

Revista
Española de
Innovación,
Calidad e
Ingeniería del Software



Volumen 6, Número 3 (especial XI JICS), noviembre, 2010

Web de la editorial: www.ati.es

Web de la revista: www.ati.es/reicis

E-mail: calidadsoft@ati.es

ISSN: 1885-4486

Copyright © ATI, 2010

Ninguna parte de esta publicación puede ser reproducida, almacenada, o transmitida por ningún medio (incluyendo medios electrónicos, mecánicos, fotocopias, grabaciones o cualquier otra) para su uso o difusión públicos sin permiso previo escrito de la editorial. Uso privado autorizado sin restricciones.

Publicado por la Asociación de Técnicos de Informática (ATI), Via Laietana, 46, 08003 Barcelona.

Secretaría de dirección: ATI Madrid, C/Padilla 66, 3º dcha., 28006 Madrid



Editor

Dr. D. Luís Fernández Sanz (director)

Departamento de Ciencias de la Computación, Universidad de Alcalá

Miembros del Consejo Científico

Dr. Dña. Idoia Alarcón

Depto. de Informática
Universidad Autónoma de Madrid

Dr. D. José Antonio Calvo-Manzano

Depto. de Leng y Sist. Inf. e Ing. Software
Universidad Politécnica de Madrid

Dra. Tanja Vos

Depto. de Sist. Informáticos y Computación
Universidad Politécnica de Valencia

Dña. M^a del Pilar Romay

CEU Madrid

Dr. D. Alvaro Rocha

Universidade Fernando Pessoa
Porto

Dr. D. Oscar Pastor

Depto. de Sist. Informáticos y Computación
Universidad Politécnica de Valencia

Dra. Dña. María Moreno

Depto. de Informática
Universidad de Salamanca

Dra. D. Javier Aroba

Depto de Ing. El. de Sist. Inf. y Automática
Universidad de Huelva

D. Guillermo Montoya

DEISER S.L.
Madrid

Dr. D. Pablo Javier Tuya

Depto. de Informática
Universidad de Oviedo

Dra. Dña. Antonia Mas

Depto. de Informática
Universitat de les Illes Balears

D. Jacques Lecomte

Meta 4, S.A.
Francia

Dra. Raquel Lacuesta

Depto. de Informática e Ing. de Sistemas
Universidad de Zaragoza

Dra. María José Escalona

Depto. de Lenguajes y Sist. Informáticos
Universidad de Sevilla

Dr. D. Ricardo Vargas

Universidad del Valle de México
México

Contenidos

REICIS

Editorial	4
<i>Luís Fernández-Sanz</i>	
Presentación	5
<i>Luis Fernández-Sanz</i>	
Taxonomía de factores críticos para el despliegue de procesos software	6
<i>Sussy Bayona, Jose Calvo-Manzano, Gonzalo Cuevas, Tomás San Feliu</i>	
Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001	25
<i>Antoni Lluís Mesquida, Antònia Mas, Esperança Amengual, Ignacio Cabestrero</i>	
Implantación de CMMi nivel de madurez 2 en una PYME	35
<i>Fernando Ramos, Olimpia Torres, Nicolás Sánchez, Manuel Alba</i>	
Pruebas de Aceptación en Sistemas Navegables	47
<i>José Ponce, Francisco José Domínguez-Mayo, M. José Escalona, Manuel Mejías, Diego Pérez, Gustavo Aragón, Isabel Ramos</i>	
Análisis de métricas básicas y herramientas de código libre para medir la mantenibilidad	56
<i>Emanuel Irrazábal, Javier Garzás</i>	
Reduciendo distancia en proyectos de Desarrollo de Software Global Ágiles con técnicas de Ingeniería de Requisitos	66
<i>Mariano Minoli, Valeria de Castro, Javier Garzás</i>	
CMMI después de la certificación	76
<i>Vanesa Cabral y Juanjo Cukier</i>	
Comparando UML y OWL en la representación del conocimiento: correspondencia sintáctica	84
<i>Susana M. Ramírez, Yisel Alonso, Violen Hernández, Arturo Cesar Arias y Dayana La Rosa</i>	

Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001

Antoni Lluís Mesquida, Antònia Mas, Esperança Amengual, Ignacio Cabestrero
Departamento de Matemáticas e Informática, Universitat de les Illes Balears
{antoni.mesquida, antonia.mas, eamengual}@uib.es, nacho.cabestrero@gmail.com

Resumen

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

Palabras clave: Sistema de Gestión Integrado, Sistema de Gestión de Calidad (SGC), ISO 9001, ISO/IEC 20000, ISO/IEC 27001, ISO/IEC 9004.

