, THALES ESPAÑA GRP, S.A.U.

Carmen de León, IBERDROLA

Cristina Alias Aveledo, ALHAMBRA EIDOS

Cristina Fernández, CF Consultores

José Alberto González García, GMV

José Luis Báez García, FCC SERVICIOS INDUSTRIALES Y ENERGETICOS, S.A.

Juan Antonio Caloto Caloto, AEC

Manuel Arturo Lea Pereira, GMV

Miguel García Menéndez, iTTi

Pilar Ballesteros Vadillo, THALES ESPAÑA GRP, S.A.U.

Ramiro Carballo, CAELUM INFORMATION & QUALITY TECHNOLOGIES, S.L.

Raquel Martín Gómez, Ministerio de Defensa

Víctor Hervías Delgado, BUSINESS CONTINUITY MANAGEMENT

Rogelio Polanco Heras, ALHAMBRA EIDOS

Índice

Introducción

Propósito de este estudio

El propósito de este estudio es proporcionar una Guía a los responsables y profesionales del área de Calidad, cuyas organizaciones realizan su actividad en el campo de los Sistemas y Tecnologías de la Información y la Comunicación (CSTIC) a la hora de tener que decidir sobre qué estándar o modelo de buenas prácticas implementar para cumplir determinados objetivos de negocio o cumplir con unos requisitos legales o normativos. También proporciona un mapa de los estándares y modelos de buenas prácticas más relevantes, implantados y reconocidos en el mundo.

Cada uno de los estándares o modelos ha sido descrito brevemente, pero muy enfocado para facilitar su comprensión, destacando los elementos más importantes a la hora de decidir su implementación y aportando información sobre los factores de éxito para que dicha implementación sea lo más eficaz y eficiente posible.

Los estándares y modelos incluidos en este estudio están agrupados en áreas o dominios de interés, para facilitar tanto su clasificación como su búsqueda y relaciones entre ellos. Esta clasificación está plasmada en un Mapa de Estándares y Modelos de Buenas Prácticas que se presenta en la figura 1.

Descripción de los dominios de aplicación

El dominio de *Calidad* agrupa los estándares y modelos que están más enfocados a garantizar y gestionar la calidad de los productos y de los procesos usados para producirlos.

El dominio de *Desarrollo de Sistemas* se enfoca en los procesos necesarios para el desarrollo de los Sistemas de Información y en los modelos que evalúan la madurez de dichos procesos.

En el dominio de *Gestión de Proyectos* se consideran aquellos estándares relacionados con la gestión de proyectos y con la competencia necesaria para ejecutar las actividades de gestión de proyectos.

El dominio *Gobierno Corporativo y Gestión TI* incluye los modelos de buenas prácticas a usar tanto para el buen Gobierno Corporativo de las TIC como la Gestión de los Servicios TI, considerando también el área de Seguridad de la Información.

El dominio *Negocio* se centra en los estándares relacionados con el sistema de gestión global del negocio y su continuidad.

Estándares y modelos incluidos en este estudio

La clasificación de los estándares y modelos de buenas prácticas se han clasificado en cinco áreas o dominios de aplicación: Calidad; Desarrollo de Sistemas; Gestión de Proyectos; Gobierno Corporativo y Gestión TIC; y Negocio.

Calidad

- ISO/IEC 15939:2007 – System and software engineering – Measurement process
- ISO/IEC 25010:2011 – Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models

- **Desarrollo de Sistemas**
  - ISO/IEC 12207:2008 – Systems and software engineering -- Software life cycle processes
  - ISO/IEC 15288:2008 - Systems and software engineering -- System life cycle processes
  - Familia de estándares AQAP/PECAL
  - ISO/IEC 15504 – Mejora del Proceso software y Determinación de la Capacidad (SPICE)
  - CMMi – Capability Maturity Model Integration

Gestión de Proyectos

- ISO/IEC 21500:2012 – Guidance on Project management
- PMBOK – Project Management Body of Knowledge

Gobierno Corporativo y Gestión TIC

- UNE ISO/IEC 20000-1:2011 – Tecnología de la información. Gestión del Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio (SGS)
- ITIL – Information Technology Infrastructure Library

- ISO/IEC 38500 – Corporate governance of information technology
- COBIT – A Business Framework for the Governance and Management of Enterprise IT
- ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

Negocio

- ISO 22301:2012 – Societal security – Business continuity management systems --- Requirements
- UNE-ISO 30301-1:2011. Información y Documentación. Sistema de Gestión para los documentos. Parte 1: Requisitos del Sistema de Gestión para los documentos (SGD)
- EFQM – Modelo EFQM de Excelencia:2013
- PCI DSS *(Payment Card Industry Data Security Standard) – Requirements and Security Assessment Procedures*
- Novedades ISO/FDIS 9001:2015 – Quality management systems – Requirements

Criterios de selección

Los estándares y modelos objeto de este estudio se seleccionaron basándose en dos criterios principales:

Estándares y modelos apropiados para las áreas de actividad del Comité CSTIC (Calidad en los Sistemas y Tecnología de la Información y las Comunicaciones). Este criterio llevó a establecer los tres dominios siguientes:

Calidad

Desarrollo de Sistemas

Gobierno Corporativo y Gestión TIC

Mas dos dominios adicionales y que también tuvieran interés para los lectores

Gestión de Proyectos

Negocio

Estándares más requeridos, usados y reconocidos en el mundo TIC y de la Ingeniería de Sistemas y cuyo conocimiento y aplicación entrañaría más dificultad para las PYMES.

Se descartaron, a propósito, algunos estándares por ser muy conocidos y ampliamente desplegados en la industria como ISO 9000, ISO 14000, y también, por no ser específicos de las áreas de trabajo del Comité CSTIC. Si bien en el dominio de Negocio se incluye un apartado para explicar las diferencias entre ISO 9001:2008 e ISO 9001:2013.

Estructura del Modelo de Información

Un objetivo de este estudio ha sido la creación de un modelo de información que describa todos los estándares y modelos de buenas prácticas de forma uniforme con los mismos criterios de evaluación. El modelo de información incluye los siguientes capítulos:

Entidad Emisora

¿Qué entidad(es) ha(n) editado el estándar o modelo?

Disponibilidad

¿Dónde puedo obtener el estándar o modelo?

Clasificación (taxonomía)

¿Este estándar o modelo es internacional o nacional? ¿Es un estándar o una colección de buenas prácticas? ¿Es aplicable a un sector de la industria, a una parte de la organización o área de negocio? ¿Es certificable o no?

Referencia normativa

¿Es un estándar o es una familia de estándares? ¿Hay otros estándares o modelos que son necesarios o potencian los resultados de este estándar o modelo?

Ámbito de aplicación

¿Dónde es aplicable la implementación de este estándar/modelo? ¿Para qué propósito se aplicaría principalmente?

Certificación

¿Es este estándar o modelo certificable o evaluable? ¿Qué organismo puede hacer la certificación/evaluación?

Objetivos del estándar/modelo

¿Cuál es el propósito del estándar o modelo? ¿Cuál es el foco del estándar o modelo: la mejora, una metodología, un marco de gestión?

Agentes facilitadores para su adopción/implementación

¿Por qué debería implementarlo o usarlo? ¿Qué factores hacen interesante o imprescindible la implementación o uso de este estándar/modelo?

Ventaja competitiva y riesgos relacionados con su no implantación o uso

Si implemento el estándar o modelo, ¿Qué ventajas competitivas obtendría la organización? Y si no lo implemento, ¿En qué riesgos podría incurrir?

Reconocimiento/reputación

¿Qué referencias hay de su uso y su implantación? ¿Cuántas organizaciones implementan/usan el estándar/modelo? ¿Cuál es su reputación entre los profesionales?

Directrices sobre su uso/implementación

Este capítulo proporciona una breve descripción, de alto nivel, de los contenidos del estándar/modelo y de cómo debería usarse/implementarse para conseguir el objetivo de la organización. La descripción hace hincapié en como extraer el mayor beneficio basado en la experiencia profesional puesta al servicio de los lectores.

Relación con otros estándares/modelos

¿Hay otros estándares/modelos que tienen relación con éste o complementan/refuerzan las ventajas de su implementación?

Cómo usar esta publicación

El uso de esta publicación va a depender del conocimiento del lector sobre los estándares y modelos de buenas prácticas así como de los objetivos de su organización. Dado que el objetivo del estudio es facilitar la selección de qué estándar o modelo se necesitaría implementar en función de los objetivos empresariales, la mejor forma de usar esta publicación sería:

1. Establecer o identificar qué necesidades y objetivos tiene la organización, es decir, que quiero conseguir o mejorar con un estándar o modelo.
2. Identificar en que área o dominio de interés encaja mi objetivo o necesidad de mejora. Con la ayuda del cuadro de clasificación 1 y del mapa de estándares y modelos de la figura 1, identificar que estándares o modelos podrían ser candidatos.
3. Una vez identificados los posibles estándares/modelos, leer la correspondiente descripción del estándar/modelo fijándose primero en el capítulo **Objetivos del estándar/modelo**, y luego en el capítulo **Agentes facilitadores para su adopción/implementación**. El subcapítulo **Ventaja competitiva y riesgos relacionados con su no implantación o uso***,* nos dará una buena información para la selección final del más idóneo.
4. El capítulo **Directrices sobre su uso/implementación** indica con brevedad, pero haciendo énfasis en los aspectos claves, como implementar el estándar/modelo de la mejor manera y con más éxito.

Otra forma de usar esta publicación sería partiendo de que área o dominio quiero mejorar y con ayuda de los cuadros de clasificación 1 y 2, seleccionar que estándares o modelos tienen impacto en dicha área o dominio.

Cuadro de clasificación 1					
Estándares y Modelos de buenas prácticas	Dominios de Aplicación				
	Calidad	Desarrollo de Sistemas	Gestión de Proyectos	Gobierno Corporativo y Gestión TIC	Negocio
ISO/IEC 12207	☑	☑	☑		
ISO/IEC 15288	☑	☑	☑		
ISO/IEC 15504 (SPICE)	☑	☑	☑		
ISO/IEC 15939	☑		☑		
UNE ISO/IEC 20000				☑	
ISO/IEC 21500			☑		
ISO/IEC 22301 (BS 25999)					☑
ISO/IEC 25010 (SQuaRE)	☑				
ISO/IEC 27001				☑	☑
UNE-ISO 30301-1	☑				
ISO/IEC 38500				☑	☑
Familia AQAP/PECAL	☑	☑	☑		
PCI DSS					☑
MODELOS DE BUENAS PRACTICAS					
CMMi	☑	☑	☑	☑	☑
COBIT	☑	☑	☑	☑	☑
EFQM					☑
ITIL			☑	☑	

PMBOK			☑		

Impacto en los dominios de aplicación

El impacto se mide por la influencia que tiene la implementación o uso del estándar o modelo en las actividades y resultados de cada dominio según la gradación de la tabla siguiente:

Grado	Descripción del grado
4	El estándar o modelo trata en profundidad las actividades más relevantes del dominio de aplicación y los resultados de dichas actividades, indicando tanto lo que se necesita hacer como recomendaciones para conseguirlo.
3	El estándar o modelo trata actividades del dominio de aplicación y los resultados de dichas actividades, pero no con el detalle del nivel superior.
2	El estándar o modelo en cuestión puede ser considerado como un complemento o ayuda para otros estándares pero no trata directamente las actividades del dominio.
1	El estándar o modelo tiene muy poca influencia en las actividades y resultados del dominio.
0	Sin relevancia para el dominio.

Cuadro de clasificación 2					
Estándares y Modelos de buenas prácticas	Dominios de Aplicación				
	Calidad	Desarrollo de Sistemas	Gestión de Proyectos	Gobierno Corporativo y Gestión TIC	Negocio
ISO/IEC 12207	2	4	4	0	1
ISO/IEC 15288	2	4	4	0	1
ISO/IEC 15504 (SPICE)	4	4	4	0	2
ISO/IEC 15939	4	1	3	2	3
UNE ISO/IEC 20000	2	1	0	4	3
ISO/IEC 21500	2	2	4	2	1
ISO/IEC 22301 (BS 25999)	0	0	0	0	4
ISO/IEC 25000 (SQuaRE)	4	2	3	0	2
ISO/IEC 27001	0	0	1	3	4
UNE-ISO 30301-1	4	0	0	0	0
ISO/IEC 38500	2	3	3	4	4
Familia AQAP/PECAL	4	5	4	0	1
PCI DSS	0	0	0	0	2
MODELOS DE BUENAS PRACTICAS					
CMMI	3	4	4	2	4
COBIT	2	3	3	4	4
EFQM	3	2	1	1	4
ITIL	0	0	2	4	2

PMBOK	2	0	4	1	1

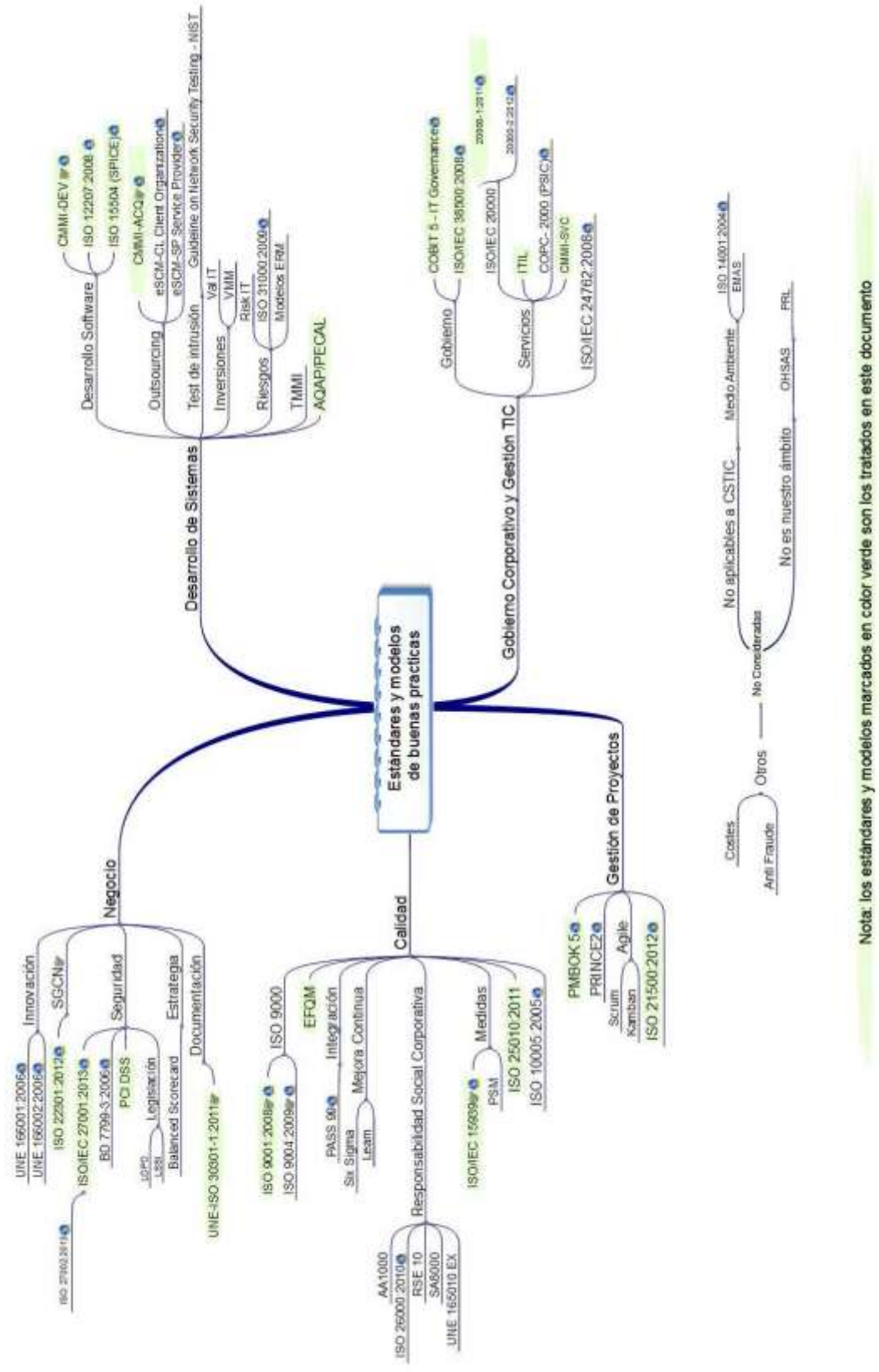

Ilustración 1 Mapa de estándares y Modelos de buenas prácticas

Dominio de la Calidad

ISO/IEC 15939:2007

ISO/IEC 15939:2007 – Systems and software engineering – Measurement process

Entidad Emisora

ISO/IEC 15939:2007 es un estándar ISO y de IEC, elaborado por el grupo de trabajo ISO/IEC JTC 1/SC 7 y se publicó en 2007.

También existe la versión en español UNE-ISO/IEC 15939:2009, idéntica al estándar en inglés, elaborada por el grupo de trabajo AEN/CTN 71 de AENOR que se publicó en 2009.

- **Disponibilidad**

El documento puede comprarse en la web de ISO www.iso.org, tanto en papel como en formato PDF, y en la web de AENOR www.aenor.es en idénticos formatos. Para ver los precios consultar la web respectiva.

- **Clasificación (taxonomía)**

ISO/IEC 15939:2007 es un estándar internacional y nacional.

- **Referencia normativa**
  - ISO/IEC 15939:2007 - Systems and software engineering – Measurement process.
  - UNE-ISO/IEC 15939:2009 – Ingeniería del software y sistemas – Procesos de Medición.
  - PSM (*Practical Software and Systems Measurement*). Iniciativa patrocinada por el Departamento de Defensa y Ejército de EE.UU y fue el embrión de este estándar. PSM (www.psmsc.com) tiene una colección extensa de especificaciones de medidas.
- **Ámbito de aplicación**

Este estándar es aplicable a todo tipo de organizaciones, independientemente de su tamaño, y tiene su aplicación principal en la toma de decisiones objetivas fundamentadas en datos reales y fiables, obtenidos como resultado del proceso de medición especificado.

Puede ser usado en el ámbito de adquisición, tanto por suministradores como por clientes, para abordar necesidades de información en relación a la calidad de un producto, a la capacidad de un proceso, o la ejecución de un proyecto.

Originariamente está desarrollado con enfoque a la Ingeniería de software y sistemas, pero el proceso especificado es genérico y flexible y podría aplicarse en otros ámbitos.

- **Certificación**

Este estándar no es certificable. Sin embargo, cualquier cliente puede exigir la conformidad con este estándar del proceso de medición del suministrador. En ese sentido, las cláusulas normativas serán de obligado cumplimiento.

Por otro lado, su implementación sería fundamental para cumplir con los requisitos de CMM y SPICE relacionados con las áreas de Medición y Análisis, así como para poder demostrar que la organización está en los niveles superiores de madurez en ambos modelos.

Objetivos del estándar

El objetivo del estándar es la descripción de un proceso de medición del software aplicable a todas las disciplinas de desarrollo de software y de gestión de la organización. El proceso se describe en términos de las actividades que se requieren implementar tanto para la especificación de la información requerida, como para la medición y el uso de los resultados del proceso, y el análisis de los datos recogidos para determinar la validez de los resultados obtenidos.

Por otro lado, el propósito del proceso de medición es recoger, analizar y reportar datos que permitan la gestión eficaz de los procesos de la organización y demostrar objetivamente la calidad de los productos que produce, y la ejecución de los proyectos.

La implementación con éxito de este proceso de medición dará como resultado:

- el establecimiento de un compromiso de la organización, sostenido en el tiempo, con la medición
- La identificación de las necesidades de información para la gestión de los procesos técnicos y de gestión

- La identificación y definición de las medidas más apropiadas para satisfacer las necesidades de información identificadas por la organización
- La identificación de las actividades de medición y su planificación
- La obtención de datos como resultado de las actividades de medición los cuales se almacenarán, se analizarán y se interpretarán adecuadamente
- Los datos obtenidos, analizados y validados se usarán para la toma de decisiones y para mejorar objetivamente la comunicación
- La evaluación objetiva de los procesos técnicos y de gestión, así como el propio proceso de medición y el conjunto de medidas de la organización

Agentes facilitadores para su adopción/implementación

Dentro de los agentes facilitadores para su implementación estarían los siguientes:

- La existencia de una cultura de gestión de procesos y de mejora continua soportada por datos objetivos, pues sería difícilmente entendible una organización con una cultura de mejora continua sin el soporte de un proceso de medición.
- La necesidad de implementar el modelo CMMI o el estándar ISO/IEC-15504 (SPICE) especialmente para niveles de madurez altos.
- La necesidad de implementar el estándar ISO/IEC-25000 (SQuaRE)
- Determinación de la capacidad de los procesos de la organización, lo que implica implementar un proceso de medición que proporcione las medidas e indicadores que permitan hacer predicciones fiables, así como estimaciones y presupuestos realistas y una gestión de riesgos eficaz.
- La necesidad de acreditar la conformidad del proceso de medición del suministrador con este estándar requerida por un cliente.
- La implementación adecuada de este estándar es un medio muy potente para reforzar la comunicación entre todos los niveles de la organización y también entre suministradores y clientes.
- Es un proceso flexible y dirigido por las necesidades de información de la dirección, de los empleados, y de los clientes.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

La ventaja principal se deriva del hecho de implementar un proceso basado en las mejores prácticas de medición del software de la industria y del Departamento de Defensa de los EEUU en la aceptación de los productos software que adquiere.

Su implementación proporciona a los jefes de proyecto, y a la alta dirección, con la información objetiva necesaria para tomar decisiones objetivas y fundamentadas para poder cumplir con éxito los objetivos técnicos, de calidad, coste y plazos de entrega de los proyectos. Todo ello reforzado porque la capacidad de los procesos de la organización es conocida y permite predecir resultados dentro de los márgenes que el control de procesos establece. Las estimaciones y predicciones son muy fiables, y los riesgos de incumplimientos de objetivos se minimizan.

El principal riesgo, derivado de su no implantación, radica en la ausencia de un proceso de medición que asegure que los productos de información (medidas e indicadores) en uso en la organización estén dirigidos a satisfacer las necesidades de información de la organización. La consecuencia es que o bien los datos no son relevantes, o los usuarios no confían en ellos. Su ausencia lleva consigo también que las medidas e indicadores se vean como una carga costosa e innecesaria, y no como la ayuda inigualable para la toma de decisiones.

Reconocimiento/reputación

Este estándar es usado principalmente en compañías que desarrollan software para el Departamento de Defensa y el Ejército de EE.UU. ya que éstos requieren la conformidad con PSM o con este estándar.

Directrices sobre su uso/implementación

Este estándar define un proceso de medición que consta de cuatro actividades, dentro de las cuales identifica unas tareas, y para estas tareas especifica las cláusulas que sí son normativas para implementar con éxito el proceso.

El esquema y el flujo de actividades y de información se muestran gráficamente en la figura siguiente:

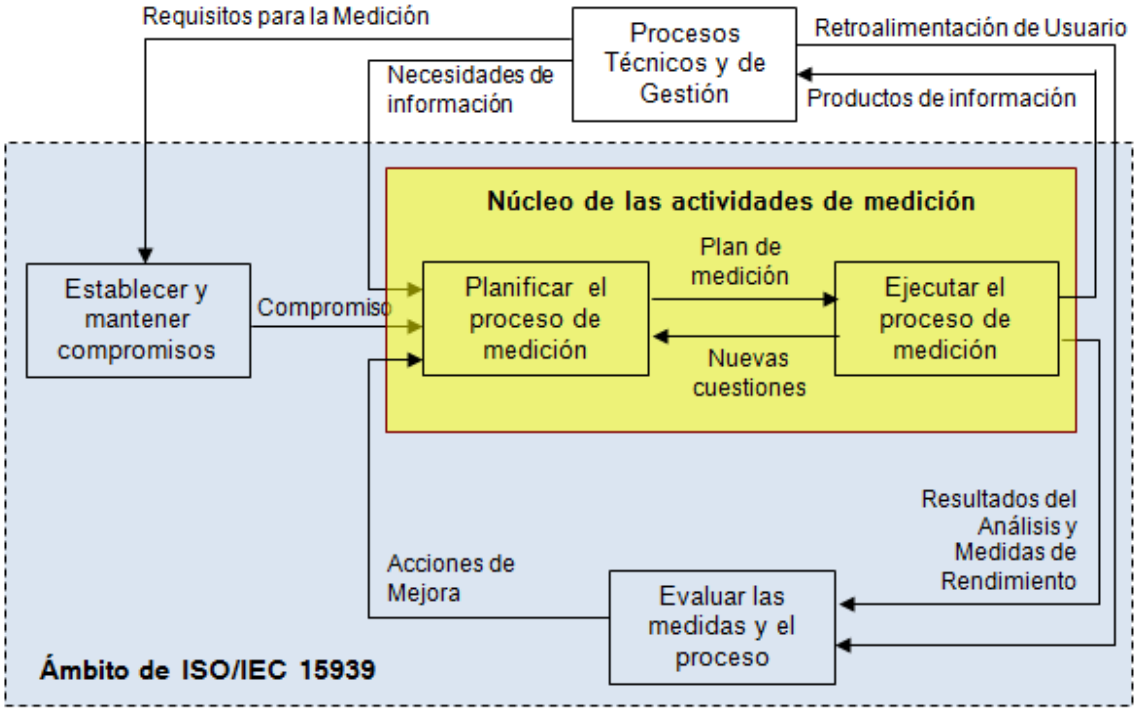

Ilustración 2 Flujo de actividades ISO/IEC 15939

Actividad 1. Establecer y mantener en el tiempo compromisos con la medición

En esta actividad la principal responsabilidad está en la dirección. Es una actividad de liderazgo, pues la dirección se compromete y compromete al personal con el proceso de medición y con el uso de las medidas para tomar decisiones objetivas. Además, la dirección tiene que asignar recursos a estas actividades y asignarles autoridad y responsabilidad para llevar a cabo las tareas requeridas por el proceso.

Actividad 2. Planificar el proceso de medición

En esta actividad, se deben identificar las partes de la organización implicadas tanto en la selección de las medidas relevantes como en la interpretación de los resultados. Para la selección de las medidas se sigue un procedimiento que consiste en:

5. Identificar aquello que necesitamos medir, es decir, que necesidades de información tenemos en los distintos niveles de la organización (dirección, proyectos, productos, procesos, clientes).

6. Priorizar las necesidades de información, pues pueden ser muchas, complejas, y no tener suficientes recursos para llevarlas a cabo.
7. Documentar y comunicar a los individuos asignados en la actividad 1, las necesidades de información que deben ser satisfechas.
8. Identificar qué medidas pueden satisfacer las necesidades de información y especificarlas apropiadamente (nombre, unidad de medida, método de medición, representación grafica, análisis e interpretación, y conexión con la correspondiente necesidad de información que satisface). PSM puede ser de ayuda en este apartado.
9. Definir los procedimientos de recolección de datos, análisis, almacenamiento, verificación y presentación de los productos de información (medidas e indicadores) que darán satisfacción a las necesidades de información.
10. Definir los criterios de evaluación de los productos de información y del proceso de medición.

Para que esta actividad se realice apropiadamente, se debe proporcionar y desplegar la tecnología adecuada para apoyar el proceso.

Actividad 3. Ejecutar el proceso de medición

Este es el punto clave del proceso, pues todas las tareas planificadas en la actividad 2 deben estar integradas dentro de las actividades técnicas y de gestión y no constituir un esfuerzo adicional que haga fracasar el proceso. Para ello debe facilitarse la recolección de datos, su almacenamiento, tratamiento y análisis para su interpretación y presentación como productos de información revisados y aprobados para el uso por los usuarios de las medidas.

Actividad 4. Evaluación de las medidas y del proceso

Esta actividad se centra en la evaluación tanto de la adecuación de las medidas seleccionadas como del proceso de medición en su conjunto. Los productos de información se evalúan frente a los criterios especificados y se determinan si son adecuados al propósito que sirven o si deben ser modificados o suprimidos. Igual se debe hacer con el proceso de medición para determinar sus fortalezas y sus debilidades.

De la evaluación de ambos, medidas y proceso de medición, se derivaran planes de mejora y lecciones aprendidas que serán comunicadas a la organización.

Relación con otros estándares/modelos

ISO/IEC 12207 Systems and software engineering – Software life cycle processes

ISO/IEC 15288 Systems and software engineering – System life cycle processes

ISO/IEC 15504 Information technology – Process assessment

ISO/IEC 21500 Guidance on Project Management

ISO/IEC 25000 Software engineering – Software product Quality Requirements and Evaluation (SQuaRE)

PSM Practical Software and Systems Measurement (*www.psmsc.com*)

CMMI Capability Maturity Model Integration

ISO/IEC 25010:2011

ISO/IEC 25010:2011 – Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models

Entidad Emisora

ISO/IEC 25010:2011 System and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models es un estándar de ISO y de IEC elaborado por el grupo de trabajo ISO/IEC JTC 1/SC 7 y publicado en 2011.

- **Disponibilidad**

El documento puede adquirirse en la web de ISO www.iso.org al precio de 138 CHF (es decir, unos 115€), tanto en papel como en formato PDF. Únicamente existe en inglés.

Clasificación (taxonomía)

Es un estándar internacional cuyo campo de aplicación es la calidad del producto software.

- **Referencia normativa**

ISO/IEC 25010:2011 es un estándar encuadrado en la familia ISO 25000, conjunto de normas denominado SQuaRE (*Software product Quality Requirements and Evaluation*)

Esta serie está sustituyendo paulatinamente los siguientes grupos de normas:

- Serie ISO/IEC 9126 *(Software engineering -- Product quality)* con las siguientes normas:
  - ISO/IEC 9126-1:2001 *(Software engineering -- Product quality – Part 1: Quality model)*: estándar no vigente remplazado por ISO/IEC 25010:2011

- ISO/IEC 9126-2:2003 (Software engineering -- Product quality – Part 2: External metrics)
- ISO/IEC 9126-3:2003 (Software engineering -- Product quality – Part 3: Internal metrics)
- ISO/IEC 9126-4:2004 (Software engineering -- Product quality – Part 4: Quality in use metrics)

– Serie ISO/IEC 14598 (Information technology – Software product evaluation)

- ISO/IEC 14598-1:1999 (Information technology -- Software product evaluation – Part 1: General overview): estándar no vigente remplazado por ISO/IEC 25040:2011
- ISO/IEC 14598-2:2000 (Information technology -- Software product evaluation – Part 2: Planning and management): estándar retirado: revisado y confirmado en 2011
- ISO/IEC 14598-3:2000 (Information technology -- Software product evaluation – Part 3: Process for developers): estándar no vigente remplazado por ISO/IEC 25041:2012
- ISO/IEC 14598-4:1999 (Information technology -- Software product evaluation – Part 4: Process for acquirers): estándar no vigente remplazado por ISO/IEC 25041:2012
- ISO/IEC 14598-5:1998 (Information technology -- Software product evaluation – Part 3: Process for evaluators): estándar no vigente remplazado por ISO/IEC 25041:2012
- ISO/IEC 14598-6:2001 (Information technology -- Software product evaluation – Part 6: documentation of evaluation modules): estándar revisado y confirmado en 2008

- **Ámbito de aplicación**

Este estándar es aplicable a todo tipo de organizaciones, independientemente de su tamaño, y tiene como finalidad principal la mejora de la calidad del producto software mediante la implementación de las siguientes características:

Adecuación funcional	grado en el que un producto o sistema proporciona las funciones que satisfacen las necesidades tanto implícitas como las establecidas cuando se usa bajo determinadas condiciones

Eficiencia en el funcionamiento	rendimiento en relación con la cantidad de recursos utilizados en unas condiciones establecidas
Compatibilidad	grado en el que un producto, sistema o componente puede intercambiar información con otros productos, sistemas o componentes, y/o desempeñar las funciones previstas, compartiendo el mismo entorno de hardware o software
Usabilidad	grado en el que un producto o sistema puede ser utilizado por usuarios específicos para lograr los objetivos establecidos con eficacia, eficiencia y satisfacción en un determinado contexto de uso
Fiabilidad	grado en el que un sistema, producto o componente realiza determinadas funciones bajo condiciones especificadas durante un período de tiempo establecido
Seguridad	grado en el que un producto o sistema protege los datos y la información, de forma que las personas, otros productos u otros sistemas tengan el acceso a los datos adecuado de acuerdo a su tipo y nivel de autorización
Mantenibilidad	grado de eficacia y eficiencia con las que un producto o sistema puede ser modificado por los responsables del mantenimiento
Portabilidad	grado de eficacia y eficiencia con el cual un sistema, producto o componente puede ser transferido de un hardware, software, o entorno de uso u operacional a otro.

- **Certificación**

El estándar ISO/IEC 25010:2011 es certificable. Hasta ahora únicamente AENOR ha emitido un certificado asociado a una de las características de calidad establecidas: Mantenibilidad.

Objetivos del estándar/modelo

El principal objetivo de esta serie es disponer de un conjunto de normas lógicamente organizado, unificado y mejorado que cubra los dos grandes procesos de especificación de requisitos de calidad de software y evaluación de la calidad del software y de los sistemas informáticos, siendo ambos soportados por un proceso de medición de la calidad del software y de los sistemas.

Además:

- Establece criterios para la especificación de los requisitos de calidad del software y de los sistemas informáticos
- Incluye un modelo desarrollado en dos partes que permite alinear las definiciones de calidad del cliente con los atributos del proceso de desarrollo.
- Facilita y recomienda unas medidas de la calidad del producto software y de los sistemas que pueden ser utilizadas tanto por los desarrolladores como por los adquirientes y evaluadores del producto.

Agentes facilitadores para su adopción/implementación

Hasta ahora la mayoría de las actividades de calidad en relación al software se han centrado en la mejora de los procesos de desarrollo pero esto no garantiza la calidad del producto obtenido sino más bien su homogeneidad y su uniformidad.

Esta norma, sin embargo, se centra en facilitar los requisitos para poder medir la calidad del producto software como tal.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

La principal ventaja buscada al implantar este estándar sería la mejora de la calidad del software desarrollado lo que supondría:

- Disponer de criterios para poder determinar los niveles de calidad deseables y requeridos lo que permite establecer los niveles de servicio adecuados tanto para los desarrolladores como para los usuarios.
- Detección de errores durante el desarrollo lo que permite reducir el número de errores en producción y facilita el mantenimiento.
- Prever la calidad de los resultados de forma que se puedan planificar y controlar los recursos y los plazos.
- Mejora de la integración con otros sistemas en producción.

Todo ello debería suponer una ventaja frente a los competidores al permitir mejoras en plazos y en uso de recursos lo que supone un impacto positivo en tanto en la calidad como en el precio del producto.

Reconocimiento/reputación

Este estándar se encuentra en una fase muy temprana de implantación habiéndose emitido únicamente un certificado por AENOR en España en el año 2013 para la característica de mantenibilidad.

No se ha emitido ningún otro certificado hasta ahora.

Directrices sobre su uso/implementación

La implementación se realiza mediante un proceso de varias fases:

11. Establecer los requisitos de la evaluación
12. Especificar la evaluación
13. Diseñar la evaluación
14. Realizar la evaluación
15. Concluir la evaluación

La familia ISO 25000 define los modelos y los procesos para medir la calidad pero no establece una correlación entre las métricas y los umbrales requeridos para identificar el nivel de calidad del producto software.

Por ello, las pruebas las realiza un laboratorio acreditado para esta actividad que define un modelo y un proceso de calidad alineado con el estándar ISO 25000, y además un conjunto de propiedades de calidad medibles sobre el código fuente del producto software en un entorno automatizado.

Relación con otros estándares/modelos

ISO/IEC 25010:2011 es un estándar encuadrado en la familia ISO 25000, conjunto de normas denominado SQuaRE (*Software product Quality Requirements and Evaluation*) que sustituyen a la series ISO/IEC 9126 e ISO/IEC 14598.

En la figura siguiente se representan los grupos principales que la forman denominados división:

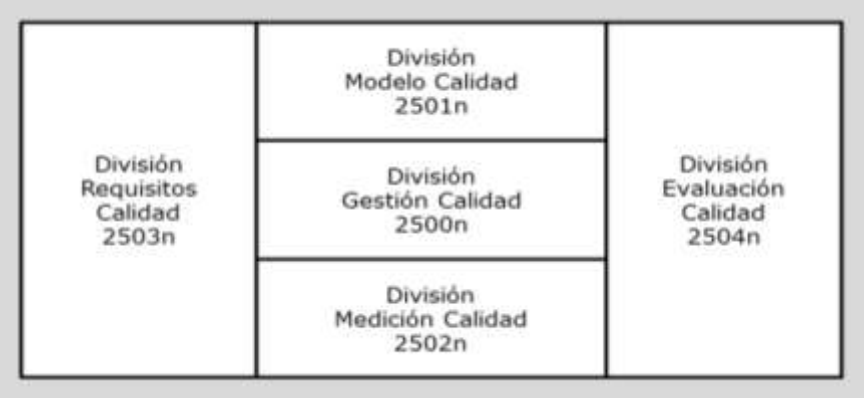

Ilustración 3 División Extendida 25050 - 25099

- ISO/IEC 2500n: define los modelos, términos y referencias comunes que aplican a toda la familia.
- ISO/IEC 2501n: presenta modelos de calidad detallados para el producto software y para los sistemas, para la calidad en uso y los datos.
- ISO/IEC 2502n: define un modelo de referencia de medida de calidad del producto software y del sistema.
- ISO/IEC 2503n: sirve de ayuda para la especificación de requisitos de calidad.
- ISO/IEC 2504n: facilita requisitos, recomendaciones y guías para la evaluación del producto.
- ISO/IEC 25050-25099: asignada para contener normas relacionadas con dominios de aplicaciones específicas que complementen la familia SQuaRE.

Este estándar está destinado a ser utilizado de forma conjunta con el resto de los estándares de la serie SQuaRE (ISO/IEC 25000 a ISO/IEC 25099) y con las normas ISO/IEC 14598 hasta que sean totalmente reemplazadas por la serie ISO/IEC 2504n.

En la tabla que se presenta a continuación aparecen los estándares desarrollados pertenecientes a esta familia:

Código	Título
ISO/IEC 25000:2014	Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Guide to SQuaRE
ISO/IEC 25001:2014	Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Planning and management
ISO/IEC 25010:2011	Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models
ISO/IEC 25012:2008	Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Data quality model
ISO/IEC 25020:2007	Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Measurement reference model and guide
ISO/IEC 25021:2012	Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Quality measure elements
ISO/IEC 25030:2007	Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Quality requirements
ISO/IEC 25040:2011	Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Evaluation process
ISO/IEC 25041:2012	Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Evaluation guide for developers, acquirers and independent evaluators
ISO/IEC 25045:2010	Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Evaluation module for recoverability
ISO/IEC 25051:2014	Software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing

Código	Título
ISO/IEC 25062:2006	Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Common Industry Format (CIF) for usability test reports
ISO/IEC 25063:2014	Systems and software engineering -- Systems and software product Quality Requirements and Evaluation (SQuaRE) -- Common Industry Format (CIF) for usability: Context of use description
ISO/IEC 25064:2013	Systems and software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Common Industry Format (CIF) for usability: User needs report
ISO/IEC 26513:2009	Systems and software engineering - Requirements for testers and reviewers of user documentation
ISO/IEC TR 25060:2010	Systems and software engineering -- Systems and software product Quality Requirements and Evaluation (SQuaRE) -- Common Industry Format (CIF) for usability: General framework for usability-related information

Domino de Desarrollo de Sistemas

ISO/IEC 12207:2008

ISO/IEC 12207:2008 – Systems and software engineering -- Software life cycle processes

Entidad Emisora

ISO/IEC 12207:2008 es un estándar ISO y de IEC, publicado por primera vez en 1995. Es el estándar para los procesos de ciclo de vida del software de la organización ISO.

- **Disponibilidad**

El documento puede comprarse en la web de ISO www.iso.org al precio de 224 CHF (a fecha de publicación de la ficha), y en AENOR www.aenor.es al precio de 192,10 € (fecha de publicación de la ficha). Ambas normas se pueden consultar en la biblioteca de AENOR.

El estándar UNE 71044:1999 – Ingeniería de sistemas y del Software. Procesos del ciclo de vida del SW, es la traducción de ISO/IEC 12207:1995. El estándar UNE-71044 puede comprarse en AENOR www.aenor.es al precio de 48,59 €.

Clasificación (taxonomía)

El estándar ISO/IEC 12207 es un estándar internacional. Es el estándar para los procesos de ciclo de vida del software de la organización ISO. Aplica, como su título indica, a los procesos del ciclo de vida del software así como a la ingeniería del software y de sistemas. No era un estándar certificable, aunque desde su publicación se ha comenzado a certificar.

- **Referencia normativa**

Esta del estándar ha sufrido hasta la edición actual de 2008 las siguientes modificaciones:

- ISO/IEC 12207:1995. Primera publicación.
- ISO/IEC 12207:1995/Amd 1:2002. Primera modificación.

- ISO/IEC 12207:1995/Amd 2:2004. Segunda modificación.
- ISO/IEC 12207:2008. Publicación actual.

IEEE Std 12207™-2008– Systems and software engineering — Software life cycle processes

- **Ámbito de aplicación**

Este estándar es aplicable a todo tipo de organizaciones, independientemente de su tamaño, y tiene su aplicación principal en los siguientes aspectos:

- En la adquisición de sistemas o productos software
- En los servicios necesarios para el suministro, desarrollo, operación, mantenimiento y disposición de productos o porciones de productos software, tanto si son ejecutados interna o externamente a una organización.

- **Certificación**

Se está procediendo a certificar conjuntamente ISO 15504- Proceso de evaluación del Software/ ISO 12207:2008- Proceso del ciclo de vida Software.

Objetivos del estándar

Proporcionar un marco de referencia común para los procesos del ciclo de vida del SW.

Este estándar internacional también proporciona un proceso que puede emplearse para definir, controlar y mejorar los procesos del ciclo de vida del software.

Agentes facilitadores para su adopción/implementación

Un agente facilitador para la implantación del estándar ISO 12207 es la obligación en algunas certificaciones, como por ejemplo la PECAL 160, que englobaba los estándares ISO 12207 e ISO 9001.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

El hecho de ser obligatoria su implantación para obtener ciertas certificaciones hace que el no implantarlo descalifique directamente a la empresa que no inicia su implantación, puesto que no podrá acceder a la certificación correspondiente.

Por otro lado si la empresa no necesita la certificación en cuestión, el implantar este estándar proporciona un marco de referencia a la hora de crear y gestionar el SW, para "hablar el mismo lenguaje".

Además este estándar contempla un conjunto exhaustivo de procesos que cada organización puede adecuar a su sistema, proyecto o aplicación concreta e incluso para un SW independiente y/o empotrado en otro.

Como posibles riesgos de no usar e implementar esta norma podríamos indicar un cierto caos en los procesos de la organización al no alinearse con los en ella indicados y que proporcionan un mapa de los necesarios y como consecuencia de falta de procesos o falta de alineación con los indicados por la norma, una ausencia de actividades importantes que garanticen la calidad de los productos. Otro riesgo de no usarla ni implantara sería la ausencia de un lenguaje común con la industria del software que es precisamente una de las ventajas que da la adopción de este estándar.

Reconocimiento/reputación

A fecha 15/01/2010 había en el ámbito español, 16 empresas certificadas en ISO 12207:2008- Proceso del ciclo de vida Software (fuente INTECO). Por ser una certificación relativamente nueva se supone que el número de certificaciones crecerá, no obstante el uso está ampliamente extendido entre todos los profesionales del sector TIC.

Directrices sobre su uso/implementación

Para iniciar la implementación de esta norma se debe tener claro a que parte de la organización se quiere aplicar, la norma da la posibilidad de que sea incluso a nivel de proyecto o aplicación. La dinámica que yo aconsejo es que no se creen procesos artificiales sino que los existentes se adecuen a lo requerido por la norma y se les de la formalidad exigida por esta.

Se debe hacer un ejercicio de fraccionamiento de los procesos en actividades y estás a su vez en tareas. Se deberían asignar propietarios a los procesos que serían los responsables de asegurar su alineamiento con las directrices marcadas por la organización y comunicar las acciones a emprender para corregir posibles desviaciones.

A continuación se indican una serie de consideraciones a tener en cuenta durante la implementación y posterior uso de la norma:

Se trata de un estándar que está orientado para ser usado en situaciones en las que haya en principio dos partes, ya sean internas o externas a la misma organización (si es por una sola parte será como auto imposición). Bien mediante acuerdo informal o contrato con responsabilidades legales.

No está indicado para software preexistente (COTS), salvo que forme parte de otro SW.

Este estándar contiene un conjunto de procesos principales, procesos de menor nivel, actividades y tareas pensadas para ser adaptadas a los proyectos SW. El proceso de adaptación consiste en la eliminación de los procesos, actividades y tareas no aplicables.

Se considera cumplimiento con un proceso o actividad cuando todas las tareas se llevan a cabo según se especifique en el contrato.

En este estándar no se especifican los detalles de cómo implementar o llevar a cabo las actividades y tareas incluidas en los procesos.

Así mismo no identifica el nombre, el formato o el contenido explicito de la documentación a generar, ni el modelo del ciclo de vida concreto para el desarrollo del SW (producto o servicio).

Se debe documentar como excepción cualquier incumplimiento autorizado a este estándar.

Se debe aclarar que una excepción puede disminuir la percepción de conformidad con este estándar por parte del cliente.

Las listas de tareas dadas en este estándar son ejemplos.

Este estándar agrupa los procesos en procesos del ciclo de vida del sistema, estos a su vez se subdividen en procesos contractuales (con clientes, compra suministros), organizativos que posibilitan la realización de los proyectos (modelo de ciclo de vida, infraestructura, etc.), propios de la ejecución de los propios proyectos (planificación, evaluación, gestión, etc.), procesos técnicos (análisis de requisitos, diseño, integración, etc.) y procesos del ciclo de vida del SW, éstos a su vez se subdividen en procesos de implementación del SW (análisis, diseño, integración, etc.), procesos de soporte del SW (documentación, gestión de la configuración, auditorias, etc.) y procesos para el re-uso del SW.

El estándar contiene así mismo un proceso de adaptación en el anexo-A y el PRM (modelo de referencia de procesos), conforme a ISO/IEC 15504-2, con sus 6 niveles de capacidad en el anexo B (ambos normativos).

Los procesos, actividades y tareas de este estándar internacional se pueden aplicar solos o en conjunción con los del estándar ISO/IEC 15288. La aplicación de este estándar con referencias al estándar ISO/IEC 15288 dependerá de la entidad, dentro del proyecto, de la parte HW y será decidido por la organización.

El anexo D del estándar muestra una alineación entre los procesos de ISO/IEC 12207 y de ISO/IEC 15288.

Relación con otros estándares/modelos

El estándar ISO/IEC 12207 tiene relaciones con otros estándares tales como los que se indican a continuación:

- ISO/IEC 2382-1:1993- Tecnología de la información. Vocabulario. Parte I: Términos fundamental. (revisada y confirmada en 2010)
- ISO /IEC 2382-20:1990- Tecnología de la Información. Vocabulario. Parte 20: Desarrollo de sistemas. (revisada y confirmada en 2010)
- UNE-EN ISO 9000:2005 - Sistemas de gestión de la calidad. Fundamentos y vocabulario. (ISO 9000:2005).
- UNE-EN ISO 9001:2008 - Sistemas de gestión de la calidad. Requisitos. (ISO 9001:2008) Esta versión del estándar de referencia no está referenciada originalmente en la versión analizada, por ser posterior.
- ISO/IEC 25010:2011 - Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models. Esta versión del estándar de referencia no está referenciado originalmente en la versión analizada (ISO/IEC 9126-1:2001), por ser posterior.
- IEEE Std 1517-1999, IEEE Standard for Information Technology—Software Life Cycle Processes—Reuse Processes.
- IEEE/EIA 12207.0-1996, Industry Implementation of International Standard ISO/IEC 12207:1995 Standard for Information Technology — Software Life Cycle Processes.

- UNE-EN ISO 9004:2009, Gestión para el éxito sostenido de una organización. Enfoque de gestión de la calidad. (ISO 9004:2009) Esta versión del estándar de referencia no está referenciado originalmente en la versión analizada, por ser posterior.
- ISO 10007:2003 Quality management systems — Guidelines for configuration management.
- ISO 13407:1999, Ergonomics — Ergonomics of human-system interaction — Human-centred design process for interactive systems.
- ISO 9241-11:1998, Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability.
- ISO/IEC TR 9294:2005, Information technology — Guidelines for the Management of Software Documentation.
- ISO 13407:1999, Ergonomics — Ergonomics of human-system interaction — Human-centred design process for interactive systems.
- ISO/IEC 14764:2006, Software Engineering — Software life cycle processes — Maintenance.
- ISO/IEC TR 15271:1998, Software Engineering — Software life cycle processes — Guide for ISO/IEC 12207 (Software Life Cycle Processes).
- ISO/IEC 15288:2008, Systems Engineering — System life cycle processes.
- ISO/IEC/IEEE 15289:2011 Systems and software engineering -- Content of life-cycle information products (documentation)
- ISO/IEC 15504: (all parts), Information Technology — Process Assessment.
- ISO/IEC 15939:2007, Software and System Engineering — Measurement.
- ISO/IEC 16085:2006, System and Software Engineering — Life Cycle Management — Risk management.

NOTA.- Las normas posteriores a la edición de la ISO/IEC 12207 se han incluido porque han sustituido a las inicialmente referenciadas en ella.

ISO/IEC 15288:2008

ISO/IEC 15288:2008 – Systems and software engineering -- System life cycle processes

Entidad Emisora

ISO/IEC 15288:2008 es un estándar de ISO y de IEC para describir el ciclo de vida de sistemas[1], más concretamente de los procesos que lo integran. La primera edición se publicó en 2002. La segunda edición se publicó en 2008, siendo la actualmente en vigor.

- **Disponibilidad**

El documento puede comprarse en la web de ISO www.iso.org al precio de 178 CHF (a fecha de publicación de la ficha).

Clasificación (taxonomía)

El estándar ISO/IEC 15288 es un estándar internacional. Es el estándar para los procesos de ciclo de vida de sistemas, si bien aplica indistintamente a los procesos del ciclo de vida de sistemas y a la ingeniería de sistemas en general. Este estándar es no certificable.

- **Referencia normativa**

Los siguientes documentos son indispensables para la aplicación de este estándar:

- ISO/IEC 12207:2008, Systems and software engineering – Software life cycle processes.
- ISO/IEC 15504-2:2003, Information technology -- Process assessment -- Part 2: Performing an assessment.

- **Ámbito de aplicación**

[1] Se refiere a los sistemas creados por el hombre.

Este estándar es aplicable a todo el ciclo de vida de sistemas, incluyendo la concepción, el desarrollo, la producción, la utilización, el soporte y la retirada de los sistemas. Asimismo es aplicable a la adquisición y el suministro de los sistemas, tanto si se lleva a cabo internamente o externamente a la propia organización. Los procesos del ciclo de vida de este estándar pueden ser aplicados concurrentemente, iterativamente y recursivamente al sistema y a sus elementos.

Existe una amplia variedad de sistemas, en función de su propósito, dominio de aplicación, complejidad, tamaño, innovación, adaptabilidad, cantidad, localización, vida útil y evolución. Este estándar describe los procesos que comprende el ciclo de vida de cualquiera de estos tipos de sistemas. Por consiguiente, aplica a sistemas únicos, a sistemas producidos en serie y a sistemas adaptables. Asimismo aplica a sistemas independientes o autónomos y a sistemas que están embebidos o integrados en otros sistemas mayores, más complejos y completos.

Este estándar proporciona un modelo de referencia de procesos, caracterizado en términos del objetivo y de los resultados de cada proceso, que suponen el desempeño satisfactorio de las actividades que abarcan. Por consiguiente este estándar puede ser utilizado como un modelo de referencia para soportar la evaluación de procesos según se especifica en ISO/IEC 15504-2:2003.

El Anexo B de este estándar proporciona información acerca del uso de los procesos del ciclo de vida del sistema como un modelo de referencia de procesos. Por su parte, el Anexo C describe las piezas o elementos del proceso para su uso en el modelo de referencia de procesos.

- **Certificación**

Este estándar es no certificable.

En cuanto a la declaración de conformidad con respecto a este estándar, es posible hacerlo en base únicamente a las dos fórmulas siguientes:

- *Full conformance*. Se define el conjunto de procesos para los cuales se desea proclamar la conformidad.
- La *Full conformance* se logra si se demuestra que todos los requisitos de todos los procesos del conjunto definido han sido satisfechos, utilizando los resultados de los procesos como evidencia.
- *Tailored conformance*. Se define el conjunto de procesos para los cuales se desea proclamar la conformidad. Se adaptan (se excluyen o se modifican) las cláusulas del estándar que sean necesarias para esos procesos, siguiendo los términos indicados en el Anexo A del estándar.

- La *Tailored conformance* se logra si se demuestra que todas las cláusulas así adaptadas de todos los procesos del conjunto definido han sido satisfechas, utilizando los resultados de los procesos como evidencia.

Objetivos del estándar

Este estándar establece un marco de trabajo común para describir el ciclo de vida de sistemas. Define un conjunto de procesos y terminología asociada. Estos procesos pueden ser aplicados en cualquier nivel en la jerarquía de la estructura de un sistema. Los conjuntos seleccionados de estos procesos pueden ser aplicados a través del ciclo de vida para gestionar y llevar a cabo las etapas del ciclo de vida de un sistema. Esto se consigue mediante la involucración de todas las partes interesadas, con el fin último de alcanzar la satisfacción del cliente.

Este estándar proporciona asimismo procesos que soportan la definición, el control y la mejora de los procesos del ciclo de vida utilizados dentro de una organización o de un proyecto. Las organizaciones y los proyectos pueden utilizar estos procesos del ciclo de vida para la adquisición y el suministro de los sistemas.

Este estándar afecta a sistemas que pueden estar configurados por uno o más de los siguientes elementos: hardware, software, datos, personas, procesos (es decir, procesos para proporcionar servicios a los usuarios), procedimientos (es decir, instrucciones para los operadores), instalaciones, materiales y entidades naturales.

Si un elemento del sistema es software, los procesos del ciclo de vida documentados en ISO/IEC 12207:2008 pueden ser utilizados para implementar ese elemento del sistema.

ISO/IEC 15288:2008 y ISO/IEC 12207:2008 están armonizados para utilización concurrente en un único proyecto o en una única organización.

Así pues, el propósito de este estándar es proporcionar un conjunto definido de procesos para facilitar la comunicación entre adquiridores, suministradores y otros participantes en el ciclo de vida de sistemas.

Los procesos de este estándar pueden ser utilizados como base en el establecimiento de los entornos del negocio, como por ejemplo métodos, procedimientos, técnicas, herramientas y personal debidamente formado.

Agentes facilitadores para su adopción/implementación

Este estándar no es certificable por sí mismo. Sin embargo, desde su origen, se ha puesto especial interés en mantenerlo armonizado con el estándar ISO 12207. Es por ello que en cierta manera los agentes facilitadores de ISO 12207 se pueden considerar asimismo agentes facilitadores de ISO 15288, el cual extiende el punto de interés desde los sistemas software a todo tipo de sistemas, pero conservando el fundamento y la terminología de los procesos del ciclo de vida de sistemas.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

Entre los beneficios que aporta la aplicación de este estándar se encuentran los siguientes:

- La ingeniería de sistemas y la gestión de sistemas se enfocan en el ciclo de vida completo de sistemas: el ciclo de vida de sistemas es modelado, y los sistemas se construyen a partir de experiencia probada y de lecciones aprendidas.
- Proporciona un enfoque holístico a la ingeniería de sistemas (software, hardware, datos, personas, procesos, procedimientos, recursos/medios, documentos, entidades naturales).
- Proporciona un marco de trabajo de procesos que es fácil de adaptar para cumplir las necesidades de un proyecto o de una organización, y reducir los riesgos del desarrollo.
- Proporciona la base para mejorar los siguientes aspectos: la calidad del producto, la productividad, la integración entre todos los actores participantes, y la satisfacción del cliente.
- Proporciona un mejor fundamento para el crecimiento y la realización de mejoras en los productos.

Reconocimiento/reputación

Según la propia ISO, este estándar ISO/IEC 15288 puede tener un impacto considerable en el mundo de los negocios, siguiendo los pasos de estándares como ISO 9000. Así como los estándares ISO 9000 han destilado las características esenciales de la gestión de la calidad en un conjunto de requisitos genéricos que cualquier organización puede utilizar en su beneficio, ISO/IEC 15288 ofrece una cartera de procesos genéricos para la gestión óptima de todas las etapas del ciclo de vida de cualquier producto o servicio, en cualquier sector.

Los principios y las prácticas que recoge ISO/IEC 15288 pueden aplicarse en todos los sectores de la industria. De hecho, son bien conocidos por las comunidades aeroespacial y de defensa, están siendo aplicados en industrias asociadas con el transporte y la energía, y están empezando a influenciar aspectos técnicos de servicios a la sociedad en áreas como la atención sanitaria y el orden público. En un futuro previsible, los enfoques descritos en este estándar llegarán a estar extendidos en toda la industria.

Directrices sobre su uso/implementación

Este estándar puede ser utilizado en uno o más de los siguientes modos:

- *Por una organización*: para ayudar a establecer un entorno de procesos deseados. Estos procesos pueden estar soportados por una infraestructura de métodos, procedimientos, técnicas, herramientas y personal formado. La organización puede entonces emplear este entorno para llevar a cabo y gestionar sus proyectos a través de las etapas de su ciclo de vida. En este modo este estándar se utiliza para evaluar la conformidad de este entorno establecido así declarado con respecto a sus provisiones.
- *Por un proyecto*: para ayudar a seleccionar, estructurar y emplear los elementos de un entorno establecido para proporcionar productos y servicios. En este modo este estándar se utiliza en la evaluación de la conformidad del proyecto con respecto al entorno establecido así declarado.
- *Por un adquiriente y un suministrador*: para ayudar a desarrollar un acuerdo en relación a procesos y actividades. Mediante el acuerdo, se seleccionan, negocian, acuerdan y realizan los procesos y actividades a llevar a cabo a partir de los identificados en este estándar. En este modo este estándar se utiliza como guía en el desarrollo del acuerdo.
- *Por asesores de procesos*: para servir como modelo de referencia de procesos a utilizar en la realización de evaluaciones de procesos que puedan ser utilizadas para soportar la mejora de los procesos de una organización.

Relación con otros estándares/modelos

Los principales estándares relacionados con ISO/IEC 15288:2008 son los siguientes:

- ISO/IEC 12207:2008, Systems and software engineering – Software life cycle processes.
- ISO/IEC TR 24748:2011, Systems and software engineering – Life cycle management (multiple parts).

- ISO/IEC TR 19760:2003, A Guide for the application of ISO/IEC 15288 System life cycle processes.
- ISO/IEC 15504:2004, Information Technology – Process assessment (multiple parts).
- IEEE Std 1220-2005, IEEE Standard for Application and Management of the Systems Engineering Process.
- IEEE Std 1228-1994, IEEE Standard for Software Safety Plans.
- IEEE Std 1233-1998 Edition (R2002), IEEE Guide for Developing System Requirements Specifications.
- IEEE Std 1362-1998, IEEE Guide for Information Technology – System Definition – Concept of Operations (ConOps Document).
- IEEE Std 1471-2000, IEEE Recommended Practice for Architectural Description for Software-Intensive Systems.

Familias de estándares AQAP / PECAL

Entidad Emisora

La Familia de estándares AQAP / PECAL está constituida por un conjunto complementario y casi idéntico de dos grupos o familias de estándares:

Allied Quality Assurance Publications (AQAP): son un conjunto de estándares de aseguramiento de la calidad que publica la *Organización del Tratado del Atlántico Norte* (OTAN) para el aseguramiento de la calidad en las adquisiciones de los países miembros de la OTAN que haya ratificado el correspondiente acuerdo (STANAG).

Publicación Española para la Calidad (PECAL): son la traducción al español de las estándares AQAP. Existe una relación biunívoca entre un estándar AQAP y su PECAL equivalente. Cada estándar PECAL supone una traducción casi exacta del estándar AQAP equivalente, con unas mínimas modificaciones del *Ministerio de Defensa del Reino de España* (MDE).

Por tanto, la entidad emisora de los estándares AQAP es la OTAN, a través del grupo *Allied Committee* 327 (AC/327) del *Life Cycle Management Group* (LCMG) dependiente de la *Conference of National Armaments Directors* (CNAD) de la OTAN, donde están representados los países miembros de la OTAN. Mientras que la entidad emisora de los estándares PECAL es el MDE, a través del *Área de Inspecciones Industriales* (AII), que depende directamente de la *Dirección General de Armamento y Material* (DGAM).

La Unidad de Ingeniería de Calidad (UIC) del AII es la depositaria y responsable de la divulgación, distribución e interpretación de los estándares PECAL. El único órgano en España con la autoridad para emitir certificados PECAL y AQAP es la DGAM.

- **Disponibilidad**

Ambos grupos de familias son gratuitos y se pueden descargar desde las siguientes URL:

- Familia AQAP:

http://nso.nato.int/nso/nsdd/listpromulg.html

- Familia PECAL:

  http://www.defensa.gob.es/info/servicios/servicios-tecnicos/aseguramiento-calidad/

Clasificación (taxonomía)

Ambas familias de estándares se aplican en el Sector de la Defensa y Seguridad, entendida esta última en el marco conceptual del término inglés *homeland security*. No obstante lo anterior, es posible su utilización en cualquier sector.

La familia de estándares AQAP es de aplicación internacional y se requiere en contrataciones de los Ministerios de Defensa de los países miembros de la OTAN y, por extensión, de los principales contratistas de este sector.

La familia de estándares PECAL se requieren exclusivamente en el ámbito del Reino de España, pues son la traducción oficial (con los incrementos previamente comentados) de la normativa AQAP equivalente.

En ambos casos y de manera práctica en un contrato como contratista o sub-suministrador del MDE donde la aplicación de estos estándares sea un requisito, se puede requerir que:

Se deba llevar a cabo el contrato aplicando una determinada PECAL, o AQAP equivalente.

Se demuestre el cumplimiento por parte del SGC de la organización del estándar PECAL, o AQAP equivalente, requerida.

El SGC de la organización se encuentre certificado por el estándar PECAL, o AQAP equivalente, con un determinado alcance.

Los detalles exactos se encuentran en la Instrucción 39/1998, de 19 de febrero de 1998, y que se puede descargar de la página web del MDE indicada anteriormente.

- **Referencia normativa**

Ambas familias de estándares están basadas en el estándar ISO 9001:2000 y hasta la fecha han ido evolucionando en paralelo con las diferentes versiones de la ISO 9001, por lo que es previsible que también evolucionen en un futuro de la misma manera.

El conjunto de estándares, guías y otros documentos que constituyen la familia de estándares AQAP se lista en la siguiente tabla:

El conjunto de normas, guías y otros documentos que constituyen la familia de estándares PECAL se lista en la siguiente tabla:

Código	Título	Fecha
AQAP-2000 Ed. 3	NATO policy on an integrated systems approach to quality through the life cycle	2009-12-08
AQAP-2009 Ed. 3	NATO guidance on the use of the AQAP-2000 series	2010-09-21
AQAP-2050Ed. 1	NATO project assessment model	2003-09-01
AQAP-2070 Ed. 2 Ver. 2	NATO mutual Government Quality Assurance (GQA) process	2012-11-13
AQAP-2105 Ed. 2	NATO requirements for deliverable quality plans	2009-12-08
AQAP-2110 Ed. 3	NATO quality assurance requirements for design, development and production	2009-12-03
AQAP-2120 Ed. 3	NATO quality assurance requirements for production	2009-12-03
AQAP-2130 Ed. 3	NATO quality assurance requirements for inspection and test	2009-12-03
AQAP-2131 Ed. 2	NATO quality assurance requirements for final inspection	Nov 2006
AQAP-2210 Ed. 1	NATO supplementary software quality assurance requirements to AQAP-2110	2011-05-09
AQAP-2310 Ed. A Ver. 1	NATO quality management system requirements for aviation, space and defence suppliers	2013-04-12

El conjunto de normas, guías y otros documentos que constituyen la familia de estándares PECAL se lista en la siguiente tabla:

Código	Título	Fecha
PECAL-2000 Ed. 3	Política OTAN de calidad enfocada a sistemas integrados durante su ciclo de vida	Nov 2009
PECAL-2009 Ed. 3	Guía OTAN para el uso de las PECAL Serie 2000	Sep 2010
PECAL-2050 Ed. 2005	Modelo OTAN de evaluación de proyectos	Ene 2005
PECAL-2070 Ed. 2	Proceso OTAN para el mutuo Aseguramiento Oficial de la Calidad (AOC)	Abr 2009
PECAL-2105 Ed. 2	Requisitos OTAN para planes de calidad entregables	Nov 2009
PECAL-2110 Ed. 3	Requisitos OTAN de aseguramiento de la calidad para el diseño, el desarrollo y la producción	Nov 2009
PECAL-2120 Ed. 3	Requisitos OTAN de aseguramiento de la calidad para la producción	Nov 2009
PECAL-2130 Ed. 3	Requisitos OTAN de aseguramiento de la calidad para inspección y pruebas	Nov 2009
PECAL-2131 Ed. 2	Requisitos OTAN de aseguramiento de la calidad para inspección final	Nov 2006
PECAL-2210 Ed. 1	Requisitos OTAN de aseguramiento de la calidad del software, suplementarios a la PECAL 2110	Nov 2007

Código	Título	Fecha
PECAL-2310 Ed. A Ver. 1	Requisitos OTAN para los Sistemas de Gestión de la Calidad de Suministradores de Aviación, Espaciales y de Defensa	Abr 2013

En particular, el estándar 2210 relativa a la Ingeniería del Software suele ser el estándar más difícil y compleja en su implantación y aplicación, por lo que se sugiere apoyar la implantación de la misma en las buenas prácticas y procesos definidos en los estándares ISO 12207 (*Systems and software engineering - Software life cycle processes*) e ISO 15288 (*Systems and software engineering - System life cycle processes*).

A continuación se inserta una gráfica de la relación entre los estándares PECAL entre sí y con otros estándares ISO que ha sido realizada por AII y que se encuentra en su página web:

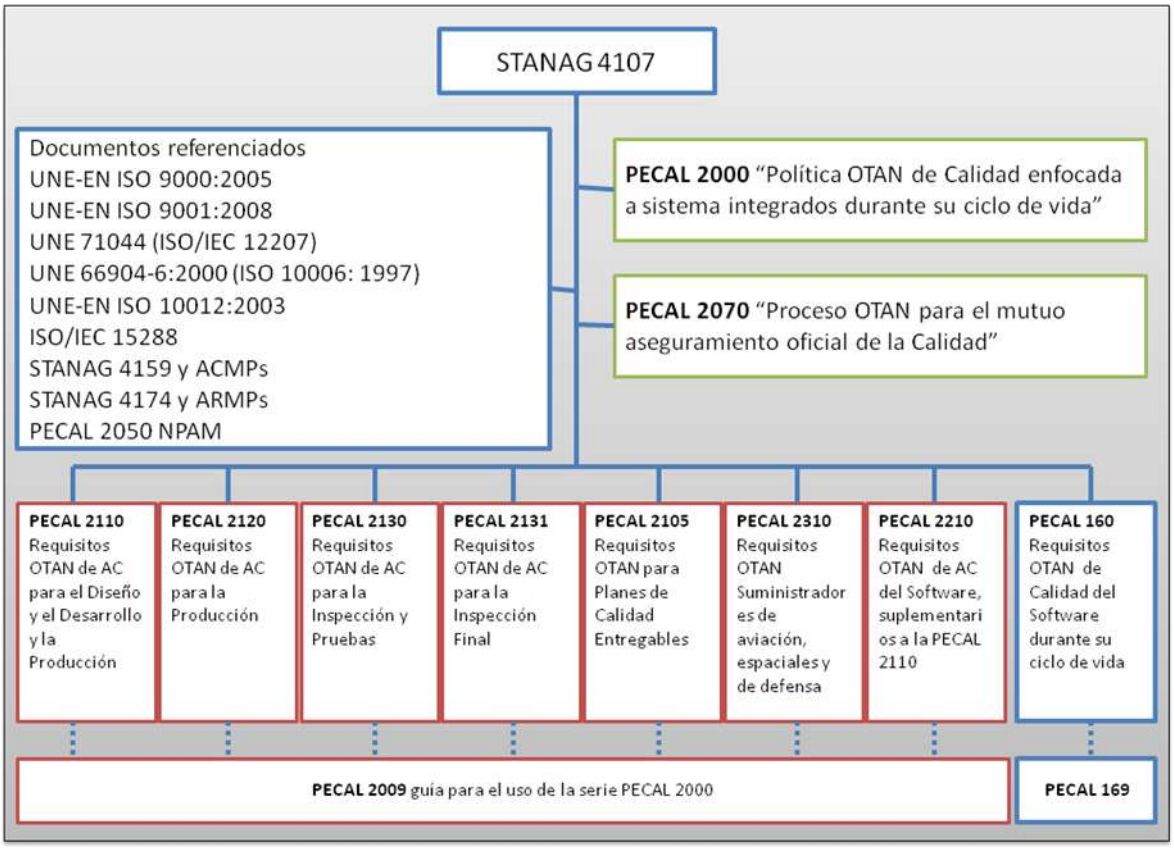

Ilustración 4 Relación Estándares PECAL entre sí y con otros estándares ISO

Nota: en dicha gráfica aparece el estándar PECAL 160 y su guía de aplicación PECAL 169, que tienen su equivalente en las AQAP con el mismo indicativo. La OTAN no recomienda el uso de dichas estándares, motivo por el cual la DGAM dejó de certificarla y pedirla en contratos. Son escasos los países miembros de la OTAN que las mantienen.

Además conviene destacar que la aplicación de la familia de estándares PECAL está condicionada y ampliada por las *Instrucciones Técnicas* (IT) de la UIC. Estas IT aclaran la interpretación del AII de dichos estándares mediante un conjunto de requisitos añadidos, comentarios y otros apuntes al respecto.

- **Ámbito de aplicación**

Estas dos familias de estándares son aplicables a cualquier tipo de organización, si bien su principal objetivo, propósito y uso previsto es su aplicación por parte de cualquier organización que vaya a establecer algún tipo de relación contractual para el suministro de productos o servicios con el MDE (en cuanto a PECAL se refiere), con cualquier país miembro de la OTAN o cualquier organismo de la OTAN (en cuanto a AQAP se refiere) o, finalmente, con cualquier contratista principal de los anteriormente mencionados.