Integrated Management System according to ISO 9001, ISO/IEC 20000 and ISO/IEC 27001

Abstract

As a consequence of the successful implementation of Quality Management Systems (QMS) according to ISO 9001 performed some years ago by an important number of organizations, nowadays when these companies decide to implement new standards, such as ISO/IEC 20000 to manage their services or ISO/IEC 27001 to manage information security, they have already implemented a QMS according to ISO 9001. In order to facilitate the implementation of these new standards to these organizations a study has been carried out, both to analyse the existing relations between the requirements proposed by these standards and to identify other unshared requirements. This paper presents a new Integrated Management System which widens the scope of the ISO 9001 QMS with the specific requirements of the two above mentioned standards.

Key words: Integrated Management System, Quality Management System (QMS), ISO 9001, ISO/IEC 20000, ISO/IEC 27001, ISO/IEC 9004.

Mesquida, A.L., Mas, A., Amengual, E., Cabestrero, I., "Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001", REICIS, vol. 6, no.3, 2010, pp.25-34. Recibido: 8-11-2010; revisado: 14-11-2010; aceptado: 24-11-2010

1. Introducción

Numerosas organizaciones del sector TI han optado por la implantación de sistemas de gestión con el objetivo de garantizar la eficacia y fiabilidad de sus procesos de negocio. Estas organizaciones normalmente han implantado sus sistemas de gestión de calidad, gestión de servicios y seguridad de la información, entre otros, de forma independiente o escasamente integrada. Sin embargo, en todos los sistemas de gestión existen ciertos elementos comunes que pueden ser gestionados de un modo integrado.

La necesidad de obtener una visión global de los sistemas de gestión, haciéndolos compatibles entre sí, de forma que permita establecer unos objetivos alineados y facilite la toma de decisiones, ha provocado que muchas organizaciones del sector se hayan cuestionado la existencia de sistemas separados y deseen integrar sus sistemas de gestión.

Durante los últimos años han surgido diversas iniciativas para ofrecer una solución a la falta de integración entre los sistemas de gestión. En ese sentido, PAS 99:2006 *Specification of common management system requirements as a framework for integration* [1], publicada por el *British Standards Institution* (BSI), es el primer marco que ha sido elaborado y constituye una especificación de requisitos comunes de los sistemas de gestión. Este estándar británico fue desarrollado como respuesta a la demanda del mercado de alinear los procesos y procedimientos en una estructura que permitiera operar con mayor eficacia. PAS 99 organiza sus requisitos bajo las seis categorías de elementos comunes propuestos en la ISO Guide 72:2001 *Guidelines for the justification and development of management system standards* [2], una norma para justificar y desarrollar estándares de sistemas de gestión.

En 2008, la *International Organization for Standardization* (ISO) publicó *The integrated use of management system standards* [3] que ofrece una guía sobre cómo integrar los requisitos de múltiples estándares de sistemas de gestión, ISO o no ISO, con el sistema de gestión de una organización.

En España, AENOR publicó en 2005, la norma UNE 66177:2005 [4] con la intención de proporcionar directrices para desarrollar, implantar y evaluar procesos de integración de los sistemas de gestión existentes en una organización.

Por otra parte, nuestro grupo de investigación, MiProSoft, en el año 2002 desarrolló un modelo de implantación simultánea de las normas ISO 9001 e ISO/IEC 15504 durante el

proyecto QuaSAR I [5] [6]. A lo largo de estos años hemos seguido trabajando en esta misma línea, y nuestro último resultado está relacionado con facilitar la implantación de la norma ISO/IEC 27001:2005 [7] en una empresa que ya tiene un nivel de madurez 1 según ISO/IEC TR 15504-7:2008 (Pathfinder) [8].