La implantación de un estándar en particular de estas familias estará determinada principalmente por el tipo de trabajo que se realice en la organización y el tipo de producto o servicio que se suministre en base a este trabajo.

Al igual que ocurre con otros estándares certificables, la certificación con respecto a una determinada AQAP / PECAL estará también condicionada por el alcance de certificación que se solicite.

A modo de ejemplo, una organización que sólo se dedique a comercializar productos finales no requerirá de la implantación de la 2110, de la 2210 ni de la 2120. Es muy probable que con la implantación de la 2130 o de la 2131, en determinados casos y en función de su alcance, sea suficiente.

Siguiendo con el ejemplo, para una organización que se dedique exclusivamente a la Producción puede ser suficiente con una 2120; si bien y a priori, la 2130 y la 2131 son claramente insuficientes.

Para finalizar con el ejemplo para cualquier organización que realice Diseño, el estándar a implantar será la 2110.

Al margen de cuál sea la principal de estas 21xx que se implante, cualquier organización que proporcione soluciones informáticas de cualquier tipo, se le requerirá 2210.

- **Certificación**

Como se ha indicado en la primera sección, la DGAM es el único Organismo en España con la autoridad para emitir certificados PECAL y AQAP.

El AII dispone de un proceso conocido y normalizado para la realización de la certificación, del seguimiento de la misma y de la re-certificación (a repetir cada tres años) donde cabe destacar que:

- La primera certificación se realiza mediante una auditoría que realiza exclusivamente el personal de la DGAM.
- Las auditorías de seguimiento se realizan por personal debidamente acreditado de Entidades de Certificación. Sin embargo, cabe destacar que el AII se reserva el derecho a realizar una auditoría a la empresa en cualquier momento ante informaciones que así lo aconsejen.
- Las auditorías de re-certificación siguen el mismo patrón que las auditorías de seguimiento con una excepción: si la certificación incluye el estándar 2210, entonces esa parte de la auditoría se realiza exclusivamente el personal de la DGAM.

A este respecto, la DGAM, a propuesta del AII, procede a la certificación de un determinado organismo frente a los estándares PECAL/AQAP que se soliciten, haciendo un único proceso y un único certificado donde se documentan claramente tanto el estándar PECAL como la AQAP equivalente.

Estos certificados se emiten en español e inglés ratificando el cumplimiento de los estándares indicados.

Son certificables los estándares 2110, 2120, 2130 y 2310 de ambas familias.

Para el caso del estándar 2210, referido expresamente a la Ingeniería Informática, se procede a su proceso de certificación de manera conjunta e indisoluble con el proceso de certificación del estándar 2110. Si se supera satisfactoriamente dicho proceso, el certificado del estándar 2110 contendrá unos párrafos indicativos del cumplimiento y certificación también por el estándar 2210.

El resto de documentos que constituyen ambas familias son estándares, guías u otro tipo de documentos que no son certificables.

Objetivos del estándar

Las familias de estándares AQAP / PECAL tienen como objetivo identificar un conjunto de requisitos OTAN para el aseguramiento de la calidad en diferentes fases del ciclo de vida de un producto o servicio. Este enfoque de "requisitos OTAN" queda patente desde el mismo título de todos los estándares de ambas familias.

Agentes facilitadores para su adopción/implementación

El principal, y casi único, agente facilitador para la adopción de alguna de las estándares de estas familias de estándares es el interés estratégico de la organización de participar como contratista, subcontratista, proveedor o colaborador con organismos directamente relacionados con la Defensa y donde se requiera la certificación por estas estándares como requisito contractual.

Conviene aclarar que por "organismos directamente relacionados con la Defensa" se quiere hacer mención directa al MDE, a la OTAN, a cualquier país miembro de la OTAN o cualquiera de las estructuras organizativas de los anteriores, así como a cualquier contratista principal del sector de Defensa.

Por otra parte, las estándares 2110, 2120, 2130, 2131 y 2310 parten de la ISO 9001:2000 (y son compatibles con las ISO 9001:2008)) en su totalidad y respetan su esquema, aportando nuevos requisitos, comentarios y otros elementos que surgen en base a las necesidades militares, en general, y de la OTAN, en particular. Esta estructura facilita bastante su implantación en organizaciones con SGC que ya están evaluados y/o certificados por ISO 9001 o por estándares basadas en esta (como por ejemplo EN 9100).

Esta facilidad no está presente en el resto de estándares de estas familias porque tanto la estándar 2210 como el resto de documentación en ambas familias tienen un esquema propio.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

La principal ventaja competitiva para una empresa es poder acceder al mercado del sector de la Defensa y Seguridad; siendo el riesgo más evidente e inmediato quedarse fuera de dicho mercado por no disponer de la certificación.

Hay organismos de la propia Administración Pública y del propio MDE que han encontrado ventajas en la adopción, implantación y certificación de la normativa PECAL / AQAP aun cuando, por su dependencia jerárquica, pudieran estar exentos de realizar dicho proceso.

Reconocimiento/reputación

Por los motivos indicados en la sección anterior, estas familias de estándares son de amplio uso y reconocimiento en el Sector de la Defensa y la Seguridad.

Directrices sobre su uso/implementación

Las principales directrices, o consejos, a tener en cuenta en la implantación de los estándares de las familias AQAP / PECAL es:

- Analizar claramente los beneficios y costes de la implantación para enmarcar la decisión de dicha implantación dentro del conjunto de decisiones estratégicas de la organización y que cuente con el respaldo y la involucración de la Alta Dirección, de tal forma que se garantice el establecimiento y aplicación de un Plan de Implantación y se dote a esta iniciativa de los Recursos necesarios.
- Determinar el alcance de la certificación que se desea alcanzar y, en función del mismo y de los productos que genere la organización, determinar las estándares AQAP / PECAL que serán el objetivo a alcanzar.
- Se debe contactar con la Unidad de Calidad del AII, ya que proporcionarán toda la documentación, formularios y pautas del proceso que se encuentre vigente para proceder a la implantación y certificación.
- *Nota*: como en todo proceso de certificación, la participación del personal auditor (en este caso de la DGAM) supone un coste económico en base a unos precios públicos.
- Se debe contactar con la Asociación Española para la Calidad (AEC) ya que son los únicos proveedores autorizados por el Comité Mixto Defensa-Industrias de Armamento y Material (CMDIN) para la realización de los cursos de formación en la normativa AQAP / PECAL.
- El CMDIN es un Comité que está constituido por representantes de la DGAM, por representantes de empresas de la Industria de Defensa y por representantes de Entidades de Certificación.
- De acuerdo con la reglamentación vigente a fecha de publicación de este documento, es necesario que el Director de Calidad (en su papel de Representante de la Dirección)-haya recibido estos cursos.
- Desde el principio, es decir una vez tomada la decisión del punto 1, se puede reducir sistemáticamente el período de tiempo de todo el proceso si se va alineando la documentación del Sistema de Gestión de la Calidad con las estándares PECAL / AQAP y si se van aplicando, a modo de piloto, en al

menos un contrato que esté en marcha (preferiblemente recién iniciado) en la organización.

A estas consideraciones particulares habría que unir todas aquellas consideraciones generales a la hora de adoptar e implantar un Sistema de Gestión de la Calidad, en general, y una normativa, en particular.

Como último detalle a tener en consideración, es importante identificar cuál es la estándares AQAP / PECAL de interés para la organización ya que impactará considerablemente en el proyecto de implantación, por lo que se aconseja leer detenidamente el apartado 1.3 de la guía AQAP / PECAL 2009, donde se identifica en su Figura 2 cuál es la forma de seleccionar las estándares AQAP / PECAL adecuadas.

Relación con otros estándares/modelos

La relación con otros estándares y modelos ha quedado recogida en el capítulo de referencia normativa.

ISO/IEC 15504-4:2008

ISO/IEC 15504-4:2008 – Information technology -- Process assessment -- Part 4: Guidance on use for process improvement and process capability determination

Entidad Emisora

ISO/IEC 15504-4 es un estándar internacional destinado a evaluar y mejorar la capacidad y madurez de los procesos de Desarrollo de Software principalmente, si bien es aplicable a otros muchos sectores. Es un estándar que comenzó a gestarse desde la comisión ISO/IEC JTC1 en el año 1993, y los 9 apartados de la redacción definitiva del estándar fueron publicándose entre los años 2003 y 2005. Como se ha indicado, no es un estándar únicamente pensado para el Desarrollo de Software, si bien su implementación se asocia generalmente a esta área acompañada de modelos de referencia específicos, el más habitual ISO/IEC 12207.

- **Disponibilidad**

El documento 15504 – Parte 4, que especifica el Proceso de Evaluación conforme a un Programa de Mejora, así como la determinación de la capacidad, puede comprarse en la web de ISO www.iso.org al precio de 138 CHF (a fecha de publicación de la ficha), y la parte 2, relativa a la realización de una evaluación basada en el modelo, puede adquirirse en la cita web al precio de 88 CHF (a fecha de publicación de la ficha).

Clasificación (taxonomía)

El estándar ISO/IEC 15504, forma parte del catálogo de estándares 35.080 de ISO que incluye además en la misma familia otras normas relativas al Desarrollo de Software, Aplicaciones, Internet, Usabilidad, Documentación del Software, etc. En este mismo catálogo de estándares se incluye ISO/IEC 12207 Procesos Para el Ciclo de Vida del Software, muy relacionada con la citada 15504.

- **Referencia normativa**

El estándar ISO/IEC 15504 establece un marco para la evaluación, no siendo específicamente un modelo normativo propiamente dicho. Se apoya en el estándar de referencia ISO/IEC 12207 para lo relativo a la evaluación de entornos de Desarrollo de Software.

El estándar ISO/IEC 15504 fue preparado por el Comité Técnico ISO/IEC JTC1 de Tecnologías de la Información de ISO.

El estándar ISO/IEC 15504 incluye un conjunto de libros que se engloban bajo el nombre de SPICE (Mejora de los Procesos de Software y Determinación de su Capacidad), por sus siglas en inglés. Los más importantes son:

- ISO/IEC 15504-1, relativo a los conceptos, terminología y vocabulario empleado por el estándar. Se inspira en buena medida en los modelos estándar para el control de la calidad en los procesos como ISO 9000 y en los modelos específicos de Desarrollo de Software como ISO/IEC 12207.
- ISO/IEC 15504-2, que trata el modelo de evaluación en una organización basada en procesos de Desarrollo de Software.
- ISO/IEC 15504-3, que desarrolla una orientación explicativa más extendida para la realización de la evaluación en base al libro citado en el punto anterior.
- ISO/IEC 15504-4, que marca orientaciones de ayuda para el desarrollo de actividades de mejora de los procesos así como la determinación de las diferentes capacidades de los mismos.
- ISO/IEC 15504-5, que plantea un ejemplo de modelo adecuado de evaluación de procesos basado en este estándar.
- ISO/IEC 15504-6, que plantea un ejemplo del ciclo de vida adecuado del modelo, de acuerdo al marco definido por el estándar ISO/IEC 15288, y a las capacidades definidas en el propio estándar, en el libro ISO/IEC 15504-2.
- ISO/IEC 15504-7, que sienta las bases para determinar el nivel de madurez de una organización de acuerdo al modelo ISO/IEC 15504.

- **Ámbito de aplicación**

Este modelo es de aplicación para muchas actividades organizativas donde la recogida de requisitos, la estimación de esfuerzos y recursos, la verificación del producto y, en general, el seguimiento del ciclo de vida de un proyecto, tienen como objetivo la realización de un determinado producto, tangible o no, que persigue cubrir una serie de requisitos funcionales y de otra índole. No obstante, dado su

origen en el Comité de Trabajo de Tecnologías de la Información, está especialmente explotado en dicho ámbito del conocimiento. Por ello, su aplicación principal pasa por los siguientes aspectos:

- El mundo del Desarrollo de Software, entendiendo como tal el entorno de producción del software, la recogida de requisitos de diferente índole entre todos los actores implicados, la gestión de recursos técnicos y humanos, el control y seguimiento de los riesgos, la verificación de la concordancia entre los requisitos, objetivos y expectativas con el conjunto de productos finalmente propuestos para entrega, el control de paquetes y versiones, etc.
- El modelo puede ser empleado como herramienta para la identificación de actividades y fases en los proyectos de Ingeniería de Software de cualquier organización dedicada a otro tipo de actividades, así como por empresas especializadas en el Desarrollo de Software para terceros, como garantía de Calidad en el cumplimiento de los estándares y compromisos marcados con los contratos de desarrollo con sus Clientes.
- Al ser un modelo de desarrollo por procesos técnicos de ingeniería de software y fases con requisitos concretos para cada proceso, es replicable además en las herramientas software utilizadas comúnmente como apoyo al desarrollo y para el control de procesos de desarrollo de software por parte de las organizaciones.

- **Certificación**

ISO/IEC 15504-4 (junto con el libro 15504-7 que clarifica el camino hacia la madurez) es certificable de manera directa por las firmas auditoras de primer nivel, y en el caso de España principalmente por AENOR y BUREAU VERITAS. Este certificado no cuenta con acreditación de respaldo emitida por ENAC, de ahí la importancia de seleccionar una firma auditora de primer nivel que garantice directamente el prestigio de la certificación obtenida.

Objetivos del estándar

El objetivo del estándar ISO/IEC 15504-4 consiste en la identificación del grado de madurez de una organización respecto de una serie de procesos primarios (directamente implicados en el desarrollo de software), de soporte, y organizacionales. El estándar marca 6 niveles de madurez que van desde el nivel 0 (incompleto) hasta el nivel 5 (en optimización).

Igualmente, el estándar establece varios puntos de alineación de los procesos de desarrollo de software con otros ámbitos como son la Seguridad de Información (ISO/IEC 27000), la Gestión de Servicios (ISO/IEC 20000) y la Gestión de Procesos

(ISO 9000). La compartición de estructura, enfoque a procesos y modelo de evaluación periódico permite definir mecanismos de control y mejora continua en aquellas organizaciones que cuentan con Sistemas Integrados de Gestión como por ejemplo PAS99.

Agentes facilitadores para su adopción/implementación

Dentro de los agentes facilitadores encontramos, por un lado, la obligatoriedad de acreditar un nivel de madurez exigido para poder acceder a contratos con las Administraciones Públicas o empresas que lo requieran y, por otro lado, la necesidad de la organización de alcanzar mejoras significativas en las siguientes áreas:

- Aseguramiento de la calidad esperada tras las diferentes fases y actividades relacionadas con el Ciclo de Desarrollo de Software.
- Asegurar que los entregables, así como el conjunto de elementos que componen una solución de software se adecúa a los criterios y requisitos marcados por todas las partes interesadas.
- Medición de la calidad de los productos, así como el correcto cumplimiento de cada uno de los hitos.
- Identificación de no conformidades e ineficiencias en los procesos de desarrollo de software.
- Asegurar el control de entregables y versiones de acuerdo a los modelos estándar marcados por la organización.
- Integrar los procesos de software en el sistema integral de procesos de la organización.
- Hacer a la organización más rentable y eficiente.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

La implementación de la serie de normas ISO/IEC 15504, apoyada en los procesos de ingeniería de software específicos como los identificados en ISO/IEC 12207, ayudarán a las organizaciones a completar con éxito el camino, no siempre sencillo, de identificar las diferentes necesidades que deben ser cubiertas por un sistema software, evaluar su estabilidad y robustez, y asegurar el paso de las diferentes etapas hasta su puesto en producción. La ventaja competitiva que aporta este modelo desde las 7 perspectivas del negocio se pueden resumir en:

- Eficacia: El modelo permite asegurar que se realizan todos los pasos necesarios que requiere la organización para el desarrollo de un proyecto de software, y que por tanto el resultado de las actividades desarrolladas bajo el mismo

cumplirán con los objetivos definidos en las diferentes capas de la organización que impulsen el proyecto.

- Eficiencia: Los procesos propios del estándar relativos al control de la calidad y la métrica de los productos software obtenidos permite detectar puntos de mejora, además de no conformidades, en cada uno de los procesos. Además, un desarrollo de software adecuado redunda en un mejor mantenimiento del mismo y en una reducción de sus costes globales durante su paso por producción.
- Confidencialidad, Integridad y Disponibilidad (Principios CIA de la Seguridad de la Información): El estándar se centra en el trabajo con productos software. Por ello, tiene en cuenta los requisitos de seguridad necesarios, y no olvida el tratamiento de los riesgos sobre los productos, los entregables y el propio proyecto. Además, el tratamiento de riesgos sobre la seguridad de la información, aspecto clave en el mundo del software, es un requisito incorporado en la última versión ISO/IEC 27000 sobre Seguridad de la Información.
- Confiabilidad: La utilización de un modelo de buenas prácticas para los procesos de ingeniería de software permite la obtención de un producto final confiable, que asegure un desempeño correcto en el ámbito de la organización para el que este fue diseñado de acuerdo a su alcance y objetivos.
- Cumplimiento: Hoy día, el cumplimiento y alineación con requisitos tanto organizacionales como regulatorios está más observado que nunca. Por ello, los requisitos de todo tipo que deben ser expresados para determinar las características del software son expresados gracias al estándar en un idioma comprensible, a través de procesos de consulta sencillos y fácilmente entendibles por personal no técnico desde el punto de vista de la ingeniería del software. Sus aportaciones son entradas como requisitos de cualquier software, y los mecanismos y procesos de control antes del paso a producción aseguran el cumplimiento regulatorio esperado.

El principal riesgo derivado de su no implantación radica en la no existencia de un modelo ordenado de Desarrollo de Software, entendiendo como tal desde las primeras etapas de identificación de necesidades y recogida de requisitos hasta su verificación, puesta en producción y entrada en el proceso de mantenimiento y evolución.

Otro riesgo es que puede derivar en una Gestión de Cambios no controlada, en un progresivo des-alineamiento del software con los objetivos marcados, y en una pérdida de control y conocimiento sobre el mismo por parte de la organización.

Estos riesgos, si bien son asumidos en primera persona por los Dptos. de TI que deben soportar el ruido producido por el mal funcionamiento del software y el mantenimiento de sistemas mal diseñados, impactan directamente sobre las organizaciones en su conjunto, dado que el software es un recurso transversal y vital para el conjunto de departamentos de prácticamente cualquier compañía y cualquier sector de actividad.

Reconocimiento/reputación

Desde la implantación del modelo de evaluación por niveles de ISO/IEC 15504 – SPICE de AENOR en 2010 hasta la actualidad, más de 100 organizaciones se han certificado, la mayoría de ellas en el nivel 2 de madurez, si bien cada vez más tratan de alcanzar niveles superiores (más de 10 organizaciones a día de hoy ya disponen de una certificación de Nivel de Madurez 3).

Dentro del abanico de empresas certificadas, están presentes principalmente empresas del sector TI directamente vinculadas con el mundo del desarrollo de software, y que han incorporado en sus organizaciones procesos específicos de Ingeniería del Software. También es destacable la presencia en esta lista de organizaciones certificadas vinculadas al mundo de la automoción, dentro del marco específico del propio estándar conocido como Automotive SPICE.

Además, el estándar guarda un cierto paralelismo con modelos con un mayor reconocimiento de mercado como CMMI, lo que facilita su presentación en el mercado mundial de Ingeniería del Software.

Directrices sobre su uso/implementación

El principal beneficio del estándar es que éste puede ser aplicado progresivamente, estableciendo un modelo de madurez basado en el crecimiento, tanto en el volumen de proyectos certificados con las buenas prácticas, de acuerdo a los objetivos e intereses propios que se marque la compañía, como en el conjunto de actividades y procesos de Ingeniería de Software implementados:

- En el Nivel 1 de Madurez (el nivel 0 se considera "fail"), la organización evidencia un compromiso básico con la implementación de procesos de Ingeniería de Software tendentes a la mejora en la gestión y calidad de sus actividades de desarrollo de software.

  El nivel 1 se conseguiría con tener implantada la norma ISO 9000.

- En el nivel 2 de Madurez, la organización puede además evidenciar ante el equipo evaluador que dispone de evidencias de la implantación de los

procesos objetivo, además de su cumplimiento en varios proyectos, que serán referenciados para ser utilizados durante el proceso de auditoría mostrando con ello el rendimiento de dichos procesos en las actividades de producción de software.

Abordar la implementación de este nivel 2 sería el paso adecuado para establecer una gestión de proyectos robusta que se utilizaría como base para determinar las mejores prácticas, las cuales serán llevadas al nivel de procesos de la organización. En este nivel la medición debe iniciarse como base para la mejora y el conocimiento de la capacidad de los procesos.

- En el nivel 3 de Madurez, la organización puede evidenciar que todas sus actividades de desarrollo de software se encuentran establecidas, controladas y gestionadas de acuerdo a los procesos de desarrollo de software que ella misma ha identificado para todos los proyectos que desarrolla, y no solamente una selección de los mismo.

El nivel 3 es adecuado para organizaciones que quieren implantar una gestión de procesos robusta, consiguiendo tener caracterizado el rendimiento de todos sus procesos mediante el uso generalizado de procesos estándares y comunes en todos los proyectos de la organización. Se implanta una economía de escala en la gestión de las mejoras pues estas se pilotan en un proyecto y se despliegan en todos los demás proyectos, una vez se ha determinado que es una mejora efectiva (con medidas).

- En el nivel 4 de Madurez, la organización debe evidenciar que ha dado el salto de tener controlados y medidos los procesos de ingeniería de software, y que se encuentra en un estado de medición avanzado sobre sus propios procesos y el control y gobierno de los mismos para la mejora.

El nivel 4 determina un estado de madurez muy elevado que evidencia una destreza e implantación natural en las actividades de control de Calidad y mejora continua de sus procesos de software de manera general.

- En el nivel 5 de Madurez (máximo), la organización ha alcanzado un nivel de madurez en sus procesos de Ingeniería de Software tal, que es capaz de poner en marcha iniciativas de Innovación y Optimización de sus procesos de desarrollo de software, por encima de los requisitos marcados por los estándares de referencia en el mercado para el mundo de la Ingeniería de Software.

La implantación de ISO/IEC 15504 evidencia por tanto algunos aspectos clave, que en unos puntos guardan similitud con otras normas ISO generalistas, mientras que en otros ofrecen un planteamiento completamente distinto:

- El estándar prevé el establecimiento de los requisitos clásicos de compromiso de la Dirección, disponibilidad de los recursos, seguimiento PDCA, seguimiento de las no conformidades y evaluación de la eficacia de las acciones correctivas y de mejora, etc.
- El estándar establece e identifica procesos de Ingeniería de Software, alineados con ISO 12207, divididos en 5 grandes bloques, que son Clientes y Proveedores, Ingeniería, Soporte, Gestión y Organización.
- Se definen 2 dimensiones clave para encuadrar a la compañía:
  - Los diferentes procesos y categorías identificados e implementados por cada organización (procesos de los bloques de Ingeniería, Soporte, etc.)
  - El grado de madurez de la organización en el manejo de sus procesos (desde la identificación, en los niveles más bajos, hasta la innovación y optimización del Nivel 5 de madurez).
- Como aspecto destacable, hay que tener presente que dos organizaciones certificadas no tienen por qué tener los mismos procesos implementados, ni siquiera en el mismo nivel de certificación (sí que deberían tener no obstante la misma madurez mínima para los procesos declarados ante el equipo evaluador si estuvieran en el mismo nivel), y por tanto cada certificado que declara el nivel de madurez debe venir acompañado por el listado de procesos de Ingeniería de Software que se encuentran declarados y han sido por ello evaluados por el equipo evaluador.

Relación con otros estándares/modelos

El estándar más destacable relacionado con ISO/IEC 15504 es el citado ISO/IEC 12207, estándar específico que recoge un importante volumen de procesos de Ingeniería de Software.

Derivada de su relación con dicho estándar 12207, ISO/IEC 15504 identifica una serie de procesos software que pueden ser apoyados por estándares específicos de otro ámbito, y para los cuales disponen de una alineación importante en su enfoque, que se citan a continuación.

ISO/IEC 27001, estándar relacionado con la Seguridad de la Información, establece la Gestión de los Proyectos como uno de sus objetivos de control en el Anexo A de su última versión.

ISO/IEC 20001, estándar relacionado con la Gestión de Servicios, establece paralelismos que pueden ser aprovechados para el desarrollo del mantenimiento del

software en entornos en producción, a través de procesos importantes como la Gestión de Incidentes y Problemas, Gestión del Cambio, Capacidad, etc.

ISO/IEC 25000 / SQUARE, estándar relacionado con la Calidad de un Producto Software, y que pone el foco en el entregable final derivado de las actividades de Ingeniería de Software, y que dispone de libros muy interesantes para complementar una implantación 15504, como ISO/IEC 25012, relativo a Modelos de Calidad de los Datos, o ISO/IEC 25021, que trata el tema de las métricas que pueden ser utilizadas a lo largo de todo el ciclo de desarrollo del software.

Dentro de la familia ISO 9000, estándar general para la Gestión de la Calidad basado en Procesos, existe un estándar de referencia poco conocido, ISO 90003 – Gestión de la Calidad en Ingeniería del Software, que constituye una guía para la implantación de procesos de calidad ISO 9000 en entornos de desarrollo de software.

El estándar de reciente publicación ISO 21500 de Desarrollo de Proyectos, identifica fases e hitos que son fácilmente equivalentes en un entorno de Ingeniería de Software desde la recogida de requisitos básicos hasta la puesta en producción y cierre del proyecto o su correspondiente entrega y paso a servicio.

Estándares de nicho, como el Ciclo de Vida para la Pequeña Empresa ISO/IEC 29110, que se encuentra en elaboración, pero de gran interés para las iniciativas empresariales relacionadas con el mundo de la Ingeniería del Software.

Igualmente, cualquier estándar de Desarrollo de Software que proponga procesos y métodos para el Desarrollo de Software puede relacionarse con ISO/IEC 15504, incluyendo en este listado, a título puramente de ejemplo, métodos como SCRUM.

CMMI®

CMMI®: Capability and Maturity Model®. Integration

Entidad Emisora

El modelo CMMI fue desarrollado por el *Software Engineering Institute* (SEI) de la Universidad Carnegie Mellon. Desde Diciembre de 2012 es gestionado por el *CMMI Institute*.

- **Disponibilidad**

El documento puede descargarse gratuitamente desde el sitio web del CMMI Institute (www.cmmiinstitute.com).

- **Clasificación (taxonomía)**

CMMI es un modelo internacional de buenas prácticas.

Referencia normativa

El modelo CMMI v.1.3 se compone de tres constelaciones que recogen las buenas prácticas de sus correspondientes ámbitos:

CMMI for Development (CMMI para Desarrollo, abreviado como CMMI-DEV).

CMMI for Services (CMMI para Servicios, abreviado como CMMI-SVC).

CMMI for Acquisition (CMMI para Adquisición, abreviado como CMMI-ACQ).

- **Ámbito de aplicación**

Su aplicación más habitual se encuentra en el sector de tecnologías de la información, debido a que proviene del modelo originario sw-CMM desarrollado por Watts Humphrey en 1988. Sin embargo, la versión actual permite su aplicación en organizaciones de cualquier sector sobre cualquier tipo de productos o servicios.

- **Certificación**

El modelo CMMI no es certificable. Sin embargo, es evaluable a través del método SCAMPI[SM] (*Standard CMMI Appraisal Method for Process Improvement*) según se describe en el MDD v.1.3b (*Method Definition Document for SCAMPI A, B and C*).

Los resultados de las evaluaciones oficiales que hayan utilizado el método SCAMPI Clase A se pueden publicar en el sistema PARS (*Published Appraisal Results System*) en el sitio web del CMMI *Institute*, cuando han sido realizadas por una empresa asociada al CMMI *Institute*.

La organización del modelo propone dos posibles representaciones: continua y escalonada. Los resultados de la evaluación podrían indicar el nivel de madurez (desde el nivel 2 hasta el nivel 5) alcanzado respecto de la representación escalonada, o los niveles de capacidad (desde el nivel 0 hasta el nivel 3) para cada área de proceso evaluada respecto de la representación continua.

Objetivos del modelo

Este modelo pretende ser una guía para la aplicación de las mejores prácticas en una organización que adquiere o desarrolla productos o servicios, con la intención de obtener productos o servicios que cumplan con las necesidades de los clientes y los usuarios finales.

Este modelo recoge buenas prácticas correspondientes a la gestión de proyectos, la gestión de procesos, los procesos de ingeniería, los procesos de adquisición, la gestión de los servicios y otros procesos de soporte.

Agentes facilitadores para su adopción/implementación

El modelo incorpora dentro de su propia estructura un conjunto de textos de carácter informativo que pretenden facilitar la implementación de las prácticas que son esperadas para la consecución de las metas obligatorias. Esta información incluye ejemplos, descripciones de subprácticas y productos de trabajo, entre otros.

Las distintas áreas de proceso reúnen metas y prácticas con un fin común. Se clasifican en grupos de áreas de proceso, dedicados a la gestión de proyectos, la gestión de procesos, los procesos de ingeniería, la gestión de la adquisición, la gestión de los servicios y otros procesos de soporte.

Las prácticas específicas muestran como la organización puede mejorar para conseguir los objetivos de un área de proceso concreta, mientras que las prácticas genéricas favorecen la consecución de los objetivos de institucionalización de dichos procesos en la organización.

Dado que CMMI es un modelo que pretende mejorar la efectividad de las organizaciones, un conjunto de objetivos de negocio marcados por la Dirección con éste fin, supone un acicate inexcusable para la adecuada implantación de las prácticas recomendadas por el modelo: incrementos de productividad, mejora de la calidad del producto o del servicio, o cumplimiento de los estándares exigidos por los clientes finales a sus proveedores, por ejemplo.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

La implantación del modelo pretende incrementar la madurez de las organizaciones, proporcionando un proceso gestionado y definido que les permita mejorar para ser más competitivas en términos de calidad y productividad.

Frente a este objetivo deseable, se encuentra la situación de las empresas inmaduras: aquellas que responden a las necesidades de sus clientes de manera reactiva, con un planteamiento ad-hoc para cada solución, dependiendo de las personas que hayan participado en su elaboración y sin un proceso definido.

El grado de abstracción que incorporan las descripciones del modelo permite realizar una implementación adecuada al contexto de cada organización. Es un error forzar a las organizaciones a realizar métodos de trabajo artificiales y costosos, para conseguir el cumplimiento de las prácticas esperadas. Cada meta exigida en el modelo representa un objetivo que cualquier organización necesita alcanzar para conseguir reducir el riesgo de su negocio y mejorar los ratios de productividad y de calidad. Por lo tanto, una implementación adecuada debe permitir a la organización alcanzar dichos objetivos de la manera más natural, que derive de la interpretación apropiada del modelo.

Desde el punto de vista del método de evaluación SCAMPI, a la vez que se evidencia el grado de implantación del modelo CMMI, se consigue un resultado verdaderamente enfocado a la mejora de la organización. Esto se debe a que se lleva a cabo por un equipo evaluador con la adecuada experiencia en el negocio y formación en el modelo, normalmente formado por miembros de la organización evaluada, que son guiados por un CMMI SCAMPI Lead Appraiser certificado por el CMMI Institute. Este proceso guarda el estricto cumplimiento de los requisitos de

confidencialidad y no atribución para garantizar unos resultados objetivos y reconocidos por toda la organización.

Reconocimiento/reputación

Este estándar es ampliamente usado en las empresas de desarrollo de software y es reconocido como un estándar de facto a nivel mundial en dicho ámbito.

El CMMI *Institute* publica semestralmente un informe denominado *"Process Maturity Profile"* que refleja la situación del uso del modelo de manera global y por países. En dicho informe, en la fecha de publicación de este documento, se refleja que China, India y EE.UU. han albergado un mayor número de evaluaciones, seguidos de España, que ocupa la cuarta posición mundial desde el año 2009.

Directrices sobre su uso/implementación

La figura independiente de un CMMI SCAMPI *Lead Appraiser* certificado por el CMMI Institute puede proporcionar a las organizaciones una visión objetiva del grado de implementación de las prácticas del modelo CMMI para un alcance definido, denominado unidad organizacional.

En la propia definición del MDD se contemplan tres métodos de evaluación denominados SCAMPI Clase C, B y A respectivamente, cuyos resultados aportan a las organizaciones las claves para dirigir sus planes de mejora particularizados:

- El SCAMPI Clase C se lleva a cabo al inicio de un proyecto de mejora para detectar debilidades desde un punto de vista metodológico.

  Es habitual construir un plan de mejora que, partiendo de los resultados de la evaluación SCAMPI Clase C, permita alcanzar los objetivos planteados, definiendo las soluciones metodológicas necesarias para resolver las debilidades detectadas. Es importante especificar las tareas, recursos y plazos para construir dichas soluciones, impartir la formación necesaria y desplegarlas en los proyectos donde deben aplicarse.

- El SCAMPI Clase B se lleva a cabo una vez que el plan de mejora se ha ejecutado y busca evaluar el grado de implementación de las prácticas aplicadas en los proyectos donde se han desplegado las mejoras. Normalmente la organización utiliza el resultado de esta evaluación para tomar la decisión sobre la fecha en la que se llevará a cabo, con garantías de éxito, la evaluación final o SCAMPI Clase A.

- El SCAMPI Clase A se considera el método de acreditación formal de los procesos en la unidad organizacional. Consta de las fases de planificación, realización y reporte de los resultados al CMMI Institute.
    - La fase de planificación incluye la denominada *"Readiness Review"* cuya salida puede desencadenar la confirmación del calendario establecido, su aplazamiento o la cancelación del SCAMPI, en caso de que las comprobaciones sobre el equipo evaluador, la logística y las evidencias recogidas, no se consideren aceptables para finalizar con éxito la evaluación.
    - La fase de realización del SCAMPI incluye las entrevistas propiamente dichas. Durante esta fase, el equipo evaluador determina el grado de implementación del modelo a la vista de las evidencias (artefactos y afirmaciones) aportadas por la organización.
    - Tras el reporte de los resultados al CMMI Institute, se produce la publicación de los resultados en el sistema PARS (*Published Appraisal Results System*) en un plazo habitualmente inferior a 30 días.

Por otro lado, las mejoras organizacionales no se pueden reconocer si los procesos no están adecuadamente definidos y medidos, por lo que el modelo hace referencia a las actividades de medición y análisis desde los momentos iniciales de la implementación. No medir a las personas, medir lo que nos preocupa, automatizar en lo posible, identificar los aspectos a mejorar, intentar conocer el rendimiento de los procesos para optimizarlos, son recomendaciones útiles en estas situaciones iniciales.

Relación con otros estándares/modelos

SCAMPI^{SM} (Standard CMMI Appraisal Method for Process Improvement) descrito en el MDD version 1.3b (Method Definition Document for SCAMPI A, B and C).

ISO/IEC 15504, también conocido como *Software Process Improvement Capability Determination*, abreviado SPICE, en español, «Evaluación de la Capacidad de Mejora del Proceso de Software».

Alineado con CMMI para Desarrollo, contamos con ISO/IEC 12207 *Information Technology / Software Life Cycle Processes*, es el estándar para los procesos de ciclo de vida del software.

Alineado con CMMI para Desarrollo, contamos con ISO/IEC 29110: Los perfiles de ciclo de vida del Software y las guías de estándares y reportes técnicos para

pequeñas organizaciones (VSEs de sus siglas en inglés - *Very Small Entities*) están dirigidas a las pequeñas organizaciones.

Alineado con CMMI para Servicios, contamos con la Biblioteca de Infraestructura de Tecnologías de Información, ITIL (del inglés *Information Technology Infrastructure Library*), es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.

Alineado con CMMI para Servicios, la serie ISO/IEC 20000 - *Service Management* normalizada es el estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información).

Dominio de Gestión de Proyectos

ISO 21500:2012

ISO 21500:2012 – Guidance on project management

Entidad Emisora

ISO 21500 es un estándar ISO que fue desarrollado por el Comité ISO / PC 236.

- **Disponibilidad**

El estándar Internacional ISO/IEC 21500 se puede adquirir directamente del catálogo en línea de la *International Organization for Standardization* (ISO) con el título "ISO 21500:2012 - *Guidance on project management*". El estándar se encuentra disponible para su adquisición en diferentes formatos (PDF, Paper y ePub) e idiomas (Inglés, Francés y Español) y puede comprarse en la web de ISO al precio de 140 Francos Suizos (a fecha de publicación de este documento): http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50003

También puede adquirirse en la web de AENOR, en formato PDF, en los idiomas español e inglés al precio de 47,46€ (a fecha de publicación de este documento): http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0050883&PDF=Si

Clasificación (taxonomía)

Normativa española e internacional.

- **Referencia normativa**

  ISO 21500 es el primero de una familia planificada de estándares de gestión de proyectos. Está diseñado para alinearse con estándares internacionales relacionados tales como ISO 10006:2003, Sistemas de gestión de la calidad - Directrices para la gestión de la calidad en los proyectos, ISO 10007:2003, Sistemas de gestión de la calidad - Directrices para la gestión de la configuración, ISO 31000:2009, Gestión de riesgos - Principios y directrices, y algunas estándares sectoriales en industrias como la aeroespacial y de TI.

Otros estándares /metodologías relacionados en este ámbito de conocimiento son: PMBOK (*Project Management Body of Knowledge*) del PMI (*Project Managemet Institute*) (http://www.pmi.org) y PRINCE2 (*PRojects IN Controlled Environments*) de la OGC (*Office of Government Commerce*) (http://www.prince-officialsite.com).

- **Ámbito de aplicación**

Este estándar Internacional proporciona orientación para la dirección y gestión de proyectos y puede usarse por cualquier tipo de organización, ya sea pública, privada, u organizaciones civiles sin ánimo de lucro; y para cualquier tipo de proyecto, con independencia de su complejidad, tamaño o duración.

El estándar va dirigido a:

- Alta dirección y patrocinadores de proyectos para ayudar a dar apoyo y orientación a sus directores de proyecto, equipos de dirección de proyectos y equipos de proyecto.
- Directores de proyecto, equipos de dirección de proyectos y equipos de proyecto ya que tendrán una base común para poder comparar sus estándares y prácticas de proyectos con las de otros.
- Redactores de estándares, como base para el desarrollo de estándares sobre gestión de proyectos, de modo que sean consistentes unos con otros.

- **Certificación**

Este estándar, de momento, no es certificable, aunque está en fase de estudio por el Comité ISO/TC258 la posibilidad de que más adelante sea posible. Aunque no se puede certificar, existen empresas que deciden implantar este tipo de metodología para alcanzar la excelencia en la Gestión de Proyectos.

Objetivos del estándar/modelo

Este estándar proporciona una descripción de alto nivel de conceptos y procesos que se consideran que forman parte de las buenas prácticas en dirección y gestión de proyectos. Los proyectos se ubican en el contexto de programas y carteras de proyectos, no obstante, este estándar no proporciona una orientación detallada para la gestión de programas y de carteras de proyectos. Los temas relativos a la gestión general se mencionan solamente en el contexto de la dirección y gestión de proyectos.

Agentes facilitadores para su adopción/implementación

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

Los beneficios de la implantación del estándar ISO 21500 en las organizaciones son:

- Fomentar la transferencia de conocimientos entre proyectos y organizaciones para mejorar la ejecución de los proyectos.
- Hacer eficientes los procesos de licitación mediante el uso de terminología coherente de gestión de proyectos.
- Habilitar la flexibilidad de los empleados de administración de proyectos y su capacidad para trabajar en proyectos internacionales.
- Proporcionar los principios universales de gestión de proyectos y procesos.

Reconocimiento/reputación

Según un informe del comité técnico TC 258 de fecha 14 de Septiembre de 2013, la ISO 21500 es el quinto estándar más vendido en el mundo (siendo el estándar ISO 9001 el más vendido).

Directrices sobre su uso/implementación

Los contenidos del estándar se estructuran en los siguientes apartados:

1. Objeto y campo de aplicación: Describe los conceptos y procesos que se consideran forman parte de las buenas prácticas en dirección y gestión de proyectos.

2. Términos y definiciones: Se indica una serie de términos y definiciones (16) de aplicación, empleados a lo largo del estándar. Dentro del propio estándar , también se define:

- Proyecto. Conjunto único de procesos que consta de actividades coordinadas y controladas, con fechas de inicio y fin, que se lleva a cabo para lograr los objetivos del proyecto.

- Programa. Grupo de proyectos relacionados y otras actividades alineadas con metas estratégicas.
- Cartera de Proyectos. Conjunto de proyectos, programas y otro tipo de trabajos que se agrupan para facilitar la gestión eficaz de dicho trabajo de modo que se cumplan las metas estratégicas.

3. Conceptos de la dirección y gestión de proyectos: Se describen una serie de conceptos clave que son aplicables a la mayoría de los proyectos:

- Relación entre la estrategia de la organización y los proyectos
- El entorno del proyecto (factores internos y externos a la organización, gestión de cartera y de programa de proyectos)
- La gobernanza del proyecto
- La distinción entre operaciones y proyectos
- La identificación de las partes interesadas y la organización del proyecto
- Las competencias del personal del proyecto
- El ciclo de vida y las restricciones del proyecto

4. Procesos de dirección y gestión de proyectos: Se identifican los procesos de dirección y gestión (39) y se ofrece una clasificación o agrupación de los mismos desde dos puntos de vista diferentes:

- Grupos de procesos:
  - Inicio
  - Planificación
  - Implementación
  - Control
  - Cierre
- Grupos de materias:
  - Integración
  - Parte interesada
  - Alcance
  - Recurso
  - Tiempo
  - Coste
  - Riesgo

- Calidad
- Adquisiciones
- Comunicación

Estos grupos son independientes del área de aplicación o enfoque industrial.

Anexo A (informativo) los procesos de los grupos de procesos puestos en correspondencia con los grupos de materias: Representación gráfica de las relaciones existentes entre los grupos de procesos y los grupos de materias.

Nota: Se recomienda que las organizaciones deben tener un Sistema de Gestión de Proyectos alineado con la ISO 21500 Project Management y aplicarlo utilizando herramientas y técnicas como las que se detallan en el PMBoK® de PMI, entre otros.

Relación con otros estándares/modelos

Otros estándares relacionados con la Gestión y Dirección de Proyectos son:

- PMBOK. Project Management Body of Knowledge
- ICB. International Competence Baseline
- PRINCE2. Project in Controlled Environments
- P2M. Project and Program Management for Enterprise Innovation
- BS 6079 parts 1 to 4. Guide to Project Management
- DIN 69901 parts 1 to 5. Project Management. Project Management Systems
- ISO 10006. Quality Management Systems. Guideline for Quality Management in Project
- AS 4915. Project Management. General Conditions
- ISO 31000 Gestión de Riesgos

El próximo estándar relacionado será la ISO 21502 "Gestión del Portfolio".

PMBOK 5.0

PMBOK versión 5.0 – Project Management Body of Knowledge

Entidad Emisora

El PMBoK® Guide, Fifth Edition (A Guide to the Project Management Body of Knowledge) de PMI® (Project Management Institute) es un estándar ANSI (American National Standard Institute) para la profesión de Gestión de Proyecto.

El *Project Management Institute* (PMI)® (http://www.pmi.org/)es una de las mayores asociaciones de membresía profesional del mundo, con más de medio millón de miembros y personas certificadas en más de 185 países. Es una organización sin ánimo de lucro que promueve la profesión de gestión de proyectos a través de estándares mundialmente reconocidos y certificados, las comunidades de colaboración (capítulos), un extenso programa de investigación y oportunidades de desarrollo profesional.

- **Disponibilidad**

Si se es socio de PMI se puede descargar gratuitamente un documento PDF con la versión en inglés de la Guía de los Fundamentos para la Dirección de Proyectos (PMBOK).

Se obtiene un fichero PDF encriptado con tu clave de PMI y con tu nombre al pie de cada página.

El libro en papel puede solicitarse en PMI *Marketplace*. El precio es de 49,50$ para socios y 65,95$ para no socios. Los precios son a fecha de publicación de este documento.

Clasificación (taxonomía)

Es un estándar ANSI.

- **Referencia normativa**

PMBOK ® v5.0. La última versión en inglés de la guía PMBOK Guide, la quinta edición, se liberó el pasado 31 de diciembre de 2012. . La versión en español se publicó en enero de 2014.

El estándar ISO 21500 *Guidance on project management* es otro estándar directamente relacionado con el ámbito de Dirección y Gestión de Proyectos.

- **Ámbito de aplicación**

La guía describe el conocimiento y las técnicas universalmente aceptadas y necesarias para completar con éxito cualquier Proyecto de cualquier ámbito o sector.

La certificación como *Project Management Professional* (PMP)® del *Project Management Institute* (PMI)®, está reconocida internacionalmente como un estándar para acreditar el conocimiento y experiencia de los profesionales en los principios, metodologías y técnicas de Gestión/Dirección de Proyectos.

- **Certificación**

PMP es una titulación creada en 1984 válida sólo para personas. No se certifican organizaciones en PMBOK.

Para inscribirse al examen PMP, se cumplimentará una solicitud en la página web del PMI. Una vez que el PMI ha recibido la solicitud, se procesa y revisa en 5 días hábiles y se envía por email la notificación de aceptación o no aceptación para poder presentarse al examen.

En el caso de aceptación:

- Comienza el período de elegibilidad, que es de un año, en el cual se puede presentar al examen
- Se puede ser auditado por el PMI (en este caso avisarán)
- Hay que pagar los derechos de examen (*Exam Fee*)
- Hay que reservar plaza en un centro *Prometric Testing Center*. Antes de ello, es necesario disponer del número de elegibilidad que envía el PMI.

Los requisitos para certificarse son:

- Experiencia y/o formación demostrable
- Titulación grado medio (ó superior)
- 7.500 horas en 60 meses como Jefe de Proyecto (ó 4.500 h, 36 m.)
- Curso Preparación Examen PMBOK®: 35 horas

- Superar un Examen tipo test:

200 preguntas en 4 horas

175 preguntas reales (25 de relleno)

Aprobado si 106 aciertos

Otras titulaciones PMI:

- CAPM® (Certified Associate in Project Management)
- PgMP® (Program Management Professional)
- PMI-SPSM (PMI Scheduling Professional)
- PMI-RMPSM (PMI Risk Management Professional
- PMI-ACP (PMI Agile Certified Professional)

Para mantener la certificación requiere demostrar una formación continua *(Continuing Certification Requirements (CCR) Program*). Se deben obtener 60 PDUs (*Program Development Units*) en cada ciclo de 3 años. Las PDUs pueden obtenerse vía:

- Formación reglada
- Auto-Formación y actividades profesionales
- Cursos de REPs (PMI Registered Education Providers)
- Cursos de otros proveedores
- Servicios a asociaciones profesionales

Los PMP están sometidos a un Código de Conducta Profesional. Un PMP debe ser Responsable, Respetuoso, Ecuánime y Honesto.

Objetivos del estándar/modelo

Los objetivos principales de PMBOK son:

- Identificar y describir un conjunto de conocimientos y técnicas de gestión de proyecto generalmente aceptado. Generalmente aceptado quiere decir que el conocimiento y las técnicas descritas son aplicables a la mayoría de los proyectos la mayoría de las veces, y que hay un consenso amplio sobre su valor y utilidad. Generalmente aceptado no quiere decir que las prácticas y el conocimiento son o deben ser aplicadas uniformemente a

todos los proyectos; el equipo de gestión de proyectos siempre será responsable de determinar que es apropiado para cualquier proyecto dado.

- Proveer un léxico común dentro de la profesión para poder hablar de la gestión de proyectos. Mientras que hay un entendimiento de que es lo que hace en la gestión de proyecto, hay poco conocimiento relativo a los términos que se usan.

Agentes facilitadores para su adopción/implementación

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

Se identifican las ventajas de la certificación PMP desde dos puntos de vista. Desde la persona certificada y desde la organización que cuenta con profesionales certificados.

Las principales ventajas de certificarse PMP son:

16. Mostrar el compromiso con la profesión de gestión de proyectos, el código ético de PMI y la capacidad para desempeñar las funciones de un profesional de la gestión de proyectos a un nivel determinado.
17. Reconocer los conocimientos, las habilidades y las capacidades en la gestión de proyectos a nivel mundial.
18. Reflejar las capacidades en gestión de proyectos mediante el cumplimiento de los requisitos normativos establecidos por PMI.
19. Incrementar las oportunidades de empleo y promoción profesional, al demostrar competencia en los procesos de gestión de proyectos o en el conocimiento y experiencia en las áreas de especialidad de la práctica basada en estándares de la industria.
20. Actualizar continuamente los conocimientos de gestión de proyectos, ya que PMI promueve y apoya el desarrollo profesional continuo.

Las principales ventajas para una organización que cuenta con profesionales certificados PMI son:

21. Establecer un lenguaje y un marco de trabajo común para la gestión de proyectos.
22. Tendrán procesos repetibles y mejores resultados en el proyecto. La gestión de proyectos basada en PMI requiere identificar y establecer lecciones aprendidas y compartir activos de los procesos.
23. Garantizar la competencia de los jefes de proyectos para desempeñar las funciones y asumir las responsabilidades de su rol. Ya que los certificados PMP satisfacer los Requisitos del Programa Certificación Continua (CCR) para

mantener un estado de certificación activo. El programa CCR exige a los certificados PMP participar en actividades de desarrollo profesional durante todo el año.

24. Los clientes de la organización tendrán una mayor confianza porque su equipo de proyecto utiliza una terminología y prácticas comunes y reconocidas internacionalmente.
25. Los clientes tendrán una mayor confianza porque el equipo de proyecto con certificación PMI está sujeto al Código de Ética y Conducta Profesional de PMI, que muestra a los clientes de que su equipo de trabajo opera con integridad.

Reconocimiento/reputación

El Certificación PMP es la más distinguida y valorada a nivel mundial en esta área, que se ha triplicado en número en los últimos cinco años. Como PMP, los profesionales son reconocidos como miembros del grupo de practicantes certificados internacionalmente más exitosos de la profesión de la Dirección de Proyectos.

El programa PMP es un proceso de certificación como mecanismo de calificación profesional, que mide el conocimiento y la comprensión de las disciplinas del PMBOK Guide.

Directrices sobre su uso/implementación

PMBOK considera la gestión de proyectos en 47 procesos a lo largo de 10 áreas de conocimiento agrupados en 5 "grupos de procesos".

Los Grupos de Procesos son:

26. **Grupo de Procesos de Iniciación.** Define y autoriza el proyecto o una fase del mismo.
27. **Grupo de Procesos de Planificación.** Refina los objetivos y planifica las acciones requeridas para lograr los objetivos dentro del alcance del proyecto.
28. **Grupo de Procesos de Ejecución.** Integra personas y recursos para llevar a cabo el plan de dirección.
29. **Grupo de Procesos de Seguimiento y Control.** Mide y supervisa regularmente el avance, a fin de identificar las variaciones respecto del plan de dirección, de tal forma que se puedan tomar medidas correctivas si fuera necesario para alcanzar los objetivos del proyecto.
30. **Grupo de Procesos de Cierre.** Formaliza la aceptación del producto o servicio, termina el proyecto o una fase del mismo, comunicando su consecución y documentando las lecciones aprendidas.

Los grupos de procesos aplican a las 10 áreas de conocimiento que considera la versión actual del PMBOK:

31. **Integración**: Incluye los procesos y actividades necesarios para identificar, definir, combinar, unificar y coordinar los diversos procesos y actividades de la gestión de proyectos dentro de los grupos de procesos.
32. **Alcance**: Incluye los procesos necesarios para garantizar que el proyecto incluya todo (y únicamente todo) el trabajo requerido para completarla con éxito.
33. **Tiempo**: Incluye los procesos requeridos para gestionar la finalización del proyecto a tiempo.
34. **Costes:** Incluye los procesos involucrados en estimar, presupuestar y controlar los costes, de modo que se complete el proyecto dentro del presupuesto aprobado.
35. **Calidad**: Incluye los procesos y actividades de la organización ejecutante que determinan responsabilidades, objetivos y políticas de calidad a fin de que el proyecto satisfaga las necesidades por las que se ejecuta.
36. **Recursos Humanos**: Incluye los procesos que organizan, gestionan y coordinan el equipo del proyecto.
37. **Comunicaciones**: Incluye los procesos requeridos para garantizar que la generación, la recopilación, la distribución, el almacenamiento, la recuperación y la disposición final de la información del proyecto sean adecuados, oportunos y entregada a quien corresponda (interesados del proyecto o *stakeholders*).
38. **Riesgos**: Incluye los procesos relacionados con llevar a cabo la planificación de la gestión, identificación, el análisis, y la planificación de las acciones de contingencia a los riesgos, así como su seguimiento y control en un proyecto.
39. **Adquisiciones**: Incluye los procesos de compra o adquisición de los productos, servicios o resultados que es necesario obtener fuera del equipo del proyecto.
40. **Interesados *(Stakeholders):*** Incluye los procesos involucrados en identificar a los interesados del proyecto o *stakeholders*, así como la planificación, gestión y control de sus expectativas sobre el proyecto.

Cada área de proceso contiene a su vez procesos (entradas, salidas, y técnicas para ejecutarlos).

Relación con otros estándares/modelos

Otros estándares o modelos relacionados con PMBOK son:

- ISO 21500 Guidance on project management
- PRINCE2. Project in Controlled Environments

- ICB. International Competence Baseline
- P2M. Project and Program Management for Enterprise Innovation
- BS 6079 parts 1 to 4. Guide to Project Management
- DIN 69901 parts 1 to 5. Project Management. Project Management Systems
- ISO 10006. Quality Management Systems. Guideline for Quality Management in Project
- AS 4915. Project Management. General Conditions
- ISO 31000 Risk Management

Gobierno Corporativo y Gestión TIC

UNE-ISO/IEC 20000-1:2011

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

Entidad Emisora

ISO/IEC 20000-1 es un estándar ISO y de IEC, publicada por primera vez el 14 de diciembre de 2005. En 2006, el estándar internacional es publicado por AENOR como el estándar UNE, siendo entonces UNE-ISO/IEC 20000.

Es el estándar reconocido internacionalmente en gestión de servicios de TI. La serie 20000 proviene de la adopción de la serie BS 15000 desarrollada por la entidad de normalización británica, la *British Standards Institution* (BSI).

- **Disponibilidad**

El documento puede comprarse en AENOR www.aenor.es al precio de 41,69 € (a fecha de publicación de la ficha), y en la web de ISO www.iso.org la versión del estándar en inglés al precio de 116 CHF (fecha de publicación de la ficha).

Clasificación (taxonomía)

El estándar UNE-ISO/IEC 20000-1 forma parte de una familia de estándares nacional que aplica al diseño, transición, entrega y mejora de servicios, que cumple con los requerimientos de servicios y provee valor para el cliente y para el proveedor del mismo.

- **Referencia normativa**

El estándar UNE-ISO/IEC 20000-1 proviene de la serie BS 15000 desarrollada por la entidad de normalización británica, BSI. BS 15000 fue el primer estándar desarrollado para la gestión de Servicios de TI, y refleja la "guía de las mejores prácticas" contenidas en la librería ITIL (*Information Technology Infrastructure Library*).

Aplicar las mejores prácticas de la librería ITIL ayudará a la organización de TI a alcanzar la calidad en la gestión de servicio requerida por este estándar.

El estándar UNE-ISO/IEC 20000-1 consta de las siguientes partes bajo el título general de *Tecnología de la Información. Gestión del Servicio*:

- Parte 1: Requisitos del sistema de Gestión de Servicio (SGS). *Parte certificable*.
- Parte 2: Directrices o Código de Prácticas.
- Parte 3: Directrices para la definición del alcance.
- Parte 4: Modelo de referencia de procesos.
- Parte 5: Plan de implementación ejemplar.

- **Ámbito de aplicación**

Este estándar /modelo es aplicable a todo tipo de organizaciones, independientemente de su tamaño, y tiene su aplicación principal en los siguientes aspectos:

- Proveer una del estándar de referencia común para toda la organización que ofrece servicios de TI tanto a clientes internos como externos.
- Promover la adopción de un conjunto de procesos integrados para la gestión de servicios de TI, cubriendo el modelo de los procesos ITIL de soporte y provisión de servicios de TI.

Algunos autores proponen su uso para la gestión de cualquier servicio, no necesariamente de Tecnologías de la Información, aunque hasta la fecha su utilización no se ha extendido en otros ámbitos.

- **Certificación**

El estándar ISO/ICE 20000-1 es certificable por cualquier organismo acreditado por el APMG Internacional. Algunos de los organismos certificadores en España: AENOR, Bureau Veritas, SGS, Lloyds.

Objetivos del estándar

El estándar UNE-ISO/IEC 20000-1, es un estándar internacional que aplica al diseño, transición, entrega y mejora de servicios, que cumple con los requerimientos de servicios y provee valor para el cliente y para el proveedor del mismo.

Agentes facilitadores para su adopción/implementación

Dentro de los agentes facilitadores para su implementación estarían los siguientes:

- La existencia de una cultura de gestión de procesos y de mejora continua.
- La necesidad por parte del departamento interno o del proveedor de servicios de TI de implantar buenas prácticas en la gestión de su servicio. También las organizaciones que ya tienen implantadas dichas prácticas de acuerdo con la librería ITIL tendrán facilitada la implantación de este estándar.
- La necesidad de acreditar la conformidad de la gestión del servicio de TI con este estándar requerido por un cliente público o privado. Las organizaciones que presentan una certificación UNE-ISO/IEC 20000-1 demuestran profesionalidad y rigor contrastables en el control y la gestión de los servicios TI que ofrecen. Cada vez más, esta del estándar está siendo puntuada positivamente en los concursos y ofertas de servicios TI.
- La implementación adecuada de este estándar es un medio muy potente para reforzar la comunicación a/hacia los clientes (internos o externos) y también con suministradores.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

UNE-ISO/IEC 20000-1 se presenta como una ventaja competitiva para las organizaciones que la implantan. Éstas son algunas de las ventajas que obtienen las organizaciones que sí la utilizan:

- Alineamiento con el Negocio: El objetivo último del estándar es alinear el servicio de TI y su gestión con el negocio. El estándarUNE-ISO/IEC 20000-1 proporciona a las compañías o departamentos que la implantan un marco de referencia para tratar con profesionalidad la gestión de los servicios TI, de forma que éstos sirvan al Negocio y no a la tecnología.
- Buenas Prácticas: Cualquier servicio de TI interno o externo debe gestionarse siguiendo unas Buenas Prácticas reconocidas y probadas. UNE-ISO/IEC 20000-1 es un estándar certificable basado en ITIL, el estándar de facto del mercado.
- Mejora Continua: Al igual que otras estándares de Calidad, el estándar UNE-ISO/IEC 20000-1 se encuentra enfocado hacia la mejora continua a través de la aplicación del ciclo de Mejora Continua o PDCA, lo que debe asegurar una mejora progresiva de los niveles de eficiencia y eficacia de la organización en un proceso continuo de aprendizaje.
- Sostenibilidad: La certificación en sí no es siempre lo importante y probablemente menos en servicios internos, pero tiene la ventaja de poner objetivos en el tiempo y mantener la tensión de la organización a través de las auditorías periódicas.

El principal riesgo derivado de su no implantación, radica en la ausencia de un sistema de gestión que asegure que el servicio de TI proporcionado a la organización

esté controlado adecuadamente y dirigido a satisfacer las necesidades de su cliente (interno en caso de departamento de TI, externo para un proveedor de servicios de TI).

Especialmente para los departamentos de servicio interno, su ausencia puede llevar consigo también que el servicio de TI se vea como una carga costosa y no como una ayuda imprescindible para lograr los objetivos del negocio.

Reconocimiento/reputación

Existen más de 130 compañías en España, certificadas en este estándar internacional, tanto en su versión 2005 y 2011.

Dentro del abanico de empresas certificadas, están tanto compañías de servicios de TI, como departamentos TI internos de compañías de otros ámbitos.

Directrices sobre su uso/implementación

Este estándar promueve la adopción de un sistema de gestión por procesos integrados para la gestión del servicio. Describe trece procesos organizados como se muestra en la figura:

Ilustración 5 Sistema de Gestión del servicio

Un proyecto de implantación de UNE-ISO/IEC 20000-1 consta de cuatro fases:

41. Análisis y planificación
42. Diseño e implantación
43. Periodo de transición
44. Operación

Fase 1. Análisis y Planificación

Es altamente recomendable comenzar realizando un *assessment* (valoración) para analizar el punto de partida del área de TI con respecto a los requisitos del estándar. Los hallazgos identificados en esta valoración supondrán la entrada para la implementación del SGS (Sistema de Gestión del Servicio).

Se determina el alcance para la certificación.

Se realiza la planificación de la implementación de manera gradual, con un objetivo inicial de certificación.

Fase 2. Diseño e implantación

En entidades que ya dispongan de un sistema de gestión de la calidad, se recomienda realizar la adecuación del Sistema de Gestión existente a los requisitos del estándar ISO 20000, de modo que pueda constituir el marco para los nuevos procesos a implementar.

Se inicia la definición de los requisitos del sistema, incluyendo:

Plan de Gestión de Servicios

Catálogo de servicios

Objetivos del sistema

En paralelo, se inicia también la definición e implementación de los nuevos procesos. El orden recomendado de la definición de los 13 procesos de ISO 20000 es el siguiente:

45. **Procesos de Control**. En este punto, se calculan los costes por servicios para el Proceso de Gestión Financiera.
46. **Procesos de Resolución**. En muchos casos, estos procesos de resolución y control se definen e implementan en una herramienta. Se realizan las primeras tareas de formación y concienciación del personal.

47. **Procesos de provisión, relación y el proceso de diseño y transición de servicios**. Se empiezan a analizar los primeros planes y Acuerdos de Nivel de Servicio (SLA).

Fase 3. Transición

Primera auditoría interna UNE-ISO/IEC 20000-1:2011. Se realiza una auditoría interna para conocer el grado de adecuación de los procesos definidos e implementados. Se obtiene un plan de acción para resolver las no conformidades y observaciones.

Se empieza a trabajar en la implementación de acciones de mejora y acciones correctivas para resolver los hallazgos detectados en la auditoría interna y obtener un sistema de gestión acorde a la UNE-ISO/IEC 20000-1.

Se acuerdan con los *Keyusers* (o representantes del cliente) los primeros SLAs.

Se completan las versiones finales de los planes de continuidad, disponibilidad y capacidad.

Se inician los seguimientos periódicos de los procesos.

Fase 4. Operación

Todos los procesos se encuentran operativos.

Se colectan evidencias del cumplimiento de todos los procesos

Recomendaciones generales

- Nunca se recomienda certificar en una primera implantación todos los servicios de TI de la organización. La correcta selección del alcance influirá decisivamente en el éxito de la implantación.

  Éstos son los criterios de selección de servicios para certificar:

  - Elegir un número de servicios significativo, que permita una adecuada implantación de los nuevos procesos para una posterior y progresiva extensión de los mismos.
  - Servicios relevantes para la Compañía
  - Servicios básicos con impacto en otros servicios del catálogo de TI.
  - Los procesos transversales se aplican a la totalidad del servicio proporcionado por el proveedor del servicio (interno o externo), no sólo a los servicios dentro del alcance.

- La definición de los procesos debe ser sencilla, de modo que no constituya un esfuerzo adicional que haga fracasar la integración de estas prácticas en la operación diaria del servicio.
- En los procesos que requieren desarrollos o herramientas específicas para los servicios certificables, estas herramientas deben seleccionarse e implementarse con criterios de poder ampliar su alcance al resto de servicios. Sin embargo, hay que ser cuidadoso a la hora de hacer que la herramienta sirva al proceso y no adaptar el proceso a la herramienta.
- Criterios de una buena implantación:
  - Integrar UNE-ISO/IEC 20000-1 en el sistema de gestión de la compañía, si lo hubiera.
  - El Punto 4 del estándar queda cubierto en su mayor parte con el punto 4 de la ISO 9001, recomendándose su revisión.
- Para una primera implantación, se recomienda un alcance medio, pudiendo ser ampliado en sucesivas revisiones. Se sugiere empezar eligiendo servicios maduros y con un cierto valor para el negocio.

Relación con otros estándares/modelos

De manera particular, los principales modelos y estándares relacionados son los siguientes:

UNE-ISO 9001 Sistemas de Gestión de la Calidad

El Punto 4 de UNE-ISO 20000-1 queda cubierto en su mayor parte con el punto 4 de la UNE-ISO 9001. Las organizaciones que tengan una certificación del Sistema de Calidad obtendrán beneficios con la integración de los sistemas de gestión.

UNE-ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.

Las organizaciones certificadas en UNE-ISO/IEC 27001 satisfarán los requerimientos de seguridad recogidos en la UNE-ISO/IEC 20000-1

UNE-ISO 22301 Sistema de Gestión de la Continuidad del Negocio (SGCN).

Las organizaciones certificadas en UNE-ISO/IEC 22301 satisfarán completamente los requerimientos de continuidad recogidos en la UNE-ISO/IEC 20000-1, así como gran parte de los requisitos de disponibilidad.

ITIL Information Technology Infrastructure Library

Como se dijo anteriormente, las organizaciones que sigan las buenas prácticas recogidas en la librería ITIL tendrán ventajas claras para implantar los requisitos de UNE-ISO/IEC 20000-1.

UNE-ISO 38500 Gobernanza corporativa de la Tecnología de la Información (TI).

CobiT Control Objectives for Information and Related Technology
Tanto UNE-ISO 38500 como CoBiT, ofrecen marcos de referencia superiores para el Gobierno de los Sistemas de Información. La búsqueda de la eficiencia en el servicio de TI de UNE-ISO 20000-1 se complementa con la visión estratégica que proporcionan estos estándares.

De manera más general, el estándar UNE-ISO/IEC 20000-1 tiene relaciones con otras Buenas Prácticas y estándares tales como las que se ven en el siguiente esquema:

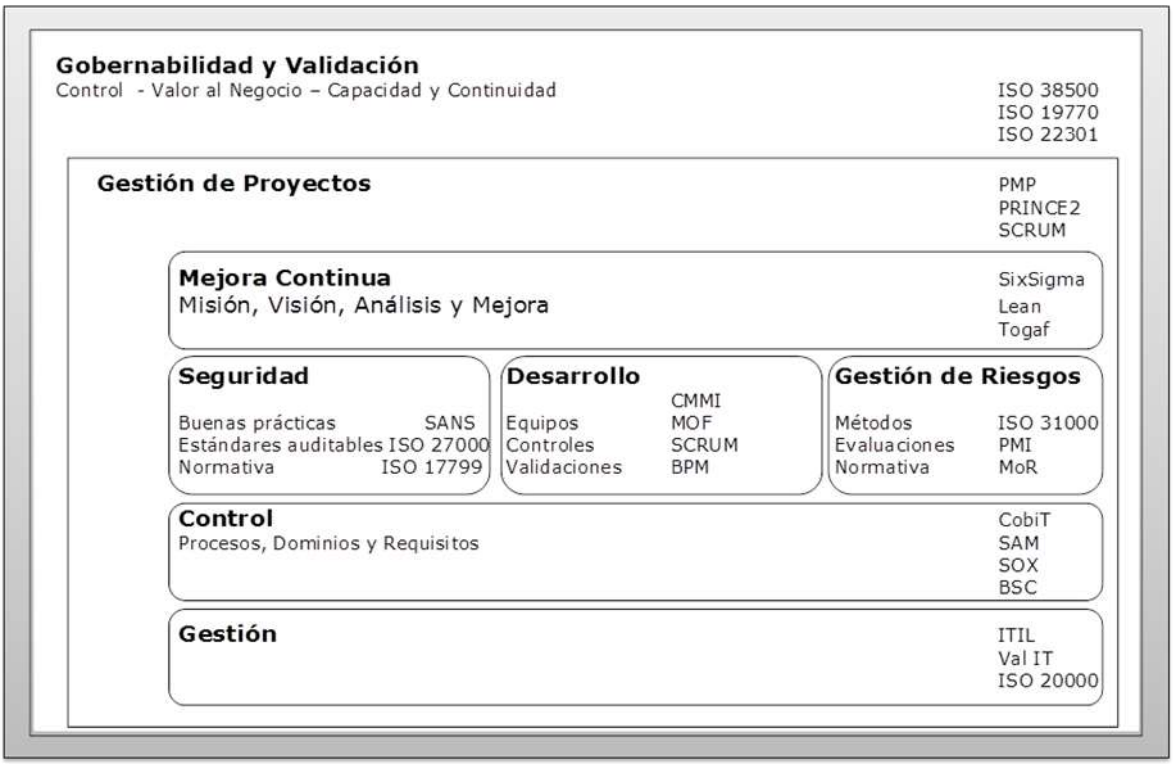

Ilustración 6 Esquema de relaciones entre normas

ITIL

ITIL – Information Technology Infrastructure Library

Entidad Emisora

ITIL es una guía de buenas prácticas para la gestión de los servicios de TI, desarrollada en las décadas de los 80 y 90 por la CCTA (*Central Computer and Telecommunication Agency*), ahora OGC (*Office of Government Commerce*) bajo contrato de Gobierno Británico. Ha sido actualizado en tres ocasiones: en 2000-2002 (V2), en 2007 la V3 y en 2011 una nueva modificación a la V3.

La OGC es la propietaria de ITIL y la APM Group (APMG) gestiona los derechos de ITIL a la OGC, la certificación de exámenes de ITIL y la acreditación de las organizaciones de formación. APMG define la certificación y acreditación para los exámenes de ITIL y publica el nuevo sistema de certificación.

El itSMF (*Information Technology Service Management Forum*), es la comunidad mundial de conocimiento para compartir prácticas sobre el gobierno y la gestión del servicio de las Tecnologías de la Información (TI).

itSMF España forma parte de la comunidad mundial de dichas prácticas. Su actividad también gira en torno a la creación y difusión de las buenas prácticas y las experiencias relativas a la gestión de los servicios y el gobierno de las TI. Está centrada en intercambiar puntos de vista, compartir experiencias y participar en el desarrollo continuo de mejores prácticas y estándares.

- **Disponibilidad**

A través del itSMF se puede tener acceso a gran cantidad de información así como de sitios y empresas que comercializan los libros de ITIL. Una de las entidades es "*it governance"* que comercializa los libros en español por 365€, y por separado, cada libro a 100€ aproximadamente.

Clasificación (taxonomía)

La biblioteca de Infraestructuras de Tecnologías de la Información, ITIL, ha sido la base para la creación de una familia de estándares internacional que aplican al

diseño, transición, entrega y mejora de servicios, que cumple con los requerimientos de servicios y provee valor para el cliente y para el proveedor del mismo. Pero ITIL, no solo se centra en la operación del servicio, sino que sus libros abarcan todo el ciclo de vida del servicio de TI.