El propósito de este artículo es identificar e interpretar los requisitos del sistema de gestión de calidad de tres normas ISO, analizando tanto los requisitos que estas normas tienen en común como los requisitos no compartidos entre ellas. Concretamente las normas consideradas son las siguientes:

- ISO 9001:2008 Sistemas de gestión de la calidad - Requisitos [9]
- ISO/IEC 20000-1:2005 Tecnología de la información - Gestión del servicio - Parte 1: Especificaciones [10] e
- ISO/IEC 27001:2005 Tecnología de la información - Técnicas de seguridad - Sistemas de Gestión de la Seguridad de la Información (SGSI) - Requisitos [11].

El objetivo final de la investigación en el que se enmarca este trabajo es llegar a elaborar una guía completa para la alineación y/o integración de los sistemas de gestión de las tres normas anteriores que permita la implantación efectiva de más de una de ellas en una organización.

2. Estándares de sistemas de gestión analizados

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

Esta norma internacional especifica los requisitos de un sistema de gestión de la calidad. La edición actual, ISO 9001:2008, sustituye a la tercera edición (ISO 9001:2000) que ha sido modificada para clarificar puntos en el texto y aumentar la compatibilidad con otras normas.

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

existente(s) con la finalidad de establecer un sistema de gestión de la calidad que cumpla con los requisitos de esta norma internacional”.

Asimismo, se han desarrollado normas específicas que constituyen una guía para la aplicación de la norma ISO 9001 en un determinado campo:

- ISO/IEC 90003:2004 *Software engineering - Guidelines for the application of ISO 9001:2000 to computer software* [12] proporciona una guía para la aplicación de ISO 9001 en la adquisición, suministro, desarrollo, operación y mantenimiento del software.
- ISO/IEC TR 90005:2008 *Systems engineering - Guidelines for the application of ISO 9001 to system life cycle processes* [13] hace lo propio con el área de sistemas.

2.2. ISO/IEC 20000-1:2005 Tecnología de la información - Gestión del servicio - Parte 1: Especificaciones

La norma ISO/IEC 20000-1 promueve la adopción de un enfoque de procesos integrados, para una provisión eficaz de servicios gestionados que satisfaga los requisitos del negocio y de los clientes.

Con la intención de desarrollar una guía para la aplicación de la norma ISO 9001 a la gestión de servicios de TI, ISO inició en 2008 un nuevo proyecto denominado ISO/IEC NP 90006 *Information technology - Guidelines for the application of ISO 9001:2000 to IT service management* [14]. Sin embargo, trascurridos dos años, el proyecto sigue en la misma fase inicial.

2.3. ISO/IEC 27001:2005 Tecnología de la información - Técnicas de seguridad - Sistemas de Gestión de la Seguridad de la Información (SGSI) - Requisitos

Esta norma internacional proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de gestión de Seguridad de la Información (SGSI).

ISO/IEC 27001, en su apartado 0.3 Compatibilidad con otros sistemas de gestión, asegura que esta norma internacional sigue las pautas marcadas en las normas ISO 9001:2000 e ISO 14001:2004 para asegurar una implementación integrada y consistente con las mencionadas normas de gestión. Esta norma internacional está diseñada para posibilitar a una organización el adaptar su SGSI a los requisitos de los sistemas de gestión

mencionados. Más concretamente, en el anexo C.1 de la misma se muestra la relación entre este estándar y la norma ISO 9001:2000.