No es un estándar certificable como ISO 20000, sino una guía de buenas prácticas y un marco de trabajo, que consta de 5 libros:

Estrategia del servicio

Diseño del servicio

Transición del servicio

Operación del servicio

Mejora continua

Cada uno de libros consta de varios "Procesos" que en total se cuentan en 26.

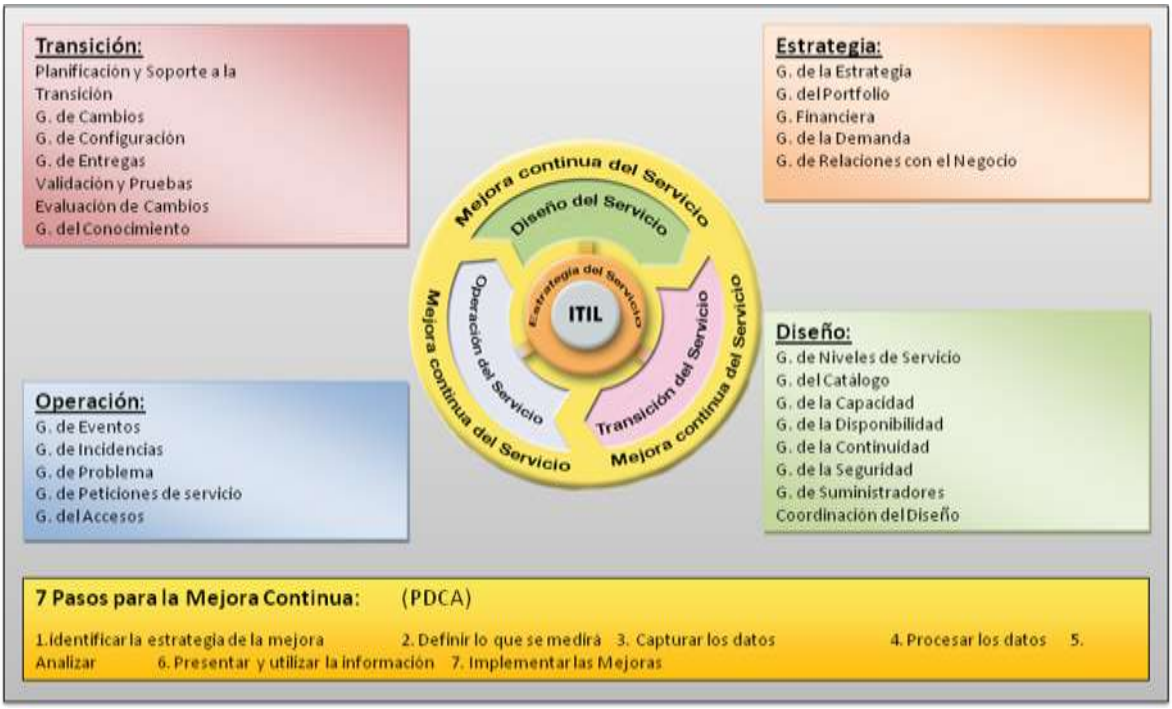

Ilustración 7 ITIL v3

- **Referencia normativa**

El estándar ITIL, que no una "norma", es un estándar internacional "de facto" para la Gestión de Servicios de TI. Los responsables de TI fueron tomando consciencia de la importancia de la Gestión de Servicios de TI y desarrollaron una terminología conjunta para tal fin. Esta es una condición imprescindible también en situaciones en las que el servicio de la infraestructura de TI tiene que ser externalizado, ya que mediante ITIL se pueden definir en estos casos las relaciones necesarias entre clientes y proveedores. La filosofía de ITIL se ha expandido desde entonces también a otros modelos de la Gestión de Servicios de TI, y les ha servido como base, como por ejemplo:

- ISO 20000 (antes BS 15000): Sistema de Gestión de Servicios de TI
- ITSM Reference Model

- **Ámbito de aplicación**

Este modelo de buenas prácticas es aplicable a todo tipo de organizaciones, independientemente de su tamaño, y tiene su aplicación principal en los siguientes aspectos:

- Proveer una referencia común para toda la organización que ofrece servicios de TI tanto a clientes internos como externos.
- Promover la adopción de un conjunto de procesos integrados para la gestión de TI cubriendo el ciclo de vida del servicio.

- **Certificación**

El modelo de mejores prácticas de ITIL, no es certificable para una organización, sino que es base para adoptar alguna de las normas certificables como ISO 20000, SOX, y otras.

El modelo de certificación de ITIL es individual, aunque una empresa puede adoptarlo como base para la formación en estas mejores prácticas para sus empleados.

El esquema de certificación individual consta de 4 niveles:

- Nivel Fundamental
- Nivel Intermedio

Experto en ITIL

Diploma de profesional avanzado en Gestión de Servicios TI

ITIL

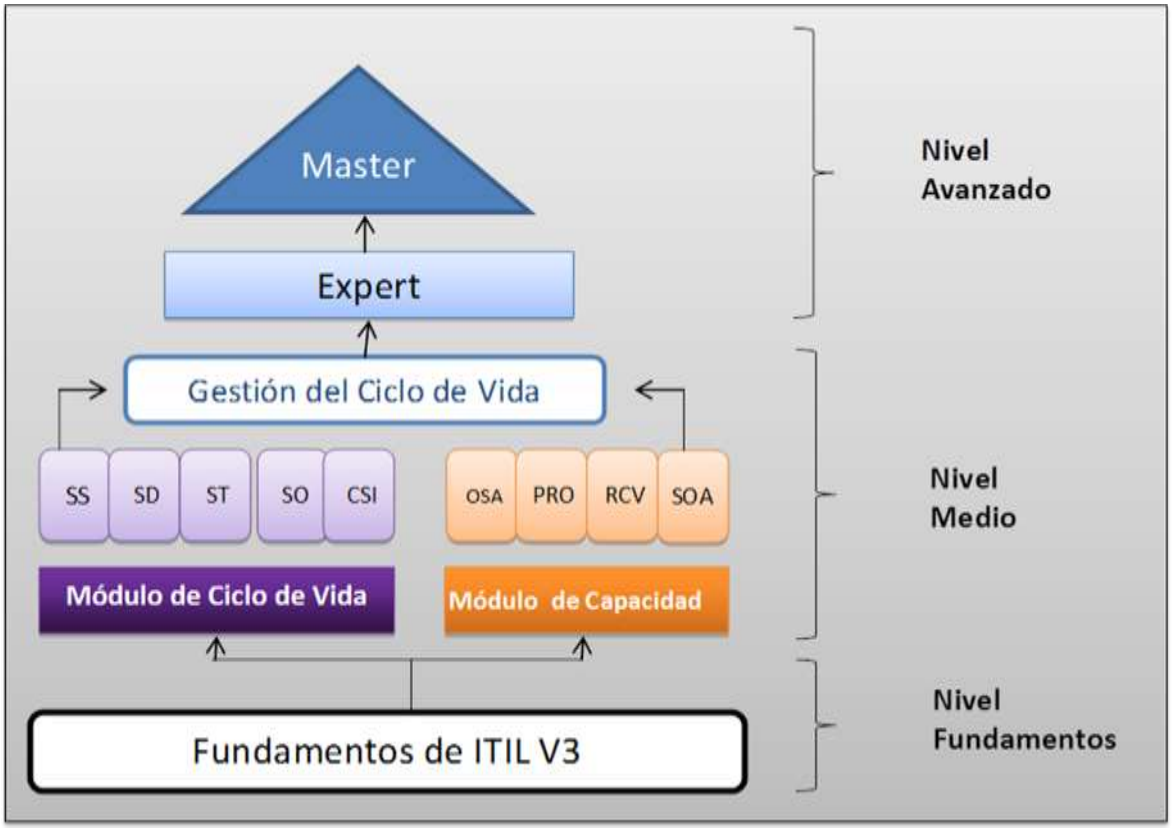

Ilustración 8 esquema de niveles ITIL V3

APM Group, organismo que gestiona las certificaciones, ha acreditado a diversos organismos examinadores en el mundo para facilitar la organización de exámenes. Hay empresas que ofrecen la formación con el correspondiente examen de acreditación.

Objetivos del estándar

Su principal objetivo es "Alinear la Tecnología al Negocio de acuerdo a una Gestión del Servicio de TI basada en Procesos", proporcionando un marco de referencia para hacerlo.

Además la Gestión es tal que apoya los procesos del Negocio. Se pone especial atención, a la Gestión de Cambios, que es el proceso con mayor responsabilidad en dicha alineación entre la Tecnología y el Negocio.

La intención era por lo tanto encontrar una vía para mejorar de forma duradera estos servicios reduciendo al mismo tiempo los costes. El objetivo consistía en desarrollar procedimientos efectivos y económicos para la oferta de servicios de TI. Se elaboró un catálogo de las llamadas "Recomendaciones de Mejores Prácticas" para la organización de TI, que se encuentran hoy en día documentadas en ITIL.

Aplicar las mejores prácticas de la librería ITIL ayudará a la organización de TI a alcanzar la calidad en la gestión de servicio.

Agentes facilitadores para su adopción/implementación

Dentro de los agentes facilitadores para su implementación estarían los siguientes:

- Es neutral respecto a plataformas de tecnologías
- Son Buenas Prácticas, no es una metodología ni son reglas. Se mantiene independiente de fabricantes, marcas, metodologías y compañias de Servicio.
- Como su objetivo es alinear la Tecnología con el Negocio, se aplican aquéllas guías y consejos de aquéllas prácticas que han demostrado ser efectivas, pero sin que sea mandatorio y dejando a cada organización la adaptación de las que necesite adaptar.
- Como se enfoca al "ciclo de vida de los servicios" se mantienen algunos principios como:

Procesos para alinear el Negocio y la Gestión de Servicios TI mediante la mejora contínua de los servicios y no enfocado a la Tecnología.

Creación de Valor, alineando con las normas de Calidad, por eso se basa en los sistemas de Calidad como la ISO9000, la ISO2000 y el modelo de Calidad Total como el modelo europeo EFQM.

El Cliente es el beneficiario directo de la entrega y resultados de los servicios.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

Las buenas prácticas de ITIL se presentan como una ventaja competitiva para las organizaciones que la implantan. Éstas son algunas de las ventajas que obtienen las organizaciones que sí la utilizan:

- Alineamiento con el Negocio: como se ha visto anteriormente, el objetivo del estándar es alinear la Tecnología y su gestión, con el Negocio. La aplicación de ITIL proporciona a las compañías o departamentos que la implantan un marco de referencia para tratar con profesionalidad la gestión de los servicios TI, de forma que éstos sirvan al Negocio y no a la tecnología.
- Buenas Prácticas: Cualquier servicio de TI interno o externo debe gestionarse siguiendo unas Buenas Prácticas reconocidas y probadas. Por eso la aplicación de ITIL, es tan importante para dicha gestión.
- Mejora Continua: Al igual que otros estándares de Calidad, ITIL se encuentra enfocado hacia la mejora continua a través de la aplicación del ciclo de Mejora Continua o PDCA, lo que debe asegurar una mejora progresiva de los niveles de eficiencia y eficacia de la organización en un proceso continuo de aprendizaje.
- Ciclo de Vida del Servicio: La esencia de la gestión basada en las buenas prácticas es la aplicación del ciclo de vida del servicio. Como se ve en las figuras, el corazón de ITIL es la Estrategia, donde se gestan todos los planes de la gestión. Luego los servicios son Diseñados para ser enviados a Transición que los va a realizar y desplegar en producción donde la Operación los Entregará y les dará soporte. Todo esto está rodeado de Mejora Continua para encontrar oportunidades de Mejora de los servicios.
- Sostenibilidad: La certificación en sí no es siempre lo importante y probablemente menos en servicios internos, pero tiene la ventaja de poner objetivos en el tiempo y mantener la tensión de la organización a través de las auditorías periódicas. No existe acreditación ITIL para las empresas u organizaciones, sino que como ya se ha dicho, la acreditación se asocia a individuos. Pero se puede hacer con otras normas del mercado que se basan en ITIL como la ISO 20000. (ver ficha ISO 20000).

La principal debilidad de la implantación de las buenas prácticas de ITIL, sin el acompañamiento de una norma que lo acredite, es la falta de métricas que ayuden a medir su desarrollo, el nivel de madurez y retorno de la inversión hecha en la Gestión de Servicios de TI. Las métricas de las normas ISO/IEC 20000 proporcionan esa ayuda.

El principal riesgo derivado de su no implantación radica en la ausencia de un sistema de gestión que asegure que el servicio de TI proporcionado a la organización esté controlado adecuadamente y dirigido a satisfacer las necesidades de su cliente (interno en caso de departamento de TI, externo para un proveedor de servicios de TI).

Especialmente para los departamentos de servicio interno, su ausencia puede llevar consigo también que el servicio de TI se vea como una carga costosa y no como una ayuda imprescindible para lograr los objetivos del negocio.

Reconocimiento/reputación

Existen miles de personas acreditadas en el mundo, en los distintos niveles de ITIL.

En el apartado **Certificación**, se ha podido leer los distintos niveles de certificación individual que existen. El *ITIL Foundation*, que es el más básico, evidentemente es el que más acreditaciones tiene en su haber.

Una compañía que tiene sus profesionales acreditados en ITIL, seguro que tendrá más herramientas y capacidad para llegar a una buena Gestión de los servicios alineados e integrados con el Negocio.

Directrices sobre su uso/implementación

La adopción y aplicación de las buenas prácticas de ITIL, promueve la adopción de un sistema de gestión por procesos integrados para la gestión del servicio. Describe 26 procesos organizados como se describe en el apartado 2. Taxonomía.

Aunque como ya se ha dicho ITIL no es una metodología, por tanto, no entra en conflicto con otros marcos de aplicación utilizados en las tecnologías de la información.

Hay que tener en cuenta que la esencia de la Gestión de Servicios basada en ITIL es la aplicación del Ciclo de Vida del Servicio. Así, un proyecto de implantación de la Gestión de Servicios TI de acuerdo con ITIL, podría tener las siguientes fases, acorde con el ciclo de vida:

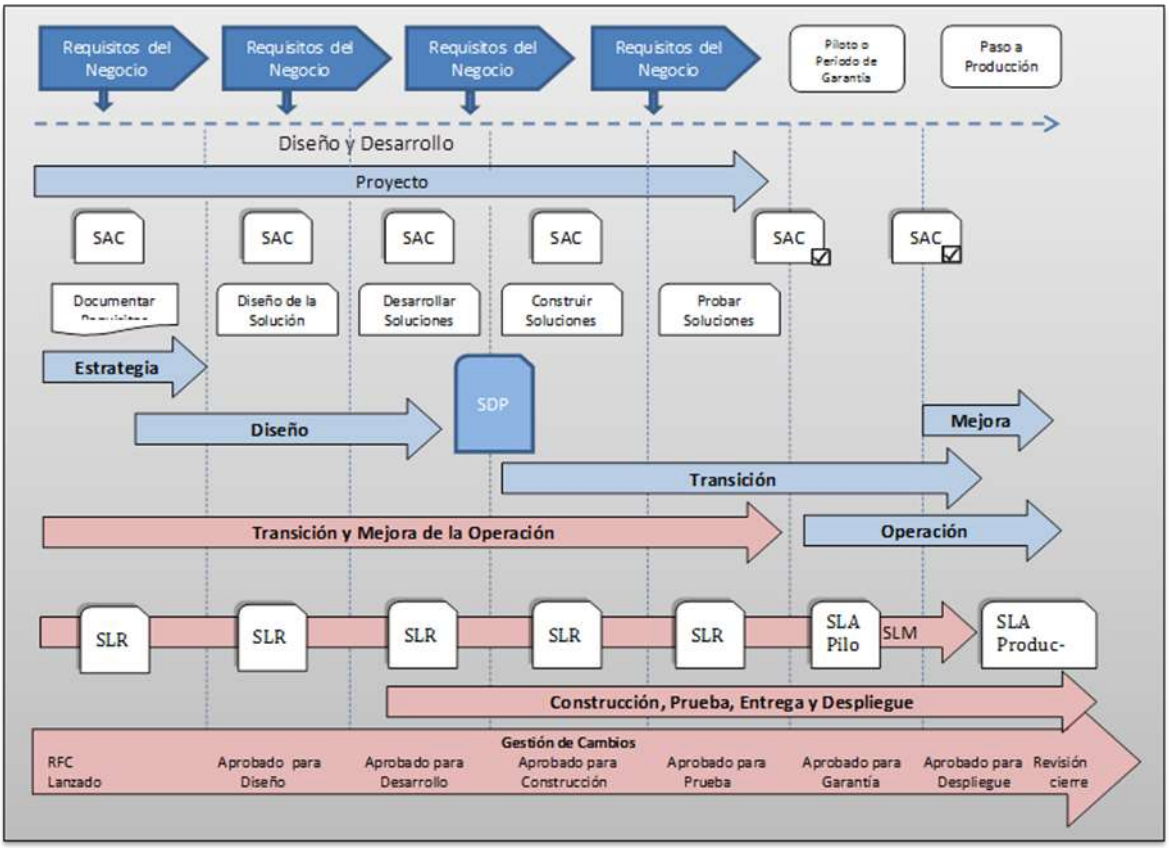

Ilustración 9 Posibles fases de un proyecto de implantación de la Gestión de Servicios TI de acuerdo con ITIL

Así, acorde con el ciclo de vida, se puede adoptar una de las metodologías existentes en el mercado, e implantar un sistema de Gestión de TI basado en las buenas prácticas de ITIL y en sus Procesos.

Recomendaciones generales

En una organización que aún no tenga suficiente grado de madurez como para implantar todas las fases del ciclo de vida del servicio, puede ser recomendable, no implantar desde el comienzo el proceso de Mejora Continua. Pero hay que tener cuidado de no perder de vista el ciclo de vida de manera completa. No valdrán excusas como la falta de recursos para ello sino, como se ha dicho, la madurez de la organización en la gestión del servicio.

También es importante la selección del/os servicios para el comienzo de la implantación de este estándar. Pensar en la selección como si fuera una certificación para la organización, ya que puede adoptarse posteriormente.

Éstos son los criterios de selección de servicios:

- Elegir un número de servicios significativo, que permita una adecuada implantación de los nuevos procesos para una posterior y progresiva extensión de los mismos.
- Servicios relevantes para la Compañía
- Servicios básicos con impacto en otros servicios del catálogo de TI.
- Los procesos transversales se aplican a la totalidad del servicio proporcionado por el proveedor del servicio (interno o externo), no sólo a los servicios dentro del alcance.
- La definición de los procesos debe ser sencilla, de modo que no constituya un esfuerzo adicional que haga fracasar la integración de estas prácticas en la operación diaria del servicio.
- En los procesos que requieren desarrollos o herramientas específicas, estas herramientas deben seleccionarse e implementarse con criterios de poder ampliar su alcance al resto de servicios. Sin embargo, hay que ser cuidadoso a la hora de hacer que la herramienta sirva al proceso y no adaptar el proceso a la herramienta.
- Para una primera implantación, se recomienda un alcance medio, pudiendo ser ampliado en sucesivas revisiones. Se sugiere empezar eligiendo servicios maduros y con un cierto valor para el negocio.

Relación con otros estándares/modelos

De manera particular, los principales modelos y estándares relacionados son los siguientes:

UNE-ISO 9001 Sistemas de Gestión de la Calidad

Las organizaciones que tengan una certificación del Sistema de Calidad obtendrán beneficios con la integración de los sistemas de gestión.

UNE-ISO/IEC 20000 Gestión de Servicios de TI

Como se dijo anteriormente, las organizaciones que quieran implantar esta norma, tendrán una verdadera ventaja si además han implantado las buenas prácticas recogidas en la librería ITIL.

UNE-ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. Las organizaciones certificadas en UNE-ISO/IEC 27001 satisfarán los requerimientos de seguridad recogidos en las buenas prácticas de ITIL.

UNE-ISO 22301 Sistema de Gestión de la Continuidad del Negocio (SGCN).

Las organizaciones certificadas en UNE-ISO/IEC 22301 satisfarán completamente los requerimientos de continuidad recogidos en las buenas prácticas de ITIL, así como gran parte de los requisitos de disponibilidad.

UNE-ISO 38500 Gobernanza corporativa de la Tecnología de la Información (TI).

CobiT Control Objectives for Information and Related Technology
Tanto UNE-ISO 38500 como CoBiT, ofrecen marcos de referencia superiores para el Gobierno de los Sistemas de Información. La búsqueda de la eficiencia en el servicio de

Según el cuadro de Gobierno de TI, las relaciones entre estándares, metodologías y buenas prácticas, se relacionan de la siguiente manera:

ISO/IEC 38500:2008

ISO/IEC 38500:2008 - Corporate governance of information technology

Entidad Emisora

ISO/IEC 38500:2008. *Corporate governance of information technology* es un estándar internacional, publicado de forma conjunta por los organismos de normalización ISO e IEC.

Su edición original está fechada el 1 de junio de 2008 y fue el primer estándar reconocido internacionalmente en el ámbito del Gobierno Corporativo de las Tecnologías de la Información.

Tiene su origen en un estándar australiano-neozelandés AS/NZS 8015-2005. Corporate governance of information and communication technology, de 31 de enero de 2005; hoy reeditada como AS/NZS ISO/IEC 38500:2010. Corporate governance of information technology (1 de marzo de 2010).

En España, el organismo normalizador, AENOR, publicó la versión local (en español) del estándar el día 10 de abril de 2013, bajo el nombre *UNE-ISO/IEC 38500:2013. Gobernanza corporativa de la Tecnología de la Información (TI)*.

Hoy el estándar se encuentra en avanzado proceso de revisión por parte de ISO siendo muy posible que su borrador *ISO/IEC DIS 38500. Information Technology – Governance of IT for the organization* vea la luz como del estándar definitiva dentro del presente año 2014.

- **Disponibilidad**

El documento, en inglés y con una extensión de quince páginas, puede adquirirse a través de ISO, tanto en su variante electrónica, como en papel, al precio de 88 CHF.

AENOR ofrece la versión en español (dieciocho páginas), también en ambos formatos, a 38,93 EUR.

Finalmente, en estos momentos, también es posible adquirir el borrador ISO/IEC DIS 38500, por 58 CHF.

La información ofrecida aquí sobre el precio y la disponibilidad de la estándare, se basa en los datos publicados por las entidades normalizadoras, a la fecha de elaboración de esta guía.

Clasificación (taxonomía)

El estándar ISO/IEC 38500 constituye la cabecera de una futura familia de estándares -parcialmente en preparación- que aplican al eficaz gobierno corporativo de las Tecnologías de la Información, asistiendo a quienes ocupan los niveles más altos de las organizaciones a comprender y cumplir sus obligaciones legales, regulatorias y éticas respecto del uso que, de las TI, se hace en el seno de aquellas.

Hasta la fecha, únicamente ha visto la luz, en forma de informe técnico, el recientemente publicado *ISO/IEC TR 38502:2014. Information technology – Governance of IT – Framework and model*. El propósito de este informe técnico es proporcionar información sobre un marco de referencia y un modelo que puedan ser usados para establecer las fronteras y las relaciones entre el gobierno corporativo -representado por el órgano de gobierno (típicamente, el consejo de administración)- y la gestión -en manos de los ejecutivos- en lo que se refiere al uso, actual y futuro, que se haga de las TI en la organización.

Aún en desarrollo, a la fecha de elaboración de esta guía, se encuentra el del estándar ISO/IEC DTS 38501. Information technology – Corporate Governance of IT Implementation Guide.

De otros desarrollos normativos que se anunciaban en 2008 como evolución natural del estándar (Gobierno de los Proyectos que impliquen Inversiones en TI y Gobierno de las TI usadas en las Operaciones en curso del Negocio) nada se ha sabido. Únicamente la original AS/NZS 8015 ha conocido el desarrollo y posterior publicación, ratificada el 18 de diciembre de 2013, de la que es hoy su del estándar hermana, *AS/NZS 8016:2013. Governance of IT enabled projects*.

- **Referencia normativa**

Como se ha señalado, el estándar ISO/IEC 38500 tiene su origen en AS/NZS 8015. Los trabajos para el desarrollo de este último habían comenzado en el año 2000, publicándose el estándar en enero de 2005.

Posteriormente, el organismo normalizador australiano elevó a ISO la petición de "internacionalizar" su AS/NZS 8015, lo que se aprobó, dando lugar a un proceso de tramitación rápida que culminaría, como se ha indicado, con la publicación, el 1 de junio de 2008, del estándar internacional ISO/IEC 38500:2008.

En 2013, el estándar internacional sería, finalmente, publicado en España como el estándar UNE-ISO/IEC 38500:2013.

- **Ámbito de aplicación**

La aplicación de unos principios generales para el buen gobierno corporativo de las TI como los recogidos en el estándar -responsabilidad, estrategia, inversión, rendimiento, conformidad y comportamiento humano- ayudará al órgano de gobierno de la organización -consejo de administración o equivalente- a comprender su papel en la dirección y control del uso que se haga de las Tecnologías de la Información en el contexto de dicha organización.

Este estándar es aplicable a todo tipo de organizaciones, incluidas las empresas -cotizadas o no-, las entidades de la Administración Pública y las organizaciones sin ánimo de lucro; independientemente de su tamaño, propósito, diseño, estructura de su propiedad y del uso, más o menos intensivo, que en ellas se haga de las TI.

Cabría señalar que el carácter general de los principios de gobierno corporativo propuestos por el estándar podrían hacerlos fácilmente trasladables a otros ámbitos de la empresa distintos de aquellos relativos al uso de las tecnologías de la información (por ejemplo, al de los recursos humanos, al de los recursos financieros, etc.).

- **Certificación**

El estándar ISO/IEC 38500 NO ES CERTIFICABLE, ni se diseñó con la idea de serlo.

No busca la puesta en marcha de un "sistema de gestión" al uso, como ocurre con otros estándares o familias ISO, sino que únicamente ofrece una serie de principios de gobierno corporativo por los que se han de regir las organizaciones -y de manera muy particular sus órganos de gobierno (consejo de administración)- en lo relativo al uso que en ellas se hace de las TI.

Objetivos del estándar

El objetivo del estándar ISO/IEC 38500 es promover un uso eficaz, eficiente y aceptable de las TI en todas las organizaciones.

A tal fin, el estándar presenta un marco de principios generales -responsabilidad, estrategia, inversión, rendimiento, conformidad y comportamiento humano- que han de ser usados por los miembros de los órganos de gobierno de las organizaciones (consejeros) cuando establezcan directrices sobre, cuando evalúen y cuando supervisen, el uso de las TI en sus respectivas organizaciones.

Agentes facilitadores para su adopción/implementación

Resulta incuestionable el hecho de que la mayoría de las organizaciones, hoy, está abrazando "lo digital". Utilizan las TI como una herramienta básica para su actividad, al tiempo que pocas son capaces de mantener un funcionamiento eficaz sin la contribución de dichas tecnologías.

Las TI son, asimismo, un factor relevante en los planes de negocio futuros de muchas organizaciones.

Hoy la inversión en TI puede representar una proporción significativa del consumo de recursos financieros y humanos de una organización. Sin embargo, a menudo el retorno de tales inversiones no queda plenamente materializado y los efectos adversos sobre la organización pueden ser, también, significativos.

Las principales razones de estos resultados negativos descansan en el excesivo énfasis que se pone en los aspectos técnicos, financieros y de calendario de las actividades de TI, frente al que se lleva el contexto general del negocio en el que las TI son aplicadas y utilizadas.

Estas circunstancias contradictorias deberían constituir, si aún no lo hacen, el más nítido impulsor de la adopción, adaptación y puesta en marcha de los dictados del estándar ISO/IEC 38500 en una organización.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

El cumplimiento, por parte de quienes pueblan los consejos de administración de las organizaciones, de los principios de responsabilidad, estrategia, inversión, rendimiento, conformidad y conducta recogidos en el estándar ISO/IEC 38500 favorecerá un eficaz, eficiente y aceptable empleo de las TI y, con ello, el equilibrio entre los riesgos y oportunidades derivados de tal uso.

Un adecuado gobierno corporativo de las TI ayuda a los consejeros a garantizar una contribución positiva, por parte de las TI, al rendimiento de la organización, a través de:

- una correcta puesta en marcha y explotación de los activos y soluciones puestos a disposición por TI;
- unas imputabilidades y responsabilidades claras, tanto en el uso, como en la provisión de TI, a la hora de lograr las metas de la organización;
- continuidad y sostenibilidad de la actividad de la organización;

- alineamiento de las prioridades de TI con las necesidades del resto del negocio;
- una asignación eficiente de los recursos disponibles;
- innovación en servicios, mercados y negocios;
- buenas prácticas en la relaciones con los diferentes grupos con intereses en la organización;
- reducción de costes para la organización; y,
- obtención real de los beneficios estimados/aprobados para cada inversion de base tecnológica.

Finalmente, un buen gobierno corporativo de las TI contribuirá, asimismo, al cumplimiento de las obligaciones -regulatorias, legales, contractuales- de los consejeros, en lo que se refiere al uso aceptable de las TI en sus respectivas organizaciones.

Por el contrario, una atención más laxa al uso que se hace de los sistemas de información de la organización, por parte de quienes están al frente de ella, puede exponerla a consecuencias de naturaleza diversa, entre las que cabría señalar las derivadas de una posible falta de alineamiento TI con el Resto del negocio, incumplimientos normativos, brechas de seguridad que comprometan activos de información clave, etc.

Reconocimiento/reputación

No existen datos sobre el grado de adopción del estándar ISO/IEC 38500, ni en España, ni a nivel internacional; aunque no sería osado suponer que dichas cifras fuesen moderadas. Asimismo, resultaría lícito pensar que su carácter de del estándar no certificable, podría restarle interés en un mercado en el que la certificación actúa de catalizador clave para la adhesión de las organizaciones a múltiples y variadas estándares.

Sin embargo, en aquellos contextos en los que su propósito ha quedado perfectamente entendido, se han hecho valer sus credenciales de haber sido la primera -y única hasta la fecha- del estándar internacional ocupada en la disciplina del Gobierno Corporativo de las TI; disciplina que, en sí misma, presenta aún elevadas posibilidades de desarrollo en nuestro entorno.

En ese sentido, cabe reseñar el mayor recorrido del que ha gozado el estándar en la órbita de los países anglosajones de geografía austral: Nueva Zelanda, Australia, Sudáfrica,…. En este último, el estándar ISO/IEC 38500 ha servido de inspiración a la tercera edición del código e informe de gobierno corporativo "King" por el que se

rigen las empresas cotizadas sudafricanas -primero, a su vez, en incorporar recomendaciones sobre el gobierno corporativo de las TI, como parte de las responsabilidades de los consejos de administración-. También en Sudáfrica, el Gobierno puso en marcha, en 2012, un ambicioso programa para el establecimiento de un sistema de gobernanza corporativa de las TI en la Administración Local, basado en el estándar ISO/IEC 38500 (entre otros marcos; entre ellos, el propio "King III").

En España, tras la publicación del texto original, por ISO, en 2008, se conoció alguna iniciativa piloto en el sector financiero, que permitió a sus protagonistas establecer un primer contacto con los principios de la norma.

Directrices sobre su uso/implementación

Es precisamente Sudáfrica quien, en estos momentos, está liderando los trabajos de desarrollo de la futura *ISO/IEC 38501. Information technology – Corporate Governance of IT Implementation Guide* -hoy, todavía borrador de del estándar técnica (DTS, *Draft Technical Standard*)-, dentro de ISO.

A la espera de lo que depare esa futura guía, se hace oportuno detallar que el estándar ISO/IEC 38500 promueve la adopción de un modelo de funcionamiento que recoge las actividades que habrá de realizar el órgano de gobierno de la organización en su faceta de guía (estableciendo directrices), de evaluador (de las propuestas de inversión que se planteen en la organización) y de supervisor (del cumplimiento de las citadas directrices y de los resultados de los planes ejecutados).

El modelo de gobierno corporativo de las TI planteado por el estándar responde al que se muestra a continuación:

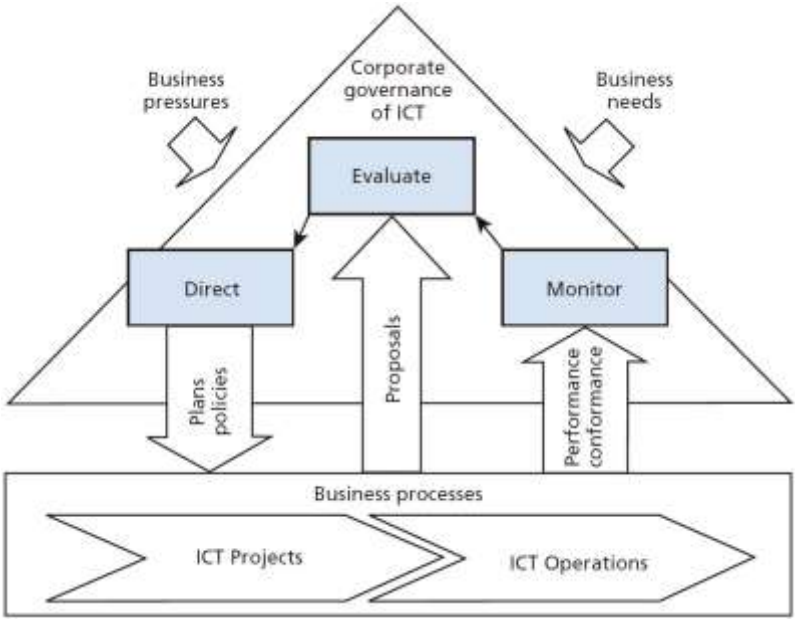

Figura 10 Modelo de gobierno corporativo de las TI planteado ISO/IEC 38500:2008

La figura, reproducida a partir de la propia del estándar ISO/IEC 38500, muestra dos ámbitos diferenciados: el del gobierno corporativo (de las TI), arriba; y el de la gestión del día a día de la organización, abajo.

En el primero aparecen coloreados los tres procesos clave que habrán de definir la actividad del órgano de gobierno, en relación al uso que se hace de las TI en la organización:

- DIRIGIR (*Direct*): establecer directrices estratégicas que guíen el futuro de la empresa en respuesta a las necesidades de la propiedad (los accionistas) y otros grupos de interés. Dichas directrices adoptarán la forma de políticas y planes;
- EVALUAR (*Evaluate*): valorar las propuestas de inversión que surgen en la empresa y aprobarlas, o no, en función, entre otros factores, de su mayor o menor proximidad a las directrices marcadas para la organización; y,
- SUPERVISAR (*Monitor*): verificar/controlar que los planes en ejecución están alcanzando los resultados esperados y aprobados (rendimiento) y que se cumplen, asimismo, el resto de requisitos (normativos, contractuales u otros) a los que la organización está sujeta (conformidad).

La puesta en marcha de un sistema de gobierno corporativo de las TI (o de mejora del existente -siempre existe uno aunque los afectados no lo sepan-) dentro de

una organización podría materializarse mediante un programa clásico de transformación en el que se recorrerían, al menos, las siguientes fases:

- FASE I: Diagnóstico de la situación de partida y definición del modelo vigente inicial.
- FASE II: Análisis de las expectativas a futuro y diseño del modelo deseado (la situación a la que se quiere llegar).
- FASE III: Identificación de acciones que permitan llegar del modelo inicial al modelo deseado y elaboración de un plan de acción que recoja las diferentes iniciativas identificadas (y priorizadas).
- FASE IV: Ejecución del plan de acción confeccionado en el paso anterior.

El capítulo que sigue, dedicado al modelo COBIT, presenta una aproximación más elaborada de este mismo enfoque del programa de transformación por etapas. Como se advertirá allí, la propuesta "implantación" de ISACA, creadora del modelo COBIT, no estará orientada a la puesta en marcha de los mecanismos subyacentes a COBIT, sino que ofrecerá un enfoque general, abierto (por ejemplo, a otras estándares de referencia como ISO/IEC 38500), para la puesta en marcha de un sistema de gobierno corporativo de las TI.

Relación con otros estándares/modelos

Los principales marcos de referencia, estándares o modelos de buenas prácticas, con los que el estándar ISO/IEC 38500 guarda relación, quedan enumerados a continuación:

- "*Report of the Committee on the Financial Aspects of Corporate Governance*" (Informe del Comité sobre Aspectos Financieros del Gobierno Corporativo).
- Conocido como "*Informe Cadbury*", en honor a Sir Adrian Cadbury, presidente del citado comité, fue publicado en Londres en 1992 y es una de las primeras, y más relevantes, fuentes bibliográficas sobre esta disciplina.
- "*OECD Principles of Corporate Governance*" (Principios de la OCDE sobre Gobierno Corporativo).
- Publicados originalmente, en 1999, por la Organización para la Cooperación y el Desarrollo Económico, fueron revisados en 2004.
- "*King Code of Governance for South Africa 2009*" (Código King de Gobierno [corporativo] para Sudáfrica 2009).

- Conocido como (código) "King III" constituye la tercera revisión de las recomendaciones en materia de gobierno corporativo emitida por la comisión presidida por Mervyn E. King, para las empresas sudafricanas. Fue publicado el 1 de septiembre de 2009. Las ediciones anteriores, King y King II, vieron la luz en 1994 y 2002, respectivamente.
- "*King Report on Corporate Governance in South Africa 2009*" (Informe King sobre el Gobierno Corporativo en Sudáfrica 2009).
- Complemento del "Código King III", el "Informe King III" ofrece una descripción detallada de los principios recogidos en el Código.
- ISO Guide 73 2002 - Risk management — Vocabulary — Guidelines for use in standards.
- ISO/IEC DTS 38501. Information technology – Corporate Governance of IT Implementation Guide.
- ISO/IEC TR 38502:2014. Information technology – Governance of IT – Framework and model.
- AS/NZS 8016:2013. Governance of IT enabled projects.
- COBIT 5. A Business Framework for the Governance and Management of Enterprise IT.

COBIT 5

COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT

Entidad Emisora

COBIT 5. A Business Framework for the Governance and Management of Enterprise IT (Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa) es un modelo de referencia de buenas prácticas, común- y globalmente aceptado, publicado por la organización internacional, de origen estadounidense, ISACA, anteriormente conocida como *Information Systems Audit and Control Association* (Asociación para el Control y la Auditoría de los Sistemas de Información).

Concebido inicialmente como un repositorio de controles que permitieran garantizar la fiabilidad de los Sistemas de Información, el modelo CobiT evolucionaría, con los años, hasta convertirse en el modelo de referencia (estándar "*de facto*") para el Gobierno y la Gestión de las TI que hoy es. La quinta edición fue oficialmente publicada por ISACA el día 10 de abril de 2012.

- **Disponibilidad**

Actualmente, COBIT -la denominada "familia" COBIT- es, en realidad, un amplio y creciente conjunto de documentos (así ha venido siendo desde sus primeras ediciones). Por ese motivo, se hace pertinente señalar que la descripción ofrecida en estas páginas hace referencia, salvo indicación en contra, a los tres documentos que constituyen el "paquete básico" del modelo que vio la luz el 10 de abril de 2012; esto es:

- *COBIT 5. A Business Framework for the Governance and Management of Enterprise IT*. (COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa);
- *COBIT 5. Enabling Processes* (COBIT 5. Procesos Habilitadores); y,
- *COBIT 5. Implementation* (COBIT 5. Implantación).

Los tres documentos -en sus ediciones, inglesa y española- están disponibles a través de ISACA (www.isaca.org/cobit) con el esquema de precios que se muestra a continuación:

COBIT 5	Miembros de ISACA (USD)	No-Miembros de ISACA (USD)
Framework (PDF)	Gratuito	Gratuito
Framework (Papel)	35	40
Processes (PDF)	Gratuito	50
Processes (Papel)	35	55
Implementation (PDF)	Gratuito	50
Implementation (Papel)	35	55

Tabla Esquema de precios y disponibilidad del modelo COBIT 5

La información ofrecida aquí sobre el precio y la disponibilidad de los componentes del modelo se basa en los datos publicados por ISACA a la fecha de elaboración de esta guía. Se recomienda consultar la web de la Asociación (www.isaca.org) a fin de obtener la información más actualizada. Las descargas gratuitas -incluso para no miembros- pueden requerir el registro previo en la web de ISACA.

Clasificación (taxonomía)

Como se ha señalado, COBIT 5 es, en realidad, un amplio y creciente conjunto de referencias bibliográficas, siendo el documento "*COBIT 5. A Business Framework for the Governance and Management of Enterprise IT*" (COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa) el que recoge la filosofía básica subyacente al modelo -la aplicación y uso de las TI en el seno de una organización, ha de servir a las necesidades del negocio-, actuando como cabecera del resto de la familia.

Hasta la fecha, han visto la luz las siguientes publicaciones de la familia COBIT 5, todas ellas disponibles, en inglés y español, en la web de ISACA:

- relativas al núcleo del modelo COBIT 5:

  - COBIT 5. *A Business Framework for the Governance and Management of Enterprise IT*. (COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa);
  - COBIT 5. *Principles: Where Did They Come From?* (Principios de COBIT 5]: ¿De dónde vienen?) [NOTA: publicación disponible sólo en inglés];
  - COBIT 5*. Enabling Processes* (COBIT 5. Procesos Habilitadores); y
  - COBIT 5*. Enabling Information* (COBIT 5. Información Habilitadora).
- relativas a la adopción y adaptación (ad@ptar™) del modelo COBIT 5:
  - COBIT 5*. Implementation* (COBIT 5. Implantación).
- **relativas a las diferentes aplicaciones que ofrece el modelo COBIT 5**, como guía de buenas prácticas para la seguridad de la información, para la auditoría de los sistemas de información o para el control y la gestión del riesgo ligado a los sistemas de información:
  - COBIT 5 *for Information Security* (COBIT 5 para la Seguridad de la Información);
  - COBIT 5 *for Assurance* (COBIT 5 para las actividades de Garantía/Auditoría); y,
  - COBIT 5 *for Risk* (COBIT 5 para el Riesgo).
- **relativas a la evaluación del modelo COBIT 5** ó, más concretamente, a la evaluación de aquellos procesos de COBIT 5 adoptados/adaptados en el seno de una organización:
  - *Process Assessment Model (PAM): Using COBIT 5* (Modelo de Evaluación de Procesos (PAM): Utilizando COBIT 5).
  - *Self-assessment Guide: Using COBIT 5* (Guía de Auto-evaluación: Utilizando COBIT 5).
  - *Assessor Guide: Using COBIT 5* (Guía del Evaluador: Utilizando COBIT 5).

Adicionalmente, sólo en ingles, ISACA ofrece una serie de guías de orientación práctica, mediante las cuales trata de mostrar y demostrar la aplicabilidad del modelo COBIT 5 en diferentes entornos organizativos y tecnológicos. Entre ellas:

- *Relating the COSO Internal Control—Integrated Framework and COBIT* (Relacionando el Marco Integrado de Control Interno de COSO con COBIT);
- *Vendor Management: Using COBIT 5* (Gestión de Proveedores: Utilizando COBIT 5);

- *Controls and Assurance in the Cloud: Using COBIT 5* (Controles y Garantía en la Nube: Utilizando COBIT 5);
- *Configuration Management Using COBIT 5* (Gestión de la Configuración Utilizando COBIT 5);
- *Securing Mobile Devices Using COBIT 5 for Information Security* (Protegiendo los Dispositivos Móviles Mediante COBIT 5 para la Seguridad de la Información); o,
- *Transforming Cybersecurity: Using COBIT 5* (Transformando la Ciberseguridad: Utilizando COBIT 5).

A las que habría que añadir algunas guías regionales, como los siguientes documentos elaborados por los capítulos de ISACA en la India:

- *RBI Guidelines Mapping With COBIT 5* (Mapeo de las Directrices RBI con COBIT 5); y,
- *Securing Sensitive Personal Data or Information Under India's IT Act Using COBIT 5* (Protegiendo los Datos de Carácter Personal o la Información Sensibles, Sujetos a la Ley de las TI de la India, Mediante COBIT 5).

Finalmente, merecen ser citados los programas de auditoría ligados a los procesos del modelo COBIT 5. Los publicados hasta ahora se corresponden con los dominios EDM (Evaluar, Orientar y Supervisar) del área de Gobierno Corporativo de las TI y APO (Alinear, Planificar y Organizar) del área de Gestión de las TI. La relación completa de todos ellos se ofrece a continuación:

- [Process] *EDM01. Ensure Governance Framework Setting and Maintenance Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] EDM01. Asegurar el Establecimiento y el Mantenimiento de un Marco de Gobierno [corporativo de las TI]);
- [Process] *EDM02. Ensure Benefits Delivery Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] EDM02. Asegurar la Entrega de Beneficios);
- [Process] *EDM03. Ensure Risk Optimisation Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] EDM03. Asegurar la Optimización del Riesgo);
- [Process] *EDM04 Ensure Resource Optimisation Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] EDM04. Asegurar la Optimización de los Recursos);

- [Process] *EDM05. Ensure Stakeholder Transparency Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] EDM05. Asegurar la Transparencia para el Accionista);
- [Process] *APO01 Manage the IT Management Framework Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO01. Administrar el Marco para la Gestión de las TI);
- [Process] *APO02 Manage Strategy Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO02. Gestionar la Estrategia);
- [Process] *APO03 Manage Enterprise Architecture Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO03. Gestionar la Arquitectura de Empresa);
- [Process] *APO04 Manage Innovation Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO04. Gestionar la Innovación);
- [Process] *APO05 Manage Portfolio Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO05. Gestionar la Cartera [de inversiones en actividades de negocio habilitadas por las TI]);
- [Process] *APO06 Manage Budget and Costs Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO06. Gestionar el Presupuesto y los Costes);
- [Process] *APO07 Manage Human Resources Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO07. Gestionar los RRHH);
- [Process] *APO08 Manage Relationships Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO08. Gestionar las Relaciones);
- [Process] *APO09 Manage Service Agreements Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO09. Gestionar los Acuerdos de Servicio);
- [Process] *APO10 Manage Suppliers Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO10. Gestionar a los Proveedores);
- [Process] *APO11 Manage Quality Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO11. Gestionar la Calidad);
- [Process] *APO12 Manage Risk Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO12. Gestionar el Riesgo);
- [Process] *APO13 Manage Security Audit/Assurance Program* (Programa de Auditoría/Garantía del [Proceso] APO13. Gestionar la Seguridad);

- **Referencia normativa**

El modelo COBIT no es, en ningún caso, un estándar, estrictamente hablando; si bien es cierto que desde su publicación inicial ha sido considerado el estándar "*de facto*" en el que se han apoyado los profesionales del Control Interno y los Auditores de Sistemas de Información para el desempeño de sus responsabilidades.

Ese estatus de estándar "*de facto*" se ve avalado, adicionalmente, por la consideración que el propio modelo hace de sí mismo, al definirse como "*generalmente aceptado*" (esto es, que goza de una aceptación general), lo que ha quedado patente, entre la comunidad auditora, desde su aparición. Hoy ISACA, con un modelo COBIT evolucionado pretende consolidarlo entre nuevas audiencias como los profesionales de la Seguridad de la Información y los dedicados a la gestión y/o al gobierno de las TI y de las inversiones de base tecnológica.

La referida "aceptación general" viene garantizada por el hecho de que COBIT está construido sobre otros marcos y estándares que, a su vez, gozan de esa aceptación general. Entre dichos estándares que cabe citar:

- *ISO/IEC 38000:2008. Corporate Governance of Information Technology* (ISO/IEC 38500:2008. Gobierno Corporativo de las Tecnologías de la Información);
- *ISO/IEC 31000:2009. Risk Management* (ISO/IEC 31000:2009. Gestión del Riesgo);
- *ISO/IEC 27000. Information Security Management* (ISO/IEC 27000. Gestión de la Seguridad de la Información); y,
- *ISO/IEC 15504-2:2003. Information technology. Process assessment. Part 2: Performing an assessment*" (ISO/IEC 15504-2:2003. Tecnologías de la Informacion. Evaluación de procesos. Parte 2: Llevando a cabo una evaluación)

En el apartado "*Relación con otros estándares/modelos*", más abajo, se hará, nuevamente, referencia a éstos, y otros, estándares o modelos.

- **Ámbito de aplicación**

COBIT 5 recoge, en su documento base, un conjunto de cinco principios clave, que no son sino principios arquitectónicos bajo cuya aplicación se sustenta el modelo:

- Principio 1: Dar respuesta a las necesidades de los distintos grupos de interés (de la organización);
- Principio 2: Cubrir la empresa de extremo a extremo (desde el Consejo de Administración, u órgano de gobierno equivalente, hasta las operaciones, haciendo del Gobierno corporativo de las TI una parte del Gobierno Corporativo de la entidad);

- Principio 3: Aplicar un marco de referencia único e integrado (que englobe a otros marcos/estándares/etc. existentes);
- Principio 4: Habilitar un enfoque holístico (que tenga en cuenta los diferentes componentes o mecanismos que interactúan a la hora de alcanzar los objetivos de la organización). ISACA da el nombre de "habilitadores" a dichos mecanismos e incluye en ellos a los siguientes:
    - principios, políticas y marcos;
    - procesos;
    - estructuras organizativas;
    - cultura, ética y conducta;
    - información;
    - servicios, infraestructura y aplicaciones; y,
    - personas, habilidades y competencias.
- Principio 5: Diferenciar el Gobierno [como responsabilidad del Consejo de Administración] de la Gestión [como responsabilidad del Equipo de Dirección/los Ejecutivos].

La aplicación de estos principios arquitectónicos contribuirá a mejorar la comprensión del modelo COBIT 5 -su orientación y alcance- y ayudará a los actores implicados, comenzando por quienes pueblan el órgano de gobierno de la organización a comprender su papel en la dirección y control del uso que se haga de las Tecnologías de la Información en el contexto de dicha organización.

A su vez, todo ello hace del modelo una herramienta aplicable a todo tipo de organizaciones, incluidas las empresas - cotizadas o no-, las entidades de la Administración Pública y las organizaciones sin ánimo de lucro; independientemente de su tamaño, propósito, diseño, estructura de su propiedad y del uso, más o menos intensivo, que en ellas se haga de las TI. Una herramienta que, en manos del Negocio -recuérdese su condición de "*Business Framework*" (marco de referencia de Negocio)- permitirá que éste [el Negocio] oriente y supervise la aplicación, uso y consecuencias de las TI en cualquier organización.

Finalmente, se hace oportuno señalar cómo la propia ISACA ha adoptado y adaptado el modelo COBIT 5 como base para la definición de su propia estrategia "*S22*"[2] (plan

[2] ISACA. "COBIT Case Study: Use of COBIT 5 for ISACA Strategy Implementation".

estratégico hasta el año 2022), llevando el enfoque ofrecido por el modelo más allá del dominio de las Tecnologías de la Información y haciéndolo válido para el conjunto de la organización.

- **Certificación**

El modelo COBIT 5 NO ES CERTIFICABLE -todavía, y con matices-, aunque sí es evaluable.

Los referidos matices llevan a aclarar dos aspectos:

- Certificación de personas.

  Desde el punto de vista de los profesionales, hay que indicar que el modelo CobiT, desde 2006, fecha del lanzamiento del programa "*Mastering CobiT*" (Dominando CobiT), sí permite la certificación de individuos.

  Propia de aquel programa fue la irrupción en el mercado del certificado profesional "*CobiT Foundation Certificate*" (Certificado en Fundamentos de CobiT).

  Asimismo, los antecedentes de dicho certificado se encuentran en la aparición, ya en 2004, de la acreditación "*Accredited CobiT Trainer*", ACT (Instructor Acreditado de CobiT), surgida en el seno de los eventos formativos "*CobiT User Conventions*" (Convenciones de Usuarios de CobiT) que dieron cabida a los primeros cursos para formadores.

  En la actualidad, desde 2012, ISACA tiene externalizada la administración de su programa formativo en torno al modelo COBIT 5 en la firma británica APMG.

  El nuevo esquema de certificados profesionales salido del citado acuerdo incluye:

  - Certificado de superación del "*COBIT 5 Foundation Examination*" (Examen de Fundamentos de COBIT 5), requisito para los dos siguientes.
  - Certificado de superación del "*COBIT 5 Implementation Examination*" (Examen de Implantación [del Gobierno Corporativo de las TI] basado en COBIT 5).
  - Certificado de superación del "*COBIT 5 Assessor Examination*" (Examen de Evaluador de COBIT 5).

  Adicionalmente, ISACA ofrece, a quien haya superado el examen de evaluador, la posibilidad de obtener, previa solicitud y acreditación de la pertinente

URL [a 2015.02.14]:: http://www.isaca.org/COBIT/Pages/COBIT-Case-Study-Use-of-COBIT-5-for-ISACA-Strategy-Implementation.aspx

experiencia profesional, la cualificación "*COBIT Certified Assessor*" (Evaluador Certificado de COBIT).

Este esquema de certificados profesionales va acompañado de las correspondientes acreditaciones dirigidas a los instructores. En ese sentido, se tienen, por un lado, la acreditación orientada a entidades formativas, "*Accredited Training Organization*", ATO (Organización Formativa Acreditada) y, por otro, las de los instructores individuales:

"*COBIT 5 Approved Trainer. Foundation*" (Instructor Aprobado de COBIT 5. Fundamentos).

"*COBIT 5 Approved Trainer. Implementation*" (Instructor Aprobado de COBIT 5. Implantación).

"*COBIT 5 Approved Trainer. Assessor*" (Instructor Aprobado de COBIT 5. Evaluador).

Recientemente, ISACA/APMG han ampliado su oferta con dos nuevas propuestas formativas que llevan asociados los oportunos certificados profesionales y acreditaciones para instructores. Se trata de:

"*Implementing NIST Cybersecurity Framework using COBIT 5*" (Puesta en Marcha del Marco de Ciberseguridad del NIST utilizando COBIT 5).

"*COBIT 5 Assessor for Security*" (Evaluador de COBIT 5 para la Seguridad).

- Certificación de organizaciones.

Aparte de la, ya citada, designación "*Accredited Training Organization*", ATO (Organización Formativa Acreditada), orientada a los centros educativos que ofrecen formación en torno al modelo COBIT 5, el panorama de la cualificación de organizaciones difiere del descrito hasta este punto, para el caso de las personas.

Tradicionalmente, COBIT, como modelo de buenas prácticas, no ha estado pensado -aparentemente- para ser certificable (entiéndase, para que las organizaciones que hubiesen adoptado/adaptado el modelo recibiesen una sanción positiva como resultado del juicio emitido por un evaluador independiente).

Esta circunstancia, sin embargo, comienza a cambiar en 2011, a raíz de la publicación del *Process Assessment Model*, PAM (Modelo de Evaluación de Procesos), que trae consigo una nueva y más rigurosa aproximación al análisis de los procesos COBIT adoptados/adaptados dentro de las organizaciones, viniendo a sustituir a los antiguos modelos de madurez de CobiT 4.1 y anteriores.

Disponible, inicialmente, para la versión 4.1 del modelo y, actualmente, publicado ya en versión de COBIT 5, PAM ofrece un esquema de evaluación de

las organizaciones basado en el estándar "*ISO/IEC 15504-2:2003. Information technology. Process assessment. Part 2: Performing an assessment*" (ISO/IEC 15504-2:2003. Tecnologías de la Informacion. Evaluación de procesos. Parte 2: Llevando a cabo una evaluación), que las haría susceptibles de resultar, finalmente, certificadas.

La figura a cargo de este tipo de evaluaciones sería, de forma natural, el "*COBIT Certified Assessor*" citado más arriba.

Hasta la fecha, se han realizado diversas evaluaciones de empresas y organizaciones en Oriente Medio, en EEUU, etc., que han sido hechas públicas; pero no se ha otorgado certificado alguno por parte de ISACA. Dichos ejercicios han quedado, únicamente, en la valoración (evaluación) emitida por el evaluador.

Objetivos del modelo

Los objetivos del modelo COBIT pasan por ofrecer a las organizaciones un marco de referencia integral que las ayude a alcanzar las metas que se hayan propuesto en materia de gobierno y gestión de las TI corporativas. Dicho de una manera más sencilla, que las ayude a crear el valor óptimo, a partir de la aplicación y uso que hagan de las TI, manteniendo el equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y de empleo de recursos.

Agentes facilitadores para su adopción/implementación

Hoy, la información es un recurso clave para cualquier organización y, desde el momento de su creación, hasta que es destruida, la tecnología juega un papel fundamental en ese ciclo de vida.

Ello lleva a que las mejoras en el establecimiento de una determinada orientación y unas directrices sobre el uso de las TI dentro de la empresa, así como la necesidad de supervisar dicho uso, deban ser actividades ampliamente reconocidas por quienes están al frente de las organizaciones como una parte esencial de sus responsabilidades en materia de gobierno corporativo; esto es, de su responsabilidad corporativa.

Como se ha dicho, COBIT 5 pasa por ser una herramienta que viene a ayudar a las organizaciones a alcanzar sus objetivos de gobierno corporativo. De ese modo,

entre los principales catalizadores para la adopción/adaptación del modelo COBIT 5 se incluyen:

- la necesidad de dar voz a más grupos con intereses en la organización, al objeto de determinar qué es lo que esperan de la información y de sus tecnologías afines (qué beneficios, a qué nivel aceptable de riesgo y a qué coste);
- la necesidad de conocer cuáles son sus prioridades para asegurar que el valor esperado del uso de las TI es, finalmente, obtenido;
- la necesidad de tratar eficazmente las expectativas divergentes -a menudo opuestas- de unos y otros grupos, en lo referente a las TI;
- la necesidad de ofrecer mayor transparencia en relación a cómo se articula la aplicación de las TI y sus resultados;
- la necesidad de ser conscientes de la creciente dependencia que el éxito de la organización tiene de cuanto hagan compañías y grupos externos (contratistas, proveedores, consultores, clientes, etc.) para aportar el valor esperado;
- la necesidad de tratar con la ingente cantidad de información que se genera con el tiempo, de forma que la misma conduzca a decisiones empresariales informadas, que resulten eficaces y eficientes;
- la necesidad de tratar con unas TI que, cada vez más, constituyen una parte integral de la organización, provocando, al mismo tiempo, una evolución en las responsabilidades de la función de TI y de quien está al frente de ella;
- la necesidad, derivado de lo anterior, de obtener un mejor control sobre soluciones de TI adquiridas de forma autónoma por el resto-del-negocio (por sus usuarios);
- la necesidad de ofrecer orientación adicional en el ámbito de la innovación y las tecnologías emergentes; y, en definitiva,
- la necesidad de alcanzar:
  - la esperada creación de valor a través del uso eficaz e innovador de las TI en la organización;
  - la satisfacción del resto-del-negocio (de los usuarios) con el nivel de compromiso y los servicios prestados desde las áreas de TI;
  - la conformidad con las leyes, reglamentos, acuerdos contractuales y las políticas internas más relevantes; y,
  - una mejora en la relación entre las necesidades del resto-del-negocio y las metas de TI.

- **Ventaja competitiva y riesgos relacionados con su no adopción/adaptación o uso**

De lo expuesto en el apartado anterior se deduce que la importancia de la información y la omnipresencia de la tecnología de la información (TI) están incrementándose en cada aspecto de los negocios y de la vida pública. Por ello, la necesidad de obtener un mayor rendimiento de las inversiones de base tecnológica y de lograr una mejor gestión del conjunto cada vez más amplio de riesgos relacionados con TI nunca ha sido mayor.

El aumento de la regulación también está impulsando el aumento de la concienciación entre los consejos de administración con respecto a la importancia de contar con un entorno de TI bien controlado y la necesidad de cumplir con las obligaciones legales, reglamentarias y contractuales pertinentes.

Un gobierno eficaz de las TI -habilitado, en este caso, por la adopción/adaptación del modelo COBIT 5- se traducirá en una mejora del rendimiento del negocio, así como en el cumplimiento de los requisitos citados.

Sin embargo, la puesta en marcha exitosa de un marco para el gobierno corporativo de las TI [basado en COBIT 5] sigue resultando una tarea difícil para muchas organizaciones. Como consecuencia, los intentos fallidos -y, más aún, los inexistentes- de abordar tal tarea pueden tener una incidencia directa en la capacidad de la organización para:

- disponer de información de alta calidad que soporte la toma de decisiones clave para el negocio;
- garantizar la contribución de las inversiones habilitadas por el uso de las TI a la generación de valor para el negocio;
- alcanzar la excelencia operativa a través de una aplicación fiable y eficiente de la tecnología;
- mantener, en un nivel aceptable, los riesgos vinculados al uso de las TI;
- optimizar el coste de los servicios y tecnologías provistos por las áreas de TI; o,
- como se ha señalado anteriormente, cumplir con el constantemente creciente número de leyes, regulaciones, acuerdos contractuales y políticas aplicables.

Reconocimiento/reputación

Para quienes pertenecen a la órbita de ISACA el reconocimiento y reputación del modelo COBIT está fuera de dudas. A las ya casi dos décadas de vida del modelo

sirviendo a auditores de sistemas de información y otros profesionales, habría que sumar el casi medio siglo que la Asociación lleva ofreciendo contenidos y servicios, relacionados con COBIT, a esos mismos colectivos profesionales.

No obstante, más allá de estas consideraciones "endogámicas", la reputación del modelo COBIT queda respaldada por el amplísimo reconocimiento que se desprende de un uso generalizado en todas las geografías del planeta, tanto en entidades privadas, cuanto en organismos de la Administración Pública.

Como prueba de ello, desde 1998, ISACA y su apéndice IT Governance Institute vienen recopilando en sus respectivas sedes *web* una relación de casos de éxito en la adopción del modelo COBIT 5 y sus antecesores y/o derivados, que hoy ronda el medio centenar de referencias. [Estas referencias pueden consultarse en la página de revelador título "*COBIT Recognition*" (Reconocimiento de COBIT) localizada en la siguiente URL: http://www.isaca.org/COBIT/Pages/Recognition.aspx].

Adicionalmente, la propia ISACA ha publicado una recopilación, bajo el título "*COBIT Global Regulatory and Legislative Recognition*" (Reconocimiento Regulatorio y Legislativo Global de COBIT), en la que se recogen nuevos ejemplos del reconocimiento del modelo COBIT como marco de referencia autorizado/recomendado por parte de diferentes instituciones públicas y organismos reguladores de países de los cinco continentes:

- África: Botswana, Islas Mauricio, Nigeria, Sudáfrica y Zambia.
- América: Argentina, Brasil, Canadá, Colombia, Costa Rica, EEUU, Guatemala, México, Paraguay, Uruguay y Venezuela.
- Asia: Emiratos Árabes Unidos, Filipinas, India, Israel, Japón y Turquía.
- Europa: Grecia, Lituania, Polonia, Rumanía e instituciones como la UE.
- Oceanía: Australia.

[El documento completo puede descargarse desde la dirección electrónica: http://www.isaca.org/COBIT/Documents/Recognition-table.pdf].

Ello, en un cierto momento, llevó a ISACA a tildar a COBIT de "*su secreto mejor guardado*"; sin embargo, hoy día, esa paradoja está superada, dada una peculiaridad del modelo consistente en su facilidad -promovida incesantemente por ISACA- para "mezclarse" con otros estándares y modelos. Esta cualidad viene justificada porque genéticamente es un modelo asentado sobre otra serie de conocidas referencias normativas y conjuntos de buenas prácticas, como se verá en "*Relación con otros estándares/modelos*", más adelante, lo que ha contribuido definitivamente a su gran aceptación general.

De igual modo, ha de señalarse que el uso de COBIT en muchos de los casos es parcial -lo que también aconsejan, tanto ISACA, como el sentido común-, desde el punto de vista de que son sólo partes del modelo las que se adoptan/adaptan, en combinación con otros estándares o marcos de referencia.

Finalmente, cabe indicar que, en el caso de España, COBIT goza, también, de un amplio reconocimiento -la base de cerca de dos millares de asociados con que cuenta ISACA en nuestro país son una envidiable correa de transmisión para divulgar las bondades del modelo-, siendo de uso habitual en los ámbitos de control de los Sistemas de Información, en sectores como el financiero, el de telecomunicaciones, las grandes empresas industriales, en las firmas de auditoría, en las empresas consultoras que ofrecen servicios relacionados con la Gestión de la Seguridad de la Informacion, etc.

Tal vez el reto, aún, sea su llegada de manera más nítida a los departamentos de Informática y a las áreas de gestión de inversiones tecnológicas, hacia donde ISACA lleva años orientando sus mensajes.

Naturalmente, sería muy recomendable que parte de sus dictados fuesen recogidos, también, por los consejos de administración.

Directrices sobre su uso/implementación

Como ya se ha ido adelantando en este texto, la principal pista sobre la puesta en marcha de un sistema de gobierno corporativo de las TI, basado en COBIT, (o de mejora del existente -siempre existe uno, aunque los afectados no lo sepan-) dentro de una organización es seguir el principio de ad@ptar™ el modelo; es decir, tomar de él aquello que realmente sea de aplicación en la organización protagonista de la iniciativa y moldearlo para que encaje en ella de la manera más adecuada. Naturalmente, ello supondrá descartar -al menos, de momento- otras partes del modelo (por ejemplo, ciertos procesos).

La propuesta que hace ISACA para la adopción/adaptación de COBIT viene recogida en la guía de implantación [¡¡Ojo, COBIT no se implanta, a pesar del nombre de la guía!!], y consiste en una aproximación circular, y por etapas, como muestra la imagen que acompaña este texto.

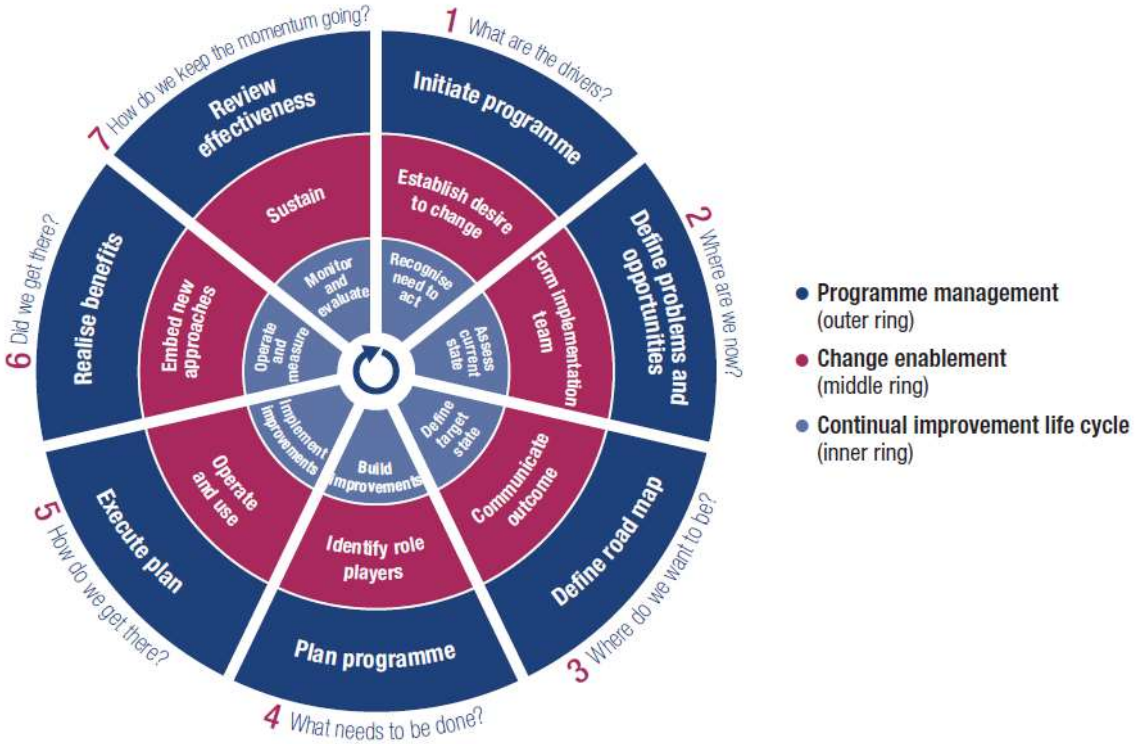

Ilustración 11 Ciclo de vida del programa de puesta en marcha de un marco de Gobierno Corporativo de las TI basado en COBIT 5

La figura, tomada del propio modelo COBIT, muestra, en círculos concéntricos, tres ámbitos diferenciados, pero interrelacionados dentro del Ciclo de Vida de la iniciativa de Gobierno Corporativo de las TI:

- en el anillo exterior se ubica la GESTIÓN general DEL PROGRAMA (*Programme management*). Se seguirá una aproximación de gestión de programa, diferenciando el programa general, de los proyectos o acciones individuales que lleve asociados;
- en el anillo central se colocan las actividades de PREPARACIÓN PARA EL CAMBIO cultural (*Change enablement*), que supondrá la nueva forma de gobernar y gestionar las TI, dentro de la organización; y,
- por último, en el anillo interior, se localizarán las actividades que darán forma al CICLO DE VIDA DE LA MEJORA CONTINUA (*Continual improvement life cycle*), que habrá de acompañar a la ejecución del programa general.

A su vez, ISACA propone un enfoque por fases para recorrer cada uno de los anillos:

- FASE I: ¿Cuáles son los catalizadores de la iniciativa?

Comienza con el reconocimiento y aceptación de la necesidad de una iniciativa de puesta en marcha, o mejora, del sistema de gobierno corporativo de las TI dentro de la organización.

En esta etapa se identifican los puntos débiles actuales y se desencadena y crea el ánimo de cambio en la alta dirección.

- FASE II: ¿De dónde se parte?

  Se concentra en la definición del alcance de la iniciativa, empleando para ello la correspondencia "*metas corporativas-metas de TI-procesos de TI*", propuesta en la cascada de objetivos de COBIT 5.

  De ese modo, los escenarios de riesgo presentes en la organización permitirán destacar los procesos clave en los que centrar los esfuerzos de la iniciativa.

  Los diagnósticos de alto nivel también pueden ser útiles para delimitar y entender áreas de alta prioridad en las que poner el foco.

  En esta segunda etapa se lleva a cabo una evaluación del estado actual y se identifican los problemas y deficiencias mediante la ejecución de un proceso de revisión de la capacidad.

  Se deberían estructurar iniciativas de gran escala como múltiples iteraciones del ciclo de vida – para cada iniciativa de implementación que exceda de seis meses, existe un riesgo de perder el impulso, el foco y la involucración de las partes interesadas.

- FASE III: ¿A dónde se desea llegar?