3. Estudio de las relaciones entre los sistemas de gestión de las tres normas

Después de años de relaciones y de trabajo continuado con las empresas del sector TIC de nuestro entorno más próximo en la aplicación de resultados de investigación, hemos podido observar que, en la mayoría de casos, cuando una empresa decide implantar una norma relativa a la gestión de servicios o a la gestión de la seguridad de la información, ya ha tenido otras experiencias previas, principalmente, con la implantación de alguna versión de la norma ISO 9001. Por este motivo, para realizar el trabajo que se presenta en este artículo, hemos partido de la norma ISO 9001:2008 y hemos realizado una investigación en dos frentes:

- Por una parte hemos analizado las relaciones y correspondencias entre los requisitos de los sistemas de gestión de la norma ISO 9001 y los de la norma ISO/IEC 20000-1.
- Por otra parte, hemos hecho lo mismo entre la norma ISO 9001 y la norma ISO/IEC 27001.

Ambos estudios han sido llevados a cabo siguiendo una estrategia iterativa, en la cual, cada uno de los requisitos de las normas ISO/IEC 20000-1 e ISO/IEC 27001 han sido comparados con todos los requisitos de la norma ISO 9001. Durante el análisis, se han establecido tres tipos distintos de correspondencias que se detallan en el siguiente apartado.

3.1. Tipos de relaciones

- **Relación total.** El requisito de la norma ISO/IEC 20000-1 o ISO/IEC 27001 en cuestión ya está contemplado por algún requisito de la norma ISO 9001. En este caso, al definir el nuevo sistema de gestión integrado, no se deberá añadir ningún aspecto específico, referente a la gestión de servicios de TI o a la seguridad de la información, al SGC ya implantado.

Un ejemplo de este tipo de relación es el siguiente: La norma ISO/IEC 20000-1 trata los requisitos de la documentación en su apartado 3.2: “Los proveedores del servicio deben facilitar documentos y registros para asegurar una planificación,

operación y control de la gestión del servicio efectivas”. Sin embargo, este requisito ya queda cubierto por la norma ISO 9001 en su apartado 4.2.1.d: “La documentación del sistema de gestión de la calidad debe incluir los documentos, incluidos los registros que la organización determina que son necesarios para asegurarse de la eficaz planificación, operación y control de sus procesos”. Del mismo modo, la norma ISO/IEC 27001 también cubre este requisito en su apartado 4.3.1.g: “Los procedimientos documentados que necesita la organización para asegurar una correcta planificación, operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles”.

- **Relación parcial.** El requisito de la norma ISO/IEC 20000-1 o ISO/IEC 27001 en cuestión amplía algún requisito de la norma ISO 9001 con aspectos propios de la gestión de servicios de TI o de la seguridad de la información.

Un ejemplo de este tipo de relación es el caso de los requisitos relacionados con el compromiso de la dirección, recogidos en el apartado 5.1 de la norma ISO 9001. En este caso, los requisitos del SGC de la norma ISO 9001 deben ser ampliados con aspectos específicos de la gestión de servicios, recogidos en los apartados 3.1.e, f y g de la norma ISO/IEC 20000-1, y con aspectos específicos de la seguridad de la información, detallados en el apartado 5.1.c de la norma ISO/IEC 27001.

- **Inexistencia de relación.** Cuando las normas ISO/IEC 20000-1 o ISO/IEC 27001 añaden requisitos propios de la gestión de servicios de TI o de la seguridad de la información.

Un ejemplo de este caso se da en los apartados 4.1, 4.2, 4.3 y 4.4 de la norma ISO/IEC 20000-1 en los que se amplían, con aspectos específicos de la gestión de servicios de TI, las definiciones de las cuatro etapas de la metodología Planificar-Hacer-Verificar-Actuar (PHVA), introducidas en el apartado 0.2 de la norma ISO 9001.

3.2. Elaboración de guías de implantación de sistemas de gestión

A partir de las relaciones extraídas en el estudio, se han elaborado dos guías de implantación de sistemas de gestión. La primera de ellas ha sido diseñada con el objetivo de

implantar el sistema de gestión de servicios de TI que propone la norma ISO 20000-1 a partir del sistema de gestión de la norma ISO 9001. La segunda guía pretende facilitar la implantación del sistema de gestión de seguridad de la información de la norma ISO/IEC 27001 a partir del sistema de gestión de la norma ISO 9001. Ambas guías guardan el mismo formato que las guías de aplicación de ISO 9001 referenciadas anteriormente [12] [13] [14].

4. Un nuevo sistema de gestión integrado

El sistema de gestión integrado resultante de esta investigación parte de los requisitos del sistema de gestión de calidad propuestos por la norma ISO 9001 y los amplía con todos los requisitos específicos de gestión de servicios de TI y de gestión de seguridad de la información que describen las normas ISO/IEC 20000-1 e ISO/IEC 27001.

La tabla 1 muestra en la primera columna únicamente los requisitos de la norma ISO 9001 que deberían ser ampliados con requisitos propios de gestión de servicios, especificados en la segunda columna, y con requisitos propios de la seguridad de la información, que se muestran en la tercera columna de la tabla. Es decir, la tabla recoge todas las relaciones parciales detectadas descritas en el apartado 3.1.

Es importante observar que el SGC integrado también deberá contemplar los requisitos específicos de gestión de servicios de TI y de gestión de seguridad de la información. Estos requisitos son los que no han guardado relación con ninguna categoría de requisitos de la norma ISO 9001, es decir, el tercer tipo de relación descrito en el apartado 3.1.

5. Conclusiones

En este artículo se ha ofrecido una visión de la situación actual de los estándares de sistemas de gestión más comúnmente demandados por las organizaciones del sector TI con la intención, tanto de presentar los modelos existentes, como de identificar sus elementos comunes, para crear un nuevo sistema de gestión integrado. El sistema de gestión integrado presentado toma como base los requisitos del SGC propuestos por la norma ISO 9001 y los amplía con todos los requisitos específicos de gestión de servicios de TI y de gestión de

seguridad de la información que describen las normas ISO/IEC 20000-1 e ISO/IEC 27001 respectivamente.

ISO/IEC 9001:2008	ISO/IEC 20000-1:2005	ISO/IEC 27001:2005
0.2 Enfoque basado en procesos	4 Planificación e implementación de la gestión del servicio	0.2 Enfoque por proceso
1 Objeto y campo de aplicación	1 Objeto y campo de aplicación	4 Sistema de gestión de seguridad de la información
4 Sistema de gestión de la calidad	3 Requisitos de un sistema de gestión	4.1 Requisitos generales
4.1 Requisitos generales		4.3 Requisitos de la documentación
4.2 Requisitos de la documentación	3.2 Requisitos de la documentación	4.3.1 Generalidades
4.2.1 Generalidades		4.3.1 Generalidades
4.2.2 Manual de la calidad	3.2 Requisitos de la documentación	4.3.2 Control de documentos
4.2.3 Control de los documentos	3.2 Requisitos de la documentación	4.3.3 Control de registros
4.2.4 Control de los registros		5 Responsabilidad de la dirección
5 Responsabilidad de la dirección	3.1 Responsabilidad de la dirección	5.1 Compromiso de la dirección
5.1 Compromiso de la dirección	3.1 Responsabilidad de la dirección	
5.2 Enfoque al cliente	4.1 Planificación de la gestión del servicio (Planificar)	7 Revisión del SGSI por la dirección
5.4 Planificación	3.1 Responsabilidad de la dirección	7.1 Generalidades
5.5.2 Representante de la dirección		7.2 Datos iniciales de la revisión
5.6 Revisión por la dirección		7.3 Resultados de la revisión
5.6.1 Generalidades		5.2 Gestión de los recursos
5.6.2 Información de entrada para la revisión		5.2.1 Provisión de los recursos
5.6.3 Resultados de la revisión		5.2.2 Concienciación, formación y capacitación
6 Gestión de los recursos	3.3 Competencia, concienciación y formación	
6.1 Provisión de recursos	5 Planificación e implementación de nuevos servicios o de servicios modificados	6 Auditorías internas del SGSI
6.2.2 Competencia, formación y toma de conciencia	4.2 Implementación de la gestión del servicio y provisión de los servicios (Hacer)	
7.3 Diseño y desarrollo	4.3 Monitorización, medición y revisión (Verificar)	8 Mejora del SGSI
7.5 Producción y prestación del servicio	4.3 Monitorización, medición y revisión (Verificar)	8.1 Mejora continua
8.2.2 Auditoría interna	4.4 Mejora continua (Actuar)	
8.2.3 Seguimiento y medición de los procesos	4.4 Mejora continua (Actuar)	
8.5 Mejora		
8.5.1 Mejora continua		