  Durante esta fase se establece un objetivo de mejora, seguido de un análisis más detallado aprovechando las directrices de COBIT 5 para identificar diferencias y posibles soluciones.

  Algunas soluciones pueden suponer beneficios inmediatos ("*quick wins*"), mientras que otras actividades pueden ser más desafiantes y de largo plazo.

  Las acciones prioritarias deberían ir dirigidas a aquellos objetivos que resulten más fáciles de conseguir y que pudieran proporcionar los mayores beneficios.

- FASE IV: ¿Qué necesita hacerse?

  En este momento se planificarán soluciones prácticas mediante la definición de proyectos individuales, apoyados por casos de negocio (estudios de viabilidad) justificados. Un caso de negocio bien desarrollado ayuda a asegurar que se identifican y supervisan los beneficios del proyecto.

  Además, se desarrollará un plan de cambios.

- FASE V: ¿Cómo se alcanza la meta?

Las soluciones propuestas son incorporadas a las prácticas del día a día, en esta fase.

Mediante las metas y métricas de COBIT 5, podrían definirse medidas y podría establecerse un mecanismo de supervisión, a fin de asegurar que se alcanza y mantiene el alineamiento con el resto-del-negocio y que se mide el rendimiento del programa general.

El éxito del programa requerirá del compromiso y la decidida apuesta de la alta dirección, así como de la asunción de la responsabilidad sobre la propiedad de la iniciativa por parte de los afectados, tanto de TI, como del resto-del-negocio.

- FASE VI: ¿Se ha logrado llegar?

Esta fase pone el acento en la operación sostenible del nuevo, o mejorado, sistema de Gobierno Corporativo de las TI y en verificar la consecución de los beneficios esperados.

- FASE VII: ¿Cómo se mantiene el impulso?

Finalmente, se revisa el éxito global de la iniciativa, se identifican requisitos adicionales para el gobierno o la gestión de las TI y se refuerza la necesidad de mejora continua.

En resumen, como se adelantaba en el capítulo anterior, dedicado al estándar ISO/IEC 38500, ISACA ofrece una aproximación que no está necesariamente orientada a la puesta en marcha de los mecanismos subyacentes a COBIT, sino que es susceptible, dado su enfoque general y abierto, de ser aplicada, también, a cualquier otro tipo de iniciativa de transformación dentro de una organización.

Relación con otros estándares/modelos

Se ha señalado en apartados anteriores la compatibilidad -siempre promovida por ISACA (y por el sentido común)- del modelo COBIT 5 con los principales marcos de referencia, estándares o modelos de buenas prácticas que ofrece el mercado. Dicha compatibilidad -mejor aún, complementariedad- queda reflejada en la siguiente figura, ya clásica en la bibliografía de ISACA:

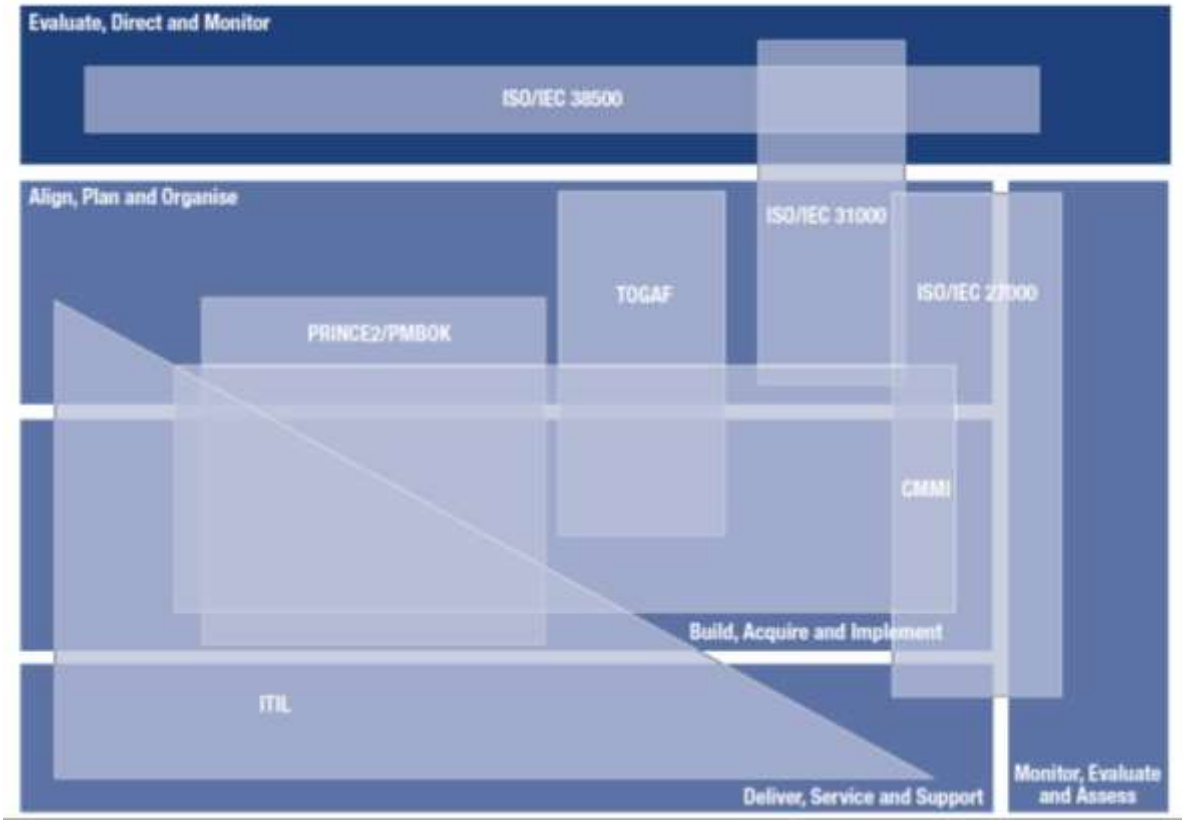

Ilustración 12 Compatibilidad del Modelo COBIT 5 con los principales marcos y estándares de referencia

Como puede apreciarse, los diferentes bloques que forman parte del puzle COBIT guardan una mayor o menor afinidad con unas u otras referencias del mercado. Así:

- "*ISO/IEC 38500:2008. Corporate Governance of Information Technology*" (ISO/IEC 38500:2008. Gobierno Corporativo de las Tecnologías de la Información) se asienta perfectamente en el área de Gobierno de COBIT 5; en particular, en el dominio EDM (Evaluar, Orientar y Supervisar);
- "*ISO/IEC 31000:2009. Risk Management*" (ISO/IEC 31000:2009. Gestión del Riesgo) encuentra su sitio de forma parcial, pero compartida, entre las áreas de Gobierno y Gestión del modelo COBIT 5; en particular, entre los dominios EDM (Evaluar, Orientar y Supervisar) y APO (Alinear, Planificar y Organizar);
- "*ISO/IEC 27000. Information Security Management*" (ISO/IEC 27000. Gestión de la Seguridad de la Información) se encuentra en la intersección de los cuatro dominios del área de Gestión de COBIT 5 (APO, BAI, DSS y MEA) dando idea de su transversalidad a cuanto tiene que ver con la gestión

de las TI, desde las actividades de planificación, pasando por las de desarrollo, hasta las de explotación y supervisión;

- "*TOGAF, The Open Group Architecture Framework*" (Marco de Arquitectura de The Open Group) se encuentra, también, a medio camino entre los dominios APO (Alinear, Planificar y Organizar) y BAI (Construir, Adquirir e Implantar) del área de Gestión de COBIT 5, situando una disciplina como la Arquitectura de Empresa entre las actividades de planificación estratégica de TI y la construcción de soluciones digitales de aplicación al negocio;
- "PRINCE2, Projects in Controlled Environments 2" (Proyectos en Entornos Controlados 2) y "*PMBoK, Project Management Body of Knowledge*" (Cuerpo de Conocimiento de la Dirección de Proyectos) orientados a la gestión de proyectos caen tangencialmente en el dominio APO (Alinear, Planificar y Organizar) por cuanto tienen que ver con la planificación de proyectos e iniciativas; y, más definidamente, en el dominio BAI (Construir, Adquirir e Implantar), por cuanto tienen que ver con la gestión de la ejecución de esos mismos proyectos e iniciativas (de construcción o despliegue de soluciones para el negocio, basadas en TI) a lo largo de su ciclo de vida;
- "*CMMI, Capabilitiy Maturity Model Integration*" (Integración del Modelo de Madurez de Capacidad) del SEI, Software Engineering Institute (Instituto de Ingeniería del Software) descansa, en su constelación de desarrollo, de manera natural con el dominio BAI (Construir, Adquirir e Implantar) de COBIT 5; y, en menor medida, con el APO (Alinear, Planificar y Organizar); y,
- finalmente, el modelo de buenas prácticas para la Gestión de los Servicios de TI, "*ITIL, IT Infrastructure Library*" (Biblioteca de Infraestructura de TI) se extiende a lo largo de tres de los dominios del área de Gestión de COBIT 5: APO, BAI y DSS (Entrega, Servicio y Soporte), si bien es con éste último con el que, tradicionalmente, ha mostrado mayor convergencia.

El programa de ISACA "*COBIT Mapping*", iniciado en 2004 y del que han salido más de dos decenas de referencias bibliográficas, ha demostrado durante más de una década la compatibilidad de COBIT (en sus diferentes ediciones) con un importante número de modelos disponibles a lo largo de estos años en el mercado.

ISO/IEC 27001:2013

ISO/IEC 27001:2013 Information technology – Security techniques -- Information security management systems – Requirements

Entidad Emisora

El estándar ISO/IEC 27001:2013 ha sido elaborado por el subcomité SC 27 Técnicas de seguridad TI que forma parte del comité técnico conjunto ISO/IEC JTC 1 Tecnologías de la información, establecido por ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional).

El comité técnico AEN/CTN 71 Tecnología de la Información es responsable de la elaboración de la versión española cuyo contenido es la traducción del estándar internacional ISO/IEC 27001:2013. Debe revisarse periódicamente la situación del estándar UNE-ISO/IEC 27001, dado que actualmente estamos en un periodo de transición por la cercanía en el tiempo de la nueva versión del estándar y a la espera de la traducción de la versión 2013.

- **Disponibilidad**

El estándar está a la venta en las distintas oficinas de AENOR así como a través de su página web (www.aenor.es). En la web de ISO (www.iso.org) puede también adquirirse la versión en inglés y en francés. Al dia de esta publicación el precio es de 118 CHF.

El estándar se puede consultar, en cualquiera de sus versiones, en las oficinas de AENOR.

Clasificación (taxonomía)

Normativa española e internacional.

- **Referencia normativa**

Los estándares internacionales sobre Sistemas de Gestión de Seguridad de Información conforman una familia de estándares con un mismo esquema de numeración que utiliza los números de la serie 27000 y siguientes. Esta familia

incluye estándares internacionales sobre requisitos, gestión del riesgo, métricas y mediciones, guías de implantación, etc.

El estándar que especifica los requisitos aplicables en el proceso de implantación y certificación es:

- ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements.

Otros estándares de la familia son:

- ISO/IEC 27002:2013 Information technology -- Security techniques -- Information security management systems - Code of practice for information security controls.
- ISO/IEC 27000:2014 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
- ISO/IEC 27003:2010 Information technology -- Security techniques -- Information security management system implementation guidance
- ISO/IEC 27004:2009 Information technology -- Security techniques -- Information security management – Measurement
- ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management
- ISO/IEC 27006:2011 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007:2011 Information technology -- Security techniques -- Guidelines for information security management systems auditing
- ISO/IEC TR 27008:2011 Information technology -- Security techniques -- Guidelines for auditors on information security controls
- ISO/IEC 27010:2012 Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011:2008 Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013:2012 Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

- ISO/IEC 27015:2012 Information technology -- Security techniques -- Information security management guidelines for financial services
- ISO/IEC TR 27019:2013 Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- ISO/IEC 27036-3:2013 Information technology -- Security techniques -- Information security management guidelines for financial services

Información adicional sobre el catálogo de estándares existentes, sus últimas versiones y las disponibles en español puede conseguirse en las webs de AENOR e ISO.

- **Ámbito de aplicación**

Aplicable a cualquier tipo de organizaciones (por ej. empresas, organismos y entes públicos, entidades sin ánimo de lucro), cualquiera que sea su tipo, tamaño, naturaleza o sector de actividad. Tiene su aplicación principal en la mejora de la gestión de la seguridad de la información.

Aplicable a toda la organización, o bien a áreas/procesos concretos del negocio.

- **Certificación**

El estándar ISO/IEC 27001:2013 es certificable por una entidad de certificación cuya competencia técnica haya sido reconocida formalmente por una entidad de acreditación. A estos efectos, la Entidad Nacional de Acreditación es ENAC.

Objetivos del estándar

- Especificar requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un SGSI, en el marco de los riesgos empresariales generales de la organización.
- Asegurar la selección de controles de seguridad, adecuados y proporcionados, que protejan los activos de información y den garantías a las partes interesadas.
- Servir para que cualquier parte interesada, ya sea interna o externa a la organización, pueda efectuar una evaluación de la conformidad, y certificar su cumplimiento.

Agentes facilitadores para su adopción/implementación

- Su adopción no está establecida formalmente como requisito legal, si bien facilita el cumplimiento de los requisitos legales de la LOPD y alinea a la organización con el ENS y la Ley 8/2011 de 28 de Abril relativa a las Infraestructuras Críticas.
- Demandado y/o valorado por los clientes a sus proveedores de servicios y/o productos que pueden realizar cualquier tipo de gestión con datos personales, información confidencial o relevante, para asegurar el cumplimiento legal y la adecuada gestión de sus datos. Independientemente del sector de actividad (tecnológico o de otro tipo).
- El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, por:
- Su correspondencia con los requisitos que establece;
- Por la demanda que establece de proveedores de confianza, y de productos certificados de seguridad, equipos, sistemas, aplicaciones o sus componentes.
- Establece un modelo de Gestión de Riesgos que puede servir de ayuda para cualquier proyecto posterior de implementación de estándares y buenas prácticas relativas a la continuidad tecnológica y de negocio.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

Aporta ventajas para la gestión de la información:

- Proporciona una metodología para la gestión de la seguridad de la información clara y estructurada.
- Proporciona sistemas y herramientas para la mejora continua en seguridad de la información, incluyendo el *feedback* que surge de la realización de auditorías externas por auditores formados, cualificados, y expertos.
- Reduce los riesgos de pérdida, robo, alteración de datos o de no disponibilidad de la información.
- Facilita establecer reglas y procedimientos de actuación para el personal de la organización, así como la información, motivación y formación del personal.
- Permite desarrollar mecanismos para asegurar la continuidad del negocio ante incidentes graves.
- Permite aumentar la seguridad de la información conforme a las necesidades y estrategia de la organización, y con base en procesos gestionados, más que en actividades de compra.
- Facilita la integración con otros sistemas de gestión (ISO 9001, ISO 14001, ISO 20000, etc.).

Proporciona ventajas comerciales, y para los responsables implicados:

- Apoya la actividad del Responsable TIC.
- Apoya el enfoque de negocio de la Dirección, facilitando su aplicación a gestión de la información, así como demuestra su compromiso con la seguridad de la información.
- Demuestra el cumplimiento de los requisitos (LOPD, LSSICE, ENS, Propiedad intelectual), la calidad en el manejo de la información.
- Genera confianza y credibilidad interna y externa (clientes, empleados, accionistas/propietarios, administraciones/jueces), y tanto a nivel nacional como internacional.
- Imagen de marca y diferenciación (certificación acreditada).
- Facilita la comercialización/venta, así como la exportación.
- Apoya la competitividad.

La no implantación del estándar puede conllevar la pérdida de oportunidades comerciales, así como carencias en la gestión de la seguridad de la información y en su gestión coherente con las prioridades y estrategias de negocio, además de un importante riesgo sobre la marca en caso de incidente de seguridad grave y notorio.

Reconocimiento/reputación

- La Organización Internacional de Normalización (ISO) elabora anualmente el informe *"ISO Survey"* en el que recoge los principales datos de la certificación ISO/IEC 27001 a nivel mundial. Los datos vienen recogiéndose desde el año 2006.
- Según dicho informe, (ISO Survey) el estándar tiene una amplia implantación a nivel mundial, manteniéndose un continuo crecimiento en los números de certificados en todos los continentes. España es uno de los países con mayor número certificados del Sistema de Gestión de Seguridad de la Información según El estándar ISO 27001, tanto a nivel europeo como mundial.
- Cada vez más las administraciones públicas y las grandes organizaciones demandan y valoran que sus clientes dispongan de esta certificación.
- El propio estándar, además de su implementación directa en las organizaciones, está sirviendo de base para la elaboración de estándares de seguridad de la información específica, como es el caso del ENS.

Directrices sobre su uso/implementación

Los contenidos del estándar se estructuran en los siguientes apartados:

48. **Introducción:** presenta el estándar, así como su enfoque a la preservación de la confidencialidad, integridad y disponibilidad de la información y la aplicación de un proceso de gestión de los riesgos, así como otros estándares de sistemas de gestión.
49. **Objeto y campo de aplicación:** detalla el objeto y campo de aplicación, estableciendo la obligatoria aplicación de los requisitos contenidos en los capítulos 4 al 10 del estándar para las organizaciones que declaren el cumplimiento de este estándar.
50. **Estándares para consulta:** referencia el estándar ISO 27000 como indispensable para la aplicación de este estándar.
51. **Términos y definiciones:** Se remite al estándar ISO/IEC 27000.
52. **Contexto de la organización:** recoge aspecto internos y externos que la organización debe tener en cuenta en la definición e implantación del sistema de gestión como, por ejemplo, necesidades y expectativas de las partes interesadas, requerimientos legales, etc.
53. **Liderazgo:** establece el liderazgo y compromiso de la alta dirección como vía para asegurar la eficacia del sistema de gestión de seguridad de la información, la determinación de la política, los roles, responsabilidades y la autoridad del personal.
54. **Planificación:** recoge requisitos a tener en cuenta en la planificación y establecimiento del sistema de gestión, particularmente para los procesos de evaluación y tratamiento de los riesgos de seguridad de información, y los objetivos de seguridad de información.
55. **Soporte:** concreta la necesidad de determinar y proveer los recursos necesarios, incluyendo los relativos a la competencia y concienciación del personal, los documentos, y las necesidades de comunicación tanto internas como externas.
56. **Operaciones:** recoge los requisitos para la planificación, implementación y control de todos los procesos necesarios para satisfacer los requisitos de seguridad de información, e implementar las acciones derivadas de la evaluación y tratamiento de los riesgos.
57. **Evaluación de resultados:** establece necesidades de monitorización, medida, análisis y evaluación de los resultados obtenidos para determinar la eficacia del sistema de gestión y, con ello, la necesidad de tomar acciones.
58. **Mejora:** recoge obligaciones respecto al tratamiento de no conformidades y el establecimiento de acciones correctivas, así como para la mejora continua.

Anexo A (Normativo) Objetivos de control y controles: enumera una lista completa de los objetivos de control y controles que se han considerado comúnmente relevantes en las organizaciones. Proporciona un punto de partida

para la selección de controles, garantizando que no se pasan por alto controles relevantes. Estos controles se deben considerar durante el proceso de creación del SGSI, en la medida que sirvan para satisfacer los requisitos identificados en la evaluación de riesgos y en el proceso de tratamiento de riesgos.

Bibliografía: Estándares y otras publicaciones de referencia.

La creación y mantenimiento del SGSI se establece aplicando el modelo PDCA, de conformidad con las siguientes pautas:

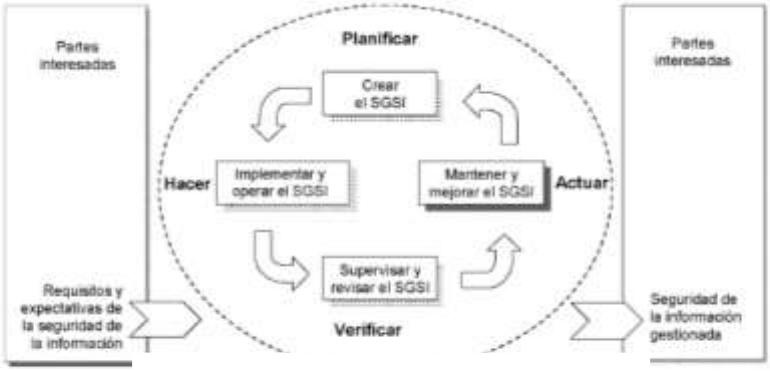

Figura 1 – Modelo PDCA aplicado a los procesos del SGSI

Planificar (creación del SGSI)	Definir la política, objetivos, procesos y procedimientos del SGSI relevantes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de obtener resultados acordes con las políticas y objetivos generales de la organización.
Hacer (implementación y operación del SGSI)	Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Verificar (supervisión y revisión del SGSI)	Evaluar y, en su caso, medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, e informar de los resultados a la Dirección para su revisión.
Actuar (mantenimiento y mejora del SGSI)	Adoptar medidas correctivas y preventivas, en función de los resultados de la auditoría interna del SGSI y de la revisión por parte de la dirección, o de otras informaciones relevantes, para lograr la mejora continua del SGSI.

Ilustración 13 Modelo PDCA aplicado a los procesos del SGSI

Aspectos clave para la implantación exitosa:

- Compromiso de la Dirección para con el desarrollo y mantenimiento del SGSI, y en particular en la decisión sobre los riesgos y el plan de tratamiento, con la definición clara de responsabilidades y autoridad, y el apoyo a los responsables asignados.
- Definición de un alcance manejable (claramente definido, acotado y adecuado a los plazos y recursos disponibles, y gradualmente ampliable según necesidades).

- Duración corta del proyecto, que no se debe prolongar en el tiempo.
- Organización interna y definición clara de la responsabilidad y autoridad (desde el inicio del proyecto).
- Concienciación, formación e información del personal.
- Cualificación del personal responsable del proceso de implantación del SGSI, que no debe basarse exclusivamente en criterios de competencia técnica en seguridad de información. Puede apoyarse en el asesoramiento de consultores externos especializados.
- Evaluación de riesgos adecuada.
- Integración con otros sistemas de gestión, y alineamiento con la estrategia de la Dirección.
- Definición e implantación de las políticas, procedimientos y normativas.
- Establecimiento de un sistema de gestión de incidencias, que reciba comunicaciones directas de los usuarios, las procese y analice para la toma de acciones.
- Seguimiento del SGSI, y actividades para la mejora continuada.
- La certificación sin ser el objetivo, es una herramienta valiosa para asegurar el cumplimiento de los requisitos aplicables. La certificación por tercera parte acreditada es la mejor referencia, dado que asegura los más altos estándares de calidad, facilitando la mejora continua, así como un mayor reconocimiento nacional e internacional.

De lo anterior se deriva que existen riesgos para el éxito de la creación y mantenimiento de un SGSI:

- Alcance poco claro o excesivamente amplio.
- Implantación excesivamente prolongada en el tiempo.
- Resistencia al cambio.
- Delegar todas las responsabilidades en los departamentos técnicos.
- Exceso de medidas técnicas en detrimento de la formación, concienciación y medidas de tipo organizativo.
- No asumir que la seguridad de la información es inherente a los procesos de negocio.
- Planes de formación, concienciación e información insuficientes o inadecuados.

Y como consecuencia, desmotivación, pérdida de enfoque o alejamiento de los objetivos iniciales, perdida de liderazgo, incremento de costes, discrepancias en la toma de acciones, etc.)

Relación con otros estándares

El estándar ISO/IEC 27001 mantiene compatibilidad con otras estándares ISO de sistemas de gestión. Con este enfoque se ha desarrollado la nueva versión, de manera que recoge y se organiza conforme a la estructura, textos y términos definidos en el Anexo SL de las directivas ISO/IEC para la consolidación de los estándares ISO de sistemas de gestión. Por ello, facilita que las organizaciones operen un único sistema de gestión que satisfaga los requisitos de diversos estándares ISO de sistemas de gestión.

Estándares certificables con las que se relaciona este estándar y que pueden implantarse de forma integrada son:

- Estándar de Sistemas de Gestión de Calidad UNE-EN ISO 9001
- ISO 20000 (Procesos comunes; ISO/IEC ha desarrollado la guía de implantación integrada de ISO/IEC 27001 e ISO/IEC 20000).

Mantiene una estrecha relación con diversa normativa legal, facilitando su gestión y cumplimiento.

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- La UNE 27001 tiene una gran correspondencia de requisitos aplicables, pudiéndose considerar que existe una práctica equivalencia.
- La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD). Real Decreto 1720/2013, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Dominio de Negocio

UNE-ISO 22301:2013

UNE-ISO 22301:2013 – Protección y seguridad de los ciudadanos. Sistema de Gestión de la continuidad del negocio (SGCN). Especificaciones

Entidad Emisora

UNE-ISO 22301 es publicado por AENOR y es la traducción exacta del estándar internacional ISO 22301, el cual es un estándar ISO basado en el británico BS 25999-2.

- **Disponibilidad**

UNE/ISO 22301 puede comprarse en la página web de AENOR, www.aenor.es, al precio de 46,92 € (especificaciones) y 62,38 € (directrices). El documento BS 259999-2 puede comprarse en la tienda online de BSI, shop.bsigroup.com, al precio de 100 libras.

En la web www.iso27001standard.com también se puede encontrar documentación y herramientas de ayuda para el estándar.

Clasificación (taxonomía)

Se trata de un estándar nacional e internacional y certificable enfocado en la Continuidad de los Negocios de las empresas en general.

Existe una adaptación del estándar para su aplicación en PYMES.

- **Referencia normativa**
  - ISO 22313:2012 Societal security -- Business continuity management systems – Guidance
  - ISO 22301:2012 Societal security -- Business continuity management systems --- Requirements
  - UNE-ISO 22301:2013 Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio (SGCN). Especificaciones.

- UNE-ISO 22313:2013 Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio (SGCN). Directrices.

UNE-ISO 22301 ha reemplazado a BSI 25999-2. Estos dos son bastante similares, pero ISO 22301 puede ser considerado como una actualización de BS 25999-2.

- **Ámbito de aplicación**

Este estándar es aplicable a todo tipo de organizaciones, independientemente de su tamaño (existe una adaptación de la norma para PYMES), y se aplica a la Continuidad de los negocios.

- **Certificación**

El estándar UNE-ISO 22301 es certificable por cualquier organismo acreditado.

Objetivos del estándar

Este estándar especifica los requisitos para un sistema de gestión encargado de proteger a la empresa de incidentes que provoquen una interrupción en la actividad, reducir la probabilidad de que se produzcan y garantizar la recuperación de la empresa.

Agentes facilitadores para su adopción/implementación

Si se implementa correctamente, la gestión de la continuidad del negocio disminuirá la posibilidad de ocurrencia de un incidente disruptivo y, en caso de producirse, la organización estará preparada para responder en forma adecuada y, de esa forma, reducir drásticamente el daño potencial de ese incidente.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

El estándar UNE-ISO 22301 permite:

- Identificar y gestionar las amenazas actuales y futuras para su empresa
- Utilizar un enfoque proactivo para minimizar el impacto de los incidentes
- Mantener sus funciones críticas listas y en funcionamiento durante momentos de crisis
- Minimizar el tiempo de interrupción tras cualquier incidencia y mejorar el tiempo de recuperación

- Demostrar su resistencia a clientes, proveedores y para ofertas de licitación

Si no dispone de un Plan de Continuidad de Negocio la empresa se está arriesgando, entre otras, a:

- No valorar el impacto que determinados riesgos que no hemos podido anular o mitigar pueden producir en la cuenta de resultados, incluso poniendo en riesgo la supervivencia de la misma
- No estar preparado para una acción eficiente en caso de interrupción parcial o total de las actividades, lo que implica pérdida de ingresos y/o incremento en costes directos, pérdidas por deterioro de la reputación, desmotivación de los trabajadores de la compañía, etc.
- Incumplimiento legal con posibles costes asociados y deterioro de la imagen de la compañía antes todas las partes interesadas (accionistas, empleados, clientes, etc.)

Reconocimiento/reputación

Este estándar está implantado eficazmente sobre todo en Reino Unido, principalmente en organizaciones del sector Bancario y en las que ya poseen certificado su sistema de gestión de la información, debido a las características de su integración.

http://www.bsigroup.com/en-GB/iso-22301-business-continuity/ISO-22301-for-SMEs/

Directrices sobre su uso/implementación

Dado que es un estándar de nueva generación su estructura es perfectamente integrable con el resto de sistemas de gestión, y por tanto las áreas de implementación son coincidentes (Contexto de la organización, Liderazgo, Planificación, Soporte, Operación, Evaluación y Mejora).

La clave está en realizar un exhaustivo análisis de impacto en el negocio que identifique las actividades, funciones y recursos que soportan la provisión de productos y servicios de la organización.

Para ello es necesario contar con el compromiso, patrocinio y apoyo de la alta dirección.

Según los resultados del análisis de impacto, en los casos en los que los riesgos no puedan eliminarse o mitigarse, habrá que establecer estrategias y prever alternativas para la disposición de los recursos o funciones críticos para el negocio en caso de incidente.

Para ello es necesaria la involucración de toda la compañía y el establecimiento de los procedimientos de actuación y los recursos alternativos necesarios.

El plan por último, se debe probar regularmente para comprobar su idoneidad, entrenar y adiestrar a las personas implicadas, y detectar los puntos de mejora.

A partir de los resultados de las pruebas de las auditorías regulares, el plan permanecerá en permanente evolución en un ciclo de mejora continua.

Relación con otros estándares/modelos

Otros estándares de ayuda en la implementación de la continuidad del negocio son:

- ISO/IEC 27031:2011 – Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
- PAS 200 – *Crisis Management – Guidance and Good Practice*
- PD 25666:2010 – Guidance on Exercising and Testing
- PD 25111 – The Human Aspects of Business Continuity
- ISO/IEC 24762:2008 ––Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services
- ISO/PAS 22399:2011 – Societal security - Guideline for incident preparedness and operational continuity management
- ISO/IEC 27001:2013 – Information technology -- Security techniques -- Information security management systems – Requirements

UNE-ISO 30301-1:2011

UNE-ISO 30301-1:2011. Información y Documentación. Sistema de Gestión para los documentos. Parte 1: Requisitos del Sistema de Gestión para los documentos (SGD)

Entidad Emisora

UNE-ISO 30301 es una norma internacional, publicada por primera vez en diciembre de 2011 a la vez la versión ISO/IEC. Es el estándar reconocido internacionalmente en gestión documental. La serie 30300 proviene de la adopción de la norma ISO 15489 desarrollada su primera versión en 2001, pero esta vez se quiso elevar la gestión documental al nivel de los *Management Systems Standards* (MSS) o Estándares de Sistemas de Gestión certificados.

- **Disponibilidad**

El documento puede comprarse en la web de ISO www.iso.org al precio de 108 CHF (a fecha de publicación de la ficha), y en AENOR www.aenor.es al precio de 45,82 € (fecha de publicación de la ficha).

Clasificación (taxonomía)

El estándar UNE-ISO 30301, forma parte de una familia de estándares internacional que especifica los requisitos para implantar un SGD cuando una organización quiere demostrar su habilidad para crear y controlar los documentos de sus actividades durante el tiempo que los necesita. En 2011, el estándar internacional es publicado como el estándar UNE, siendo entonces UNE-ISO 30301.

- **Referencia normativa**

El estándar UNE-ISO 30301 proviene del ISO/TR 15489-2:2006 Información y documentación. Gestión de documentos. Parte 2: Directrices, la parte 1 son Generalidades.

El estándar ISO 30301 fue preparado por el Comité Técnico ISO/TC 46 Información y documentación, Subcomité SC 11, Gestión de documentos.

El estándar ISO 30300 pertenece a una serie de estándares bajo el título general de Información y documentación. Sistema de gestión para los documentos:

- ISO 30300 Información y documentación. Sistema de gestión para los documentos. Fundamentos y vocabulario. Especifica la terminología para toda la serie de estándares, los objetivos y los beneficios de un SGD.
- ISO 30301 Información y documentación. Sistema de gestión para los documentos. Requisitos. Especifica los requisitos para implantar un SGD cuando una organización quiere demostrar su habilidad para crear y controlar los documentos de sus actividades durante el tiempo que los necesita.

- **Ámbito de aplicación**

Este estándar es aplicable a todo tipo de organizaciones, independientemente de su tamaño, y tiene su aplicación principal bajo los siguientes objetivos:

Gestionar información es un aspecto importante para las organizaciones del siglo XXI. Las organizaciones a través de sus actividades de negocio, procesos y sistemas, que crean, reciben y mantienen información como evidencia de su ejercicio. La información específica es conocida como registros, que actúan como evidencia de las actividades frente a los accionistas y litigios, y como base para crear conocimiento e informar en la toma de decisiones.

La creación de información es integral a cualquier actividad de una organización, a sus procesos y sus sistemas. La imparable transición a un entorno enteramente digital, es tanto un reto, como una oportunidad para gestionar eficientemente la información electrónica, creando valor y obteniendo numerosas ventajas competitivas.

La sociedad actual que demanda y precisa herramientas y metodologías para establecer un marco, ha creído necesario contar con esta del estándar para regular la creación y control de su información con un alcance sistemático y verificable.

- **Certificación**

UNE-ISO 30301 es certificable por cualquier organismo acreditado por ENAC. Algunos de los organismos certificadores en España: AENOR e IGC.

Objetivos del estándar

El estándar UNE-ISO/IEC 30301, es un estándar internacional que especifica los requisitos para implementar una política y objetivos de información a través de la implementación de los procesos documentales y sistemas, y la asignación de los recursos apropiados, estableciendo y evaluando el marco de mejora continua.

Existe en ISO un proceso de armonización para que todas las normas de sistemas de gestión compartan terminología, requisitos y estructura comunes y puedan ser perfectamente integrables compartiendo elementos metodológicos afines.

Agentes facilitadores para su adopción/implementación

Dentro de los agentes facilitadores se pueden alcanzar mejoras significativas en las siguientes áreas:

- Para asegurar que posee una información autorizada y fiable, además de demostrar evidencia de sus decisiones de negocio y acciones, que son creadas, gestionadas y accesibles a aquellos que lo necesitan, por el tiempo que son requeridas.
- Para demostrar compromiso, responsabilidad e integridad con la Dirección del organismo.
- Para eliminar redundancias y establecer consistencia.
- Para informar en la toma de decisiones.
- Para promocionar la eficiencia y eficacia de sus procesos, optimizando la información y los documentos para ser creados y utilizados.
- Para hacer a las organizaciones más rentables y eficientes.

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

La implementación de la serie de normas ISO 30300 ayudará a las organizaciones a cumplir con los objetivos de otras normas de sistemas de gestión como la calidad, la gestión de riesgos, el cumplimiento y la seguridad; ayudando por lo tanto al cumplimiento de los objetivos de la organización. Ello se consigue:

- Accesibilidad: Asegurando que se crea, gestiona y se hace accesible durante todo el tiempo que se necesita información fidedigna y fiable sobre, y evidencia de, las actividades realizadas dentro de un sistema de gestión.
- Mejora Continua: Contribuyendo a la mejora continua del desempeño de la organización mediante un sistema de gestión integrado".
- Fiabilidad: Estableciendo un enfoque sistemático y verificable sobre los procesos de control de la documentación de otros sistemas de gestión.