ISO/IEC 9001:2008	ISO/IEC 20000-1:2005	ISO/IEC 27001:2005
8.5.2 Acción correctiva		8.2 Acción correctiva
8.5.3 Acción preventiva		8.3 Acción preventiva

Tabla 1. Sistema de gestión integrado

Durante esta investigación hemos podido observar que, debido al gran número de elementos comunes entre los tres sistemas de gestión, el esfuerzo necesario para implantar el sistema de gestión integrado propuesto, sería mucho menor que el esfuerzo que supondría implantar las tres normas de manera independiente.

Siguiendo la línea de investigación iniciada en este trabajo, los autores esperan como trabajo futuro ampliar el enfoque del sistema de gestión de la calidad proporcionado por la norma ISO 9001 con el modelo propuesto por la reciente norma ISO 9004:2009 *Managing for the sustained success of an organization - A quality management approach* [15]. Esta norma proporciona una orientación para la mejora sistemática y continua del desempeño global de la organización, promoviendo la revisión de su SGC utilizando una autoevaluación según un modelo de madurez por niveles.

Agradecimientos

Esta investigación ha sido posible gracias al soporte ofrecido por los proyectos coordinados TIN2007-67843-TIN2007-67843-C06-04 “*Modelos de simulación basados en ontologías y mejora de procesos para arquitecturas orientadas a servicios*”, SOAQSIm y TIN2010-20057-TIN2010-20057-C03-03: “*Simulación aplicada a la gestión de equipos, procesos y servicios*”, Sim4Gest.

Referencias

- [1] *PAS 99:2006 Specification of common management system requirements as a framework for integration*, British Standards Institution, 2006.
- [2] *ISO Guide 72:2001 Guidelines for the justification and development of management system standards*, ISO, 2001.
- [3] *The integrated use of management system standards*, ISO, 2008.
- [4] *UNE 66177 Sistemas de gestión - Guía para la integración de los sistemas de gestión*, AENOR, 2005.
- [5] Amengual, E. y Mas, A., “A New Method of ISO/IEC 15504 and ISO 9001:2000 Simultaneous Application on Software SMEs”. *Proceedings of the Joint ESA - 3rd*

International SPICE Conference on Process Assessment and Improvement. Marzo de 2003, pp. 87-92, 2003.

[6] Mas, A. y Amengual, E., “A Method for the Implementation of a Quality Management System in Software SMEs”, En: British Computer Society, *Proceedings of the Twelfth International Conference on Software Quality Management. Marzo de 2004, pp. 61-74, 2004.*

[7] Mas, A., Mesquida, A.L., Amengual, E. y Fluxà, B., “Best practices to facilitate ISO/IEC 27000 implementation”. *Proceedings of the 5th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2010). Julio de 2010, pp. 192-198.*

[8] *ISO/IEC TR 15504-7:2008 Information technology - Process assessment - Part 7: Assessment of organizational maturity*, ISO/IEC, 2008.

[9] *ISO 9001:2008 Quality management systems - Requirements*, ISO, 2008.

[10] *ISO/IEC 20000-1:2005 Information technology - Service management - Part 1: Specification*, ISO/IEC, 2005.

[11] *ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements*, ISO/IEC, 2005.

[12] *ISO/IEC 90003:2004 Software engineering - Guidelines for the application of ISO 9001:2000 to computer software*, ISO/IEC, 2004.

[13] *ISO/IEC TR 90005:2008 Systems engineering - Guidelines for the application of ISO 9001 to system life cycle processes*, ISO/IEC, 2008.

[14] *ISO/IEC NP 90006 Information technology - Guidelines for the application of ISO 9001:2000 to IT service management*, ISO/IEC.

[15] *ISO 9004:2009 Managing for the sustained success of an organization - A quality management approach*, ISO/IEC, 2009.