El principal riesgo derivado de su no implantación, radica en la ausencia de un sistema de gestión que asegure que el servicio de TI proporcionado a la organización esté controlado adecuadamente y dirigido a satisfacer las necesidades de su cliente (interno en caso de departamento de TI, externo para un proveedor de servicios de TI).

Especialmente para los departamentos de servicio interno, su ausencia puede llevar consigo también que el servicio de TI se vea como una carga costosa y no como una ayuda imprescindible para lograr los objetivos del negocio.

Reconocimiento/reputación

Existen más de 130 compañías en España certificadas en este estándar internacional, tanto en su versión 2005 y 2011.

Dentro del abanico de empresas certificadas, están tanto compañías de servicios de TI, como departamentos TI internos de compañías de otros ámbitos.

Directrices sobre su uso/implementación

Los beneficios de la normalización en la gestión de documentos, pasa por la adopción de prácticas sistemáticas:

- Capturando y controlando los documentos (ISO 15489)
  - Fiables (en cuanto al contenido)
  - Auténticos (sobre su autoría y datación)
  - Íntegros (inalterables y completos)
  - Conformes (con los objetivos y política del SGD)
- Controlando la información sobre las actividades de la organización
- Facilitando la eficiencia y eficacia de la gestión de documentos
- Eliminando la duplicidad
- Facilitando el acceso a la información
- Ofreciendo soporte a la toma de decisiones de la Alta Dirección
- Rindiendo cuentas
- Cumpliendo con la legislación
- Responsabilidad social

- Gestionando los riesgos (ISO18128/ISO 31000)
- Facilitando la continuidad del negocio (ISO 22301)

El ciclo Deming unificado para todos los sistemas de gestión (éste es el de un SGD):

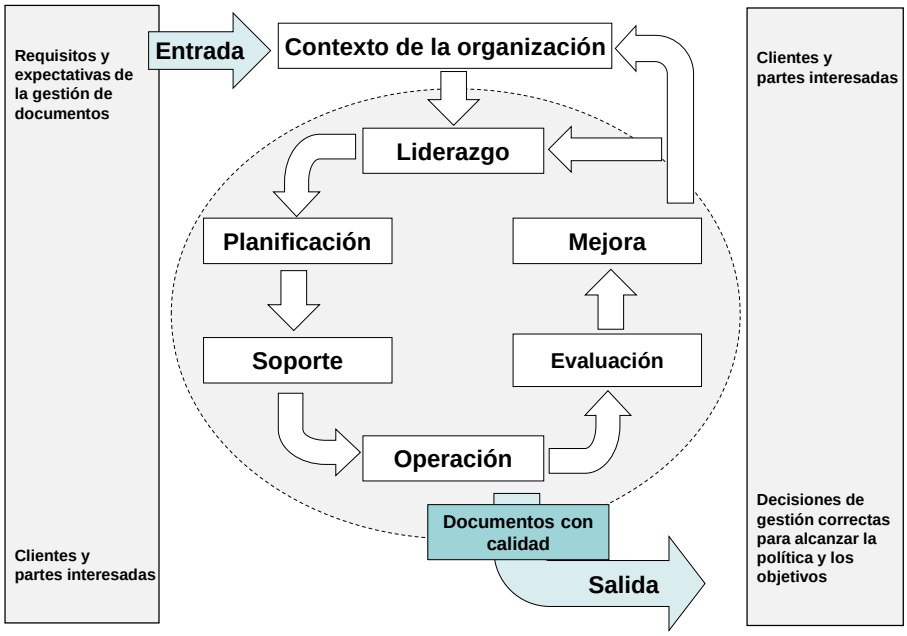

Ilustración 14 ciclo Deming unificado

La implantación del SGD consta de los siguientes requisitos:

- Identificación de factores internos y externos
- Identificación de requisitos de negocio, legales y de otra índole
- Determinación del alcance
- Compromiso demostrable de la Alta Dirección
  - Dirección estratégica
  - Recursos
  - Dirigiendo la mejora continua
- Política de la gestión documental
  - Marco documentado
  - Comunicada y aceptada

- Roles organizativos y responsabilidades asignados
  - Responsabilidades de la Dirección
  - Responsabilidades operativas
- Establecimiento de los objetivos
  - Planes para alcanzar los objetivos:
  - Qué (acciones)
  - Quién (responsables)
  - Con qué (recursos)
  - Cuando (tiempo)
  - Cómo se evaluará (indicadores)

Tratamiento de oportunidades y riesgos

- Recursos
  - Materiales
  - Humanos
- Capacitación de las personas

Las áreas de requisitos se dividen en las siguientes fases:

Fase 1. **Contexto de la Organización** (punto 4 del estándar)

4.1: La organización establecerá los factores externos e internos pertinentes

4.2: Se tendrán en cuenta los requisitos de negocio, legales y de otra índole en la creación y control de los documentos para establecer los objetivos

4.3: Deberá documentarse la definición y el alcance del SGD

Fase 2. **Liderazgo** (punto 5 del estándar)

5.1: La Alta Dirección deberá demostrar su compromiso con el SGD

5.2: La Alta Dirección deberá establecer la política de gestión documental

5.3: La Alta Dirección deberá asegurar que los roles organizativos, responsabilidades y competencias se definan, sean comunicados y asignados a todos los afectados

Fase 3. **Planificación** (punto 6 del estándar)

6.1: La organización debe considerar los factores externos e internos y sus requerimientos para determinar las oportunidades y posibles riesgos que precisen tratamiento.

6.2: La Alta Dirección deberá asegurarse que se establecen los objetivos de gestión documental y que éstos sean comunicados a todos los niveles y funciones

Fase 4. **Soporte** (punto 7 del estándar)

7.1: La Alta Dirección deberá asignar y mantener los recursos necesarios para el SGD

7.2: La organización deberá determinar la capacitación para el desempeño de las aplicaciones y procesos de gestión documental.

7.3: La organización deberá establecer un programa de formación continua en la creación y control de documentos.

7.4: La organización deberá establecer, implementar, documentar y mantener los procedimientos para la comunicación interna sobre el SGD, los objetivos y la política de gestión documental.

7.5: Deberá estar controlada la documentación requerida por el SGD.

Fase 5. **Operación** (punto 8 del estándar)

8.1: La organización deberá determinar, implementar, controlar y planificar los procesos necesarios para el tratamiento de las oportunidades y los riesgos y poder cumplir con los requisitos.

8.2: La organización deberá diseñar los procesos de gestión documental para establecer el SGD.

8.3: La organización deberá implementar los procesos en las aplicaciones para cumplir los objetivos de gestión documental.

Fase 6. **Evaluación del desempeño** (punto 9 del estándar)

9.1: La organización hará la supervisión, medición, análisis y evaluación del sistema

9.2: La organización establecerá su sistema de auditoría interna

9.3: La Dirección revisará el sistema de la organización

Fase 7. **Mejora** (punto 10 del estándar)

10.1: La organización establecerá el control de las no conformidades y acciones correctivas

10.2: La organización definirá la mejor forma de realizar la mejora continua del sistema

Además el estándar posee 3 anexos:

ANEXO A: dividido en los dos grandes bloques "Creación y Control", están distribuidos los procesos, subprocesos y su propósito (controles). En el documento <<Declaración de Aplicabilidad>> deberemos justificar aquellos que no apliquen y su correspondiente justificación. Este anexo es normativo y de obligado cumplimiento.

ANEXO B: Este anexo informativo, nos explica en su parte genérica la lista de documentos/registros, que aplican al sistema de gestión (muestra una correlación entre los principales sistemas de gestión).

Esta guía nos aporta información sobre cómo controlar sistemáticamente los documentos y registros requeridos por otros sistemas de gestión, muy útil a la hora de integrar sistemas y no redundar en documentación.

ANEXO C: para evaluar el sistema, y a modo de sugerencia, la tabla C.1 nos aporta una posible lista de preguntas de control para verificar la efectividad del sistema.

Relación con otros estándares/modelos

De manera particular, los principales estándares relacionados son los siguientes:

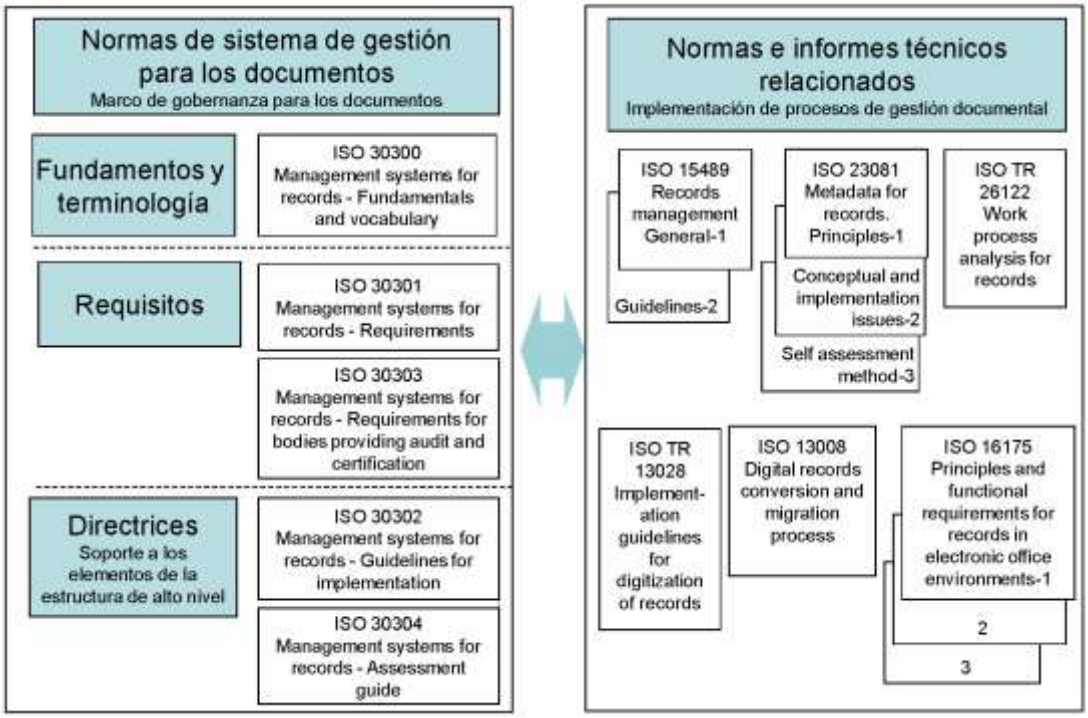

Ilustración 15 Estándares elaborados por el ISO TC 46/SC11 sobre SGD y estándares internacionales e informes técnicos relacionados

EFQM Modelo de Excelencia – 2013

Entidad Emisora

El modelo EFQM es propiedad de *European Foundation for Quality Management (EFQM).* Fue presentado por la EFQM en 1991, bajo el patrocinio de la Comisión Europea. En años sucesivos, se ha ido actualizando y existen versiones especiales para organizaciones de servicios públicos y para PYMEs. La versión actual es de 2013.

- **Disponibilidad**

El modelo puede comprarse en la web de EFQM (www.efqm.org). En el Club de Excelencia en la Gestión (CEG) (www.clubexcelencia.org/publicacions) se puede adquirir en español al precio de 24,96€ para socios y 31,20€ para no socios. Ambos precios son a fecha de publicación de este documento.

En la mismas páginas web se pueden adquirir otras publicaciones que son de excelente ayuda para la implantación del modelo y su evaluación.

Clasificación (taxonomía)

EFQM es un modelo internacional buenas prácticas cuya bondad reside en que puede ser aplicado a cualquier organización, proporcionando un lenguaje común y una estructura coherente de áreas de gestión y resultados que permite siempre establecer la correlación entre la estrategia, su despliegue y los resultados obtenidos. Como activo fundamental incluye el aprendizaje y la mejora continua del sistema de gestión.

EFQM no es certificable sino evaluable.

- **Referencia normativa**

EFQM no es un modelo normativo sino un modelo de referencia que constituye una guía de buenas prácticas, cuyo concepto fundamental es la autoevaluación basada en un análisis detallado del funcionamiento del sistema de gestión de la

organización, usando como guía los criterios del modelo y el esquema de evaluación REDER.

El modelo EFQM está basado en los 8 Conceptos Fundamentales de la Excelencia.

Ilustración 16 8 Conceptos Fundamentales de la Excelencia

- **Ámbito de aplicación**

Este modelo es aplicable a todo tipo de organizaciones, independientemente de su tamaño, sector o madurez y abarca todas las actividades de la organización.

- **Certificación**

Las entidades que hayan implantado el modelo pueden voluntariamente presentar su candidatura para obtener un Reconocimiento a la Excelencia en la Gestión basado en la evaluación de la aplicación del Modelo EFQM de Excelencia, que se instrumenta mediante los Sellos de Excelencia EFQM:

- Excelencia Europea 200+: También conocido como "Compromiso hacia la excelencia". Se accede a este sello cuando el resultado de la Autoevaluación con respecto al Modelo EFQM de Excelencia, es homologado en 200 ó más puntos EFQM. Con este proceso de reconocimiento, la organización entra en una dinámica de la mejora continua a través de las acciones de mejora. Para este nivel, la homologación por un evaluador no es imprescindible si la organización posee un Certificado ISO 9001 en vigor.
- Excelencia Europea 300+ o 3 estrellas: Se obtiene este sello cuando el resultado de la Autoevaluación, con respecto al Modelo EFQM de Excelencia, es homologado por un evaluador en 300 ó más puntos EFQM. La organización

elabora una Memoria descriptiva de las actividades de gestión y resultados conseguidos.

- Excelencia Europea 400+ o 4 estrellas: Se obtiene este sello cuando el resultado de la Autoevaluación con respecto al Modelo EFQM de Excelencia es homologado por un evaluador en 400 ó más puntos EFQM. El proceso de obtención es idéntico al correspondiente con el nivel de Excelencia Europea 300+.
- Excelencia Europea 500+ o 5 estrellas: Se obtiene este sello cuando el resultado de la Autoevaluación con respecto al Modelo EFQM de Excelencia es homologado por un evaluador en 500 ó más puntos EFQM. El formato de la Memoria para este nivel es distinto al de la memoria para los niveles de Excelencia Europea 300+ y 400+

Estos sellos se renuevan bianualmente, tras visita de evaluadores acreditados.

Objetivos del modelo

El objetivo fundamental de este modelo es ayudar a las organizaciones a conocerse mejor a sí mismas y, en consecuencia, a mejorar su funcionamiento permitiéndoles obtener una visión general de sus fortalezas y oportunidades de crecimiento.

Para ello proporcional un conjunto de buenas prácticas y un esquema de evaluación que:

- Estimulan y ayudan a las organizaciones en el desarrollo de actividades de mejora enfocadas en el logro de la excelencia en la satisfacción al cliente, la satisfacción de los empleados, el impacto en la sociedad y en los resultados de negocios.
- Apoyan a los gerentes de las organizaciones en la implementación de la Gestión Total de Calidad como factor decisivo en el logro de la ventaja competitiva a nivel global.

Agentes facilitadores para su adopción/implementación

Como agente facilitador más importante para su adopción/implementación tenemos la facilidad de su uso consistente en autoevaluaciones frente al modelo realizadas con ayuda de la herramienta PERFIL / REDER. Esta autoevaluación permite a las

empresas ser ellas mismas las que obtengan una visión general de sus fortalezas actuales y oportunidades de crecimiento.

Otro agente facilitador muy importante es que el Modelo EFQM de Excelencia es un modelo que sirve para impulsar y estimular la mejora continua permitiendo conocer siempre la correlación entre lo que hacemos (enfoque) y lo que obtenemos (resultados) y por qué lo obtenemos. Esto es posible por la estructura del modelo en la que los Enfoques, es decir, lo que hacemos producen unos resultados clave, que evaluamos siempre, lo que nos permite establecer esa correlación y aprender e innovar

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

Con la ayuda del modelo EFQM las organizaciones han comenzado a ver la ventaja competitiva que significa la gestión integral de todas sus actividades para ganar eficiencia, efectividad y ventaja competitiva, asegurando el éxito a largo plazo al satisfacer las necesidades de los clientes, empleados, entidades financieras, accionistas y la comunidad en general. Eso significa convertirse en excelente y, en la práctica, una organización excelente se reconoce por su habilidad para identificar y responder de forma eficaz y eficiente a oportunidades y amenazas.

En detalle, sus ventajas competitivas se pueden resumir en:

- Tener los mecanismos necesarios para identificar los cambios en su entorno externo y traducirlos en escenarios futuros para la organización.
- Ser capaces de convertir sus estrategias en procesos, proyectos y estructuras organizativas alineadas que permiten implantar con la rapidez adecuada los cambios necesarios a lo largo de toda la cadena de valor.
- Dotar a sus procesos de medidas e indicadores de rendimiento que les permiten revisar la eficiencia y la eficacia de dichos procesos y como éstos contribuyen a los objetivos estratégicos.
- Utilizar los datos derivados del conjunto de medidas y de indicadores de rendimiento de sus procesos para tomar decisiones informadas, gestionar la mejora e impulsar la creatividad y la innovación.
- Adaptar rápidamente la estructura de la organización para apoyar la consecución de los objetivos estratégicos.

En definitiva, la implementación de la calidad total según el modelo EFQM permite alcanzar beneficios significativos, tales como un incremento en la eficiencia, reducción de costes y mayor satisfacción de los clientes, todo orientado a mejorar los resultados de negocio de la organización.

El riesgo de no usar el modelo de referencia EFQM está la falta de visión global que da EFQM de cómo debe funcionar una organización y, por tanto, en la falta de entendimiento de cómo tienen que contribuir todas las partes de la organización en la consecución de los objetivos y en el despliegue de las estrategias. Sin EFQM es fácil gastar recursos enormes y motivación del personal sin conseguir alcanzar los objetivos estratégicos porque no se tiene el foco preciso de donde hay que hacer acciones que den el máximo beneficio a la organización.

Por otro lado, la organización podría conseguir resultados pero sin tener idea exacta y precisa de por qué se han conseguido, es decir, que no conocería la correlación entre los enfoques y sus resultados, lo que le dificultaría poder aprender y, por tanto, podría darse el caso de obtener resultados extraordinarios pero no sostenibles en el tiempo como hacen las organizaciones excelentes.

Reconocimiento/reputación

Este modelo es ampliamente usado en toda Europa donde más de 300 empresas han sido galardonadas con un Premio en sus varias modalidades en los 22 años en que se lleva celebrando, y miles de empresas han sido reconocidas en alguna de las modalidades de los sellos de Excelencia. Solo en el año 2013, 531 organizaciones consiguieron reconocimiento de EFQM.

Directrices sobre su uso/implementación

El modelo EFQM de Excelencia consta de nueve criterios de los cuales los cinco primeros: Liderazgo; Estrategia; Personas; Alianzas y recursos; y Procesos, Productos y Servicios son los denominados: Agentes. Estos Agentes indican (en los sub-criterios) lo que debe hacerse (enfoques) para obtener unos resultados extraordinarios y sostenibles en el tiempo. Los siguientes cuatro criterios: Resultados en los clientes; Resultados en las personas; Resultados en la sociedad; y Resultados Clave indican los resultados que la organización debe medir y evaluar y son la consecuencia de la puesta en acción de los Agentes.

Ilustración 17 modelo EFQM

El mapa de la figura puede leerse de la siguiente manera: "Para alcanzar el éxito una organización necesita reforzar su liderazgo y establecer una clara estrategia. Necesita desarrollar y mejorar la política con sus empleados así como cuidar a los colaboradores y mejorar los procesos con el fin de dar valor añadido a los productos y servicios que ofrece a sus clientes. Si los enfoques son correctos y bien implementados, podrá alcanzar los objetivos que desea y lo que sus grupos de interés esperan".

De la evaluación de los resultados y de las acciones emprendidas por la organización se obtiene una comprensión de cuál es el rendimiento de la organización lo que le permite aprender y fomentar la creatividad y la innovación para la mejora continua del sistema.

Para la evaluación (auto) de la implementación del modelo nos valemos del Esquema Lógico REDER:

Ilustración 18 Esquema Lógico REDER

En los *Resultados* evaluamos lo que la organización consigue. En una organización excelente, los resultados muestran *tendencias* positivas y sostenidas, los objetivos son adecuados y se alcanzan, los resultados se comparan favorablemente con los de otros y están causados por los enfoques. Además el *alcance* de los resultados cubre todas las áreas relevantes para los implicados.

Para los *Enfoques l*o que se evalúa es lo que la organización piensa hacer y las razones para ello. En una organización excelente, el enfoque será *sano* (con fundamento claro, con procesos bien definidos y desarrollados, enfocado claramente a los actores) y estará *integrado* (apoyará la política y la estrategia y estará adecuadamente enlazado con otros enfoques).

En el *Despliegue* se evalúa lo que realiza la organización para poner en práctica el enfoque. En una organización excelente, el enfoque estará *implantado* en las áreas relevantes de una forma *estructurada*.

El apartado de *Evaluación y Revisión* se refiere a lo que hace la organización para evaluar y revisar el enfoque y su despliegue. En una organización excelente, el enfoque y su despliegue estarán sujetos con regularidad a *mediciones*, se emprenderán actividades de *aprendizaje* y los resultados de ambas servirán para identificar, priorizar, planificar y poner en práctica *mejoras*.

La mejor manera de implementar el modelo EFQM de Excelencia es:

59. Empezar por la Alta Dirección de la organización. Ésta debe asistir a una formación específica para entender el modelo y lo que significará para su organización, pues ellos deben ser en todo momento los líderes que impulsarán a la organización a la Excelencia.
60. Se recomienda crear un Equipo de Excelencia que sea el que establezca la forma en que se va a gestionar este viaje hacia la Excelencia de la organización. Prepararán un plan y lo comunicarán a toda la organización.
61. Todos los actores implicados recibirán formación en el modelo haciendo especial hincapié en la formación para realizar la autoevaluación eficazmente.
62. Recoger toda la información necesaria (datos y hechos) para la realización de la autoevaluación.
63. Hacer una autoevaluación y determinar en qué nivel de implementación se encuentra la organización. La autoevaluación proporciona una puntuación y en función de ella, y del nivel objetivo a alcanzar, se establece un Plan de Acción priorizando las áreas a mejorar. Todos los criterios tienen un peso de 10%, excepto Resultados para los clientes y Resultados clave que tienen un peso de 15%. No se puede obtener cero en ningún criterio.
64. Revisar el progreso del Plan de Acción periódicamente para actuar en caso de desviaciones.

65. Cuando finalice el plan de Acción, se realizara de nuevo una autoevaluación y se analizarán los datos para determinar si se ha conseguido la puntuación que permite el reconocimiento o sello de excelencia que teníamos como objetivo. Si es así, se describe el resultado en la Memoria correspondiente (según el nivel de reconocimiento ésta es diferente).
66. Pedir la homologación por evaluador acreditado.
67. Si la puntuación es superior a 700 puntos se recomienda presentarse al Premio Europeo de Excelencia.
68. La Excelencia no es un estado final, sino un viaje sin fin, por lo que la autoevaluación debe ser una actividad continua en una organización excelente.

El modelo se puede implementar en su totalidad por criterios completos, es decir, todos los sub-criterios de cada criterio, o bien existe la posibilidad de hacerlo transversalmente implementando aquellos sub-criterios de cada criterio que tienen relación entre si y con una determinada área de actividad o competencia, son los llamados Ejes Transversales del modelo EFQM.

Los Ejes Transversales permiten la lectura del Modelo EFQM con carácter horizontal recogiendo la información de forma transversal, de modo que el análisis de los procesos y la gestión de las medidas correctoras ofrezcan una mayor homogeneidad en su comprensión.

Los Ejes Transversales y los sub-criterios que participan, o tienen influencia en cada Eje, son los siguientes:

Eje Transversal	Sub-criterios asociados
Comunicación	1c, 1d, 2d, 2e, 3d, 5b, 6, 7, 8
Responsabilidad Social de la Organización	1a, 1c, 1d, 1e, 2a, 2b, 2c, 2d, 3a, 3b, 3c, 3e, 4a, 4b, 4c, 5c, 5d, 5e, 6a, 7a, 8, 9
Creatividad e Innovación	1a, 2b, 3c, 4a, 4e, 5b, 5c, 5e, 6, 7, 8, 9
Clientes	1c, 2a, 2c, 5b, 5c, 5d, 5e, 6
Gobierno de la Organización	1b, 2a, 2b, 4b, 9
Conocimiento	2b, 3b, 4e, 7, 9
Mercado y Definición de Mercado	2a, 2b, 2c, 3b, 4a, 5c, 5d, 6, 7, 8a, 9
Personas de la Organización	1d, 2a, 2c, 3a, 3b, 3c, 3d, 3e, 7
Metodología de Procesos	1b, 2d, 5a, 5b, 6, 7, 8, 9
Proveedores / Partners	1c, 2a, 2c, 4a, 9
Sostenibilidad	1b, 1c, 2a, 2c, 3b, 5c, 6, 7, 8, 9

Trabajando con los Ejes Transversales la organización puede enfocarse en aspectos específicos y analizar y desplegar acciones correctivas actuando con mayor certidumbre sobre diferentes sub-criterios, facilitando la síntesis y agrupación de las áreas de mejora detectadas en la autoevaluación.

Relación con otros estándares/modelos

UNE-EN ISO 9001:2008 Sistemas de Gestión de la Calidad – Requisitos

PCI DSS

PCI DSS (Payment Card Industry Data Security Standard)- Requirements and Security Assessment Procedures

Entidad Emisora

PCI Security Standard Council (PCI SSC)

Es un foro abierto y de ámbito mundial fundado en 2006, cuyo fin es el establecimiento, la mejora, el almacenamiento, la difusión y la aplicación permanentes de las normas de seguridad de la industria de tarjetas de pago (PCI).

Su misión es aumentar la seguridad de los datos de cuentas de pago mediante la promoción de la educación y el conocimiento de las Normas de seguridad de la PCI.

El PCI SSC es una sociedad de responsabilidad limitada (LLC) constituida en EE.UU.

Fue fundada por American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc.

Las cinco marcas de pago comparten de manera equitativa el control del consejo, tienen igual participación en el PCI SCC y comparten la responsabilidad de llevar a cabo las actividades de la organización.

Se anima a otros interesados de la industria a unirse al grupo y a examinar las adiciones o modificaciones propuestas para las normas.

- **Disponibilidad**

El estándar se puede obtener gratuitamente en la web del *PCI Security Standard Council*: http://www.pcisecuritystandards.org

Clasificación (taxonomía)

Es un estándar internacional con aplicación en la industria de tarjetas de pago. Aplica a comerciantes, vendedores, prestadores de servicios, consultorías de seguridad, ...

- **Referencia normativa**

- Última versión: 3.0 de noviembre 2013. Existe en inglés, japonés y chino.
- La versión anterior (2.0) existía en español y en varios idiomas europeos y asiáticos.

El PCI SSC elabora otras normas relacionadas:

- **Del estándar de seguridad de datos para las aplicaciones de pago (PA-DSS):**
    - El cumplimiento de PCI DSS como tal puede no ser aplicable a los proveedores de aplicaciones de pago puesto que la mayoría no almacenan, procesan o transmiten datos de titulares de tarjetas. Sin embargo, debido a que estas aplicaciones de pago son utilizadas por comerciantes para almacenar, procesar y transmitir datos del titular, las aplicaciones de pago deben facilitar el cumplimiento del estándar por parte de los comerciantes.
    - Los requisitos del estándar de aplicaciones de pago (PA-DSS *Payment Application Security Standard*) vienen determinados por los requerimientos de PCI DSS con el fin de definir lo que una aplicación debe tener para facilitar el cumplimiento de PCI DSS.
    - Las aplicaciones seguras de pago, cuando se implementen en un entorno compatible con PCI DSS, minimizarán las posibles brechas de seguridad que puedan poner en peligro los datos de autenticación del titular de la tarjeta. Sin embargo, el uso de una aplicación compatible con PA-DSS por sí solo no asegura la conformidad con DSS, ya que dicha aplicación debe ser implementado en un entorno compatible con PCI DSS y de acuerdo con PA-DSS.
- **Requisitos de Seguridad de transacciones con PIN (PTS Pin Transaction Security):**
    - Identifica los requisitos de seguridad mínimos para las transacciones de intercambio basadas en PIN.
    - Describe los requisitos mínimos aceptables para asegurar los PINs y las claves de cifrado.
    - Ayuda a las partes involucradas en los sistemas de pago electrónico estableciendo garantías para que el PIN de los titulares de las tarjetas no se vea comprometido.
- **Ámbito de aplicación**

Aplica a todas las entidades que participan en los procesos de las tarjetas de pago**,** entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas.

PCI DSS cataloga a estas organizaciones en comercios o *merchants* (súper/hipermercados, autopistas*, e-commerce*, agencias de viajes, etc.), proveedores de servicios o *service providers* (ISP/ASP, pasarelas de pago, fabricantes de tarjetas, servicios de envío de tarjetas, procesadores de transacciones, etc.) y entidades financieras o *acquirers* (bancos, cajas de ahorro, entidades de crédito, etc.).

- **Certificación**

Desde el punto de vista de seguridad supone la conformidad con los requisitos de PCI DSS para la gestión de la seguridad, las políticas, procedimientos, arquitectura de red, diseño de software y otras medidas críticas de protección.

Las empresas con grandes volúmenes de transacciones deberán sufrir una evaluación anual "in situ" realizada por un Evaluador de Seguridad Cualificado. A las compañías que procesan menos de 80.000 transacciones por año se les permite realizar una auto evaluación utilizando un cuestionario provisto por el Consorcio del PCI (PCI SSC).

Objetivos del estándar

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos de los titulares de tarjetas y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial.

La conformidad con el estándar supone el compromiso de que los datos de los clientes titulares de tarjeta de pago se mantienen seguros a lo largo de cada transacción, y que tanto los clientes como el proveedor del servicio están protegidos contra los posibles costes y daños derivados de las violaciones de datos.

Agentes facilitadores para su adopción/implementación

Es un requerimiento de mercado "de facto".

- **Ventaja competitiva y riesgos relacionados con su no implantación o uso**

Las compañías que procesan, guardan o trasmiten datos de tarjetas deben cumplir con el estándar o se arriesgarían a la pérdida de sus permisos para procesar las tarjetas de crédito y débito (pérdida de franquicias), se enfrentarían a auditorías rigurosas o pagos de multas. Los comerciantes y proveedores de servicios de tarjetas de crédito y débito, deben validar el cumplimiento del estándar en forma periódica.

Reconocimiento/reputación

Este estándar es utilizado por entidades financieras de todo el mundo.

Directrices sobre su uso/implementación

Proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas, constituyendo un conjunto mínimo de requisitos que se puede acompañar con el uso de controles y prácticas adicionales para mitigar otros riesgos.

Descripción general de los 12 requisitos de las PCI DSS:

Desarrollar y mantener una red segura	Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta
	No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.
Proteger los datos del titular de la tarjeta	Proteja los datos del titular de la tarjeta que fueron almacenados
	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas
Mantener un programa de administración de vulnerabilidad	Utilice y actualice con regularidad los programas o software antivirus
	Desarrolle y mantenga sistemas y aplicaciones seguras
	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa

Implementar medidas sólidas de control de acceso	Asignar una ID exclusiva a cada persona que tenga acceso por computador
	Restringir el acceso físico a los datos del titular de la tarjeta
Supervisar y evaluar las redes con regularidad	Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas
	Pruebe con regularidad los sistemas y procesos de seguridad
Mantener una política de seguridad de información	Mantenga una política que aborde la seguridad de la información para todo el personal

Proceso de implementación:

Es un proceso cíclico cuyos pasos, a alto nivel, son:

Evaluar

- Conocer el estándar para entender lo que requiere a la organización en particular.
- Realizar un catálogo de activos y procesos: identificar todos los sistemas, personal y procesos involucrados en la transmisión, tratamiento o almacenamiento de los datos de los titulares de tarjetas determinando su flujo desde el inicio hasta el final.
- Nota: la responsabilidad del cumplimiento de PCI se extiende también a terceros involucrados en el flujo del proceso de datos, por lo que se debe asegurar su conformidad con el estándar. La evaluación debe ser exhaustiva para comprender qué elementos pueden ser vulnerables a los ataques de seguridad y hacia dónde se debe enfocar la corrección.
- Encontrar las vulnerabilidades: utilizar el formulario de autoevaluación (SQA *Self-Assessment Questionnaire*) para ayudar en la autoevaluación y tecnologías adecuadas para descubrir los sistemas inseguros.
- Validar con terceros: la complejidad del entorno puede requerir que se realice una correcta evaluación por parte de un Evaluador de Seguridad Cualificado (QSA *Qualified Security Assessor*). y/o un Proveedor Aprobado para el Análisis (ASV *Approved Scanning Vendor*)

- **Corregir**

La corrección es el proceso de subsanar vulnerabilidades – incluyendo defectos técnicos en código de software o prácticas inseguras en la forma en que una organización procesa y/o almacena datos de titulares de tarjetas:

- Exploración de la red con herramientas de software que analizan la infraestructura y localizan vulnerabilidades conocidas.
- Revisión y corrección de vulnerabilidades encontradas en la evaluación "in situ" (si corresponde) o mediante el proceso de autoevaluación
- Clasificación y ranking de las vulnerabilidades para ayudar a priorizar las actividades de corrección.
- Aplicar parches, soluciones, arreglos y cambios en los procesos y flujos de trabajo inseguros.
- Volver a analizar para comprobar que la corrección ha sido eficaz.

- **Informar**
  - Para el cumplimiento de PCI DSS es necesaria la existencia de informes periódicos. Deben ser enviados al banco adquiriente y a las empresas de tarjetas de pago con las que se trabaja.
  - PCI SSC no es responsable de hacer cumplir el estándar.
  - Todos los comerciantes, prestadores de servicios y procesadores pueden ser requeridos para presentar informes trimestrales de análisis, que deben ser realizados por un Proveedor Aprobado para el Análisis (ASV *Approved Scanning Vendor*).
  - Las empresas con grandes volúmenes de transacciones deberán sufrir una evaluación "in situ" anual realizada por un Evaluador de Seguridad Cualificado (*QSA Qualified Security Assessor*) y presentar los resultados a cada adquirente.

Las empresas con menor volumen de transacciones pueden ser obligadas a presentar una atestación anual de acuerdo al cuestionario de autoevaluación.

En general depende del banco adquiriente y de las empresas de tarjetas de pago con las que se trabaja.

Relación con otros estándares/modelos

Supporting Documents		
Glossary v2.0	Octubre 2010	
Navigating the PCI DSS v2.0	Octubre 2010	

PCI DSS AOC - Merchants v2.0	Octubre 2010	(español)
PCI DSS AOC - Service Providers v2.0	Octubre 2010	(español)
Prioritized Approach for PCI DSS Version 2.0	Mayo 2011	
Prioritized Approach Tool Version 2.0	Mayo 2011	
Summary of Changes from Prioritized Approach for PCI DSS Version 1.2 to 2.0	Mayo 2011	
ROC Reporting Instructions for PCI DSS v2.0	Septiembre 2011	
FAQs for use with ROC Reporting Instructions for PCI DSS v2.0	Septiembre 2011	
PCI DSS Quick Reference Guide v2.0	Octubre 2010	
PCI Quick Reference Order Form	Enero 2010	
Feedback		
Summary of PCI DSS and PA-DSS Feedback 2012	Septiembre 2012	
PCI DSS and PA-DSS 3.0 Version 3.0 Change Highlights	Agosto 2013	

Índice de figuras: