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

Antoni Lluís Mesquida,
Antònia Mas,
Esperança Amengual,
Ignacio Cabestrero

XII Jornadas de Innovación y Calidad del Software (JICS)
Grupo de calidad del software de ATI

Madrid, 25-26 de Noviembre de 2010

Introducción

Implantación de Sistemas de Gestión → **Garantizar la eficacia y fiabilidad de los procesos de negocio**

Elementos comunes que pueden ser gestionados de un modo integrado

ISO 9001:2008 | **ISO/IEC 20000-1:2005** | **ISO/IEC 27001:2005**

Visión global de los sistemas de gestión
Compatibilidad entre sistemas de gestión
Establecer de unos objetivos alineados
Facilitar la toma de decisiones

Integración de los sistemas de gestión

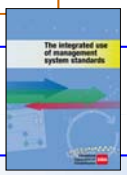
Integración de sistemas de gestión

***PAS 99:2006 Specification of common management system requirements as a framework for integration* (BSI, 2006)**

Especificación de requisitos comunes de los sistemas de gestión. Organizados bajo las 6 categorías de elementos comunes propuestos en:

***ISO Guide 72:2001 Guidelines for the justification and development of management system standards* (ISO, 2001)**

Norma para justificar y desarrollar estándares de sistemas de gestión.



***The integrated use of management system standards* (ISO, 2008)**

Guía para integrar los requisitos de múltiples estándares de sistemas de gestión, ISO o no ISO, con el sistema de gestión de una organización.

UNE 66177:2005 Sistemas de gestión - Guía para la integración de los sistemas de gestión (AENOR, 2005)

Directrices para desarrollar, implantar y evaluar procesos de integración de los sistemas de gestión existentes en una organización.

3

Propósito

Identificar e interpretar los requisitos del SGC de tres normas ISO:

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

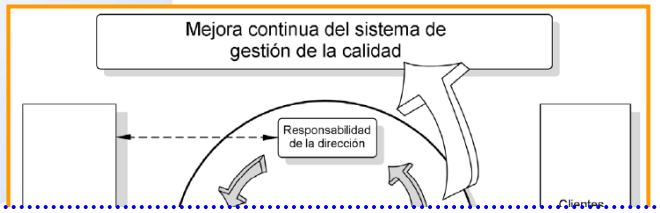
miprosoft

Sistema de Gestión Integrado

4

ISO 9001:2008

Sistemas de gestión de la calidad – Requisitos



Referencia a la integración con otros sistemas de gestión

0.4 Compatibilidad con otros sistemas de gestión

"Esta norma internacional no incluye requisitos específicos de otros sistemas de

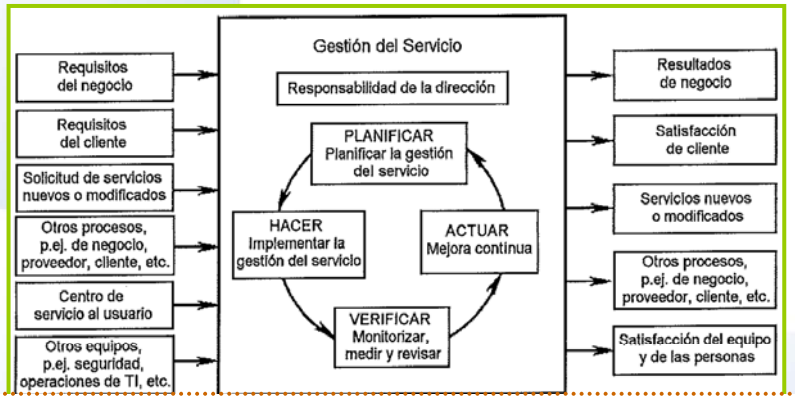
Guías para la aplicación de la norma ISO 9001:

ISO/IEC 90003:2004 ***Software engineering - Guidelines for the application of ISO 9001:2000 to computer software***: 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***: guía para la aplicación de ISO 9001 en el área de sistemas.

ISO 20000-1:2005

Tecnología de la información - Gestión del servicio - Parte 1: Especificaciones

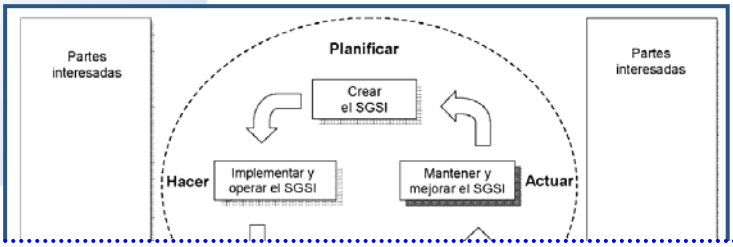


ISO/IEC NP 90006 ***Information technology - Guidelines for the application of ISO 9001:2000 to IT service management***

Nuevo proyecto iniciado en 2008 para desarrollar una guía para la aplicación de la norma ISO 9001 a la gestión de servicios de TI. Actualmente en la misma fase inicial.

ISO 27001:2005

Tecnología de la información - Técnicas de seguridad - Sistemas de Gestión de la Seguridad de la Información (SGSI) - Requisitos



Referencia a la integración con otros sistemas de gestión

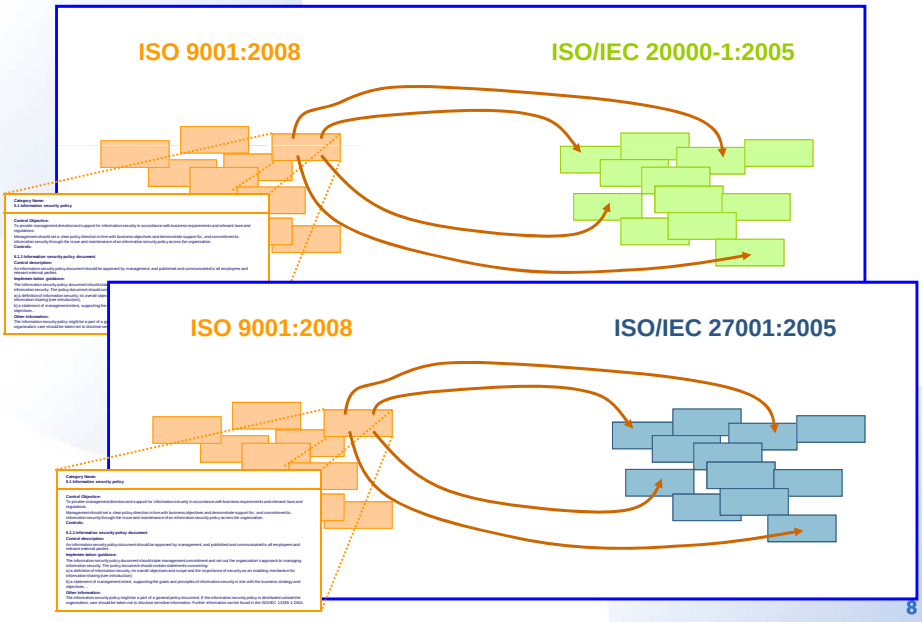
0.3 Compatibilidad con otros sistemas de gestión

"Esta norma internacional sigue las pautas marcadas en las normas ISO

ISO/IEC WD 27013 *Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001*

Nuevo borrador de trabajo para desarrollar una guía para la implantación integrada de las normas ISO/IEC 20000-1 e ISO/IEC 27001. Actualmente en fase de preparación (cierre del periodo de comentarios).

Relaciones entre los sistemas de gestión



Tipos de relaciones: Relación total

1 El requisito de la norma ISO/IEC 20000-1 o ISO/IEC 27001 ya está contemplado por algún requisito de la norma ISO 9001.

ISO/IEC 20000-1:2005

3.2 Requisitos de la documentación

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

ISO/IEC 27001:2005

4.3.1 g) Generalidades (Requisitos documentación)

"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".

ISO 9001:2008

4.2.1.d) Generalidades (Requisitos de la documentación)

"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".

En este caso, al definir el nuevo sistema de gestión integrado, no se deberá añadir ningún aspecto específico al SGC ya implantado.

9

Tipos de relaciones: Relación parcial

2 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.

ISO 9001:2008

5.1 Compromiso de la dirección

Aspectos propios de la gestión de servicios de TI

Aspectos propios de la gestión de la seguridad de la información

ISO/IEC 20000-1:2005

3.1 Responsabilidad de la dirección

Apartados e), f) y g)

ISO/IEC 27001:2005

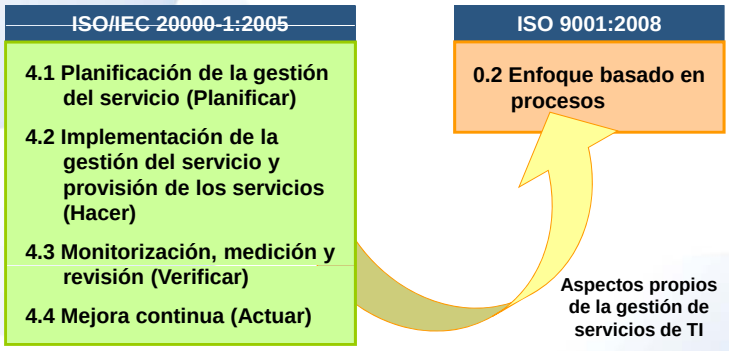
3.1 Compromiso de la dirección

Apartado c)

10

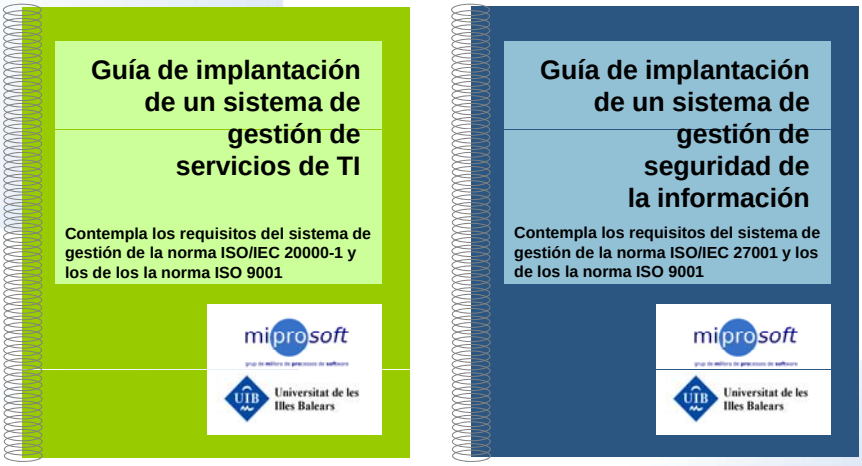
Tipos de relaciones: Inexistencia de relación

3 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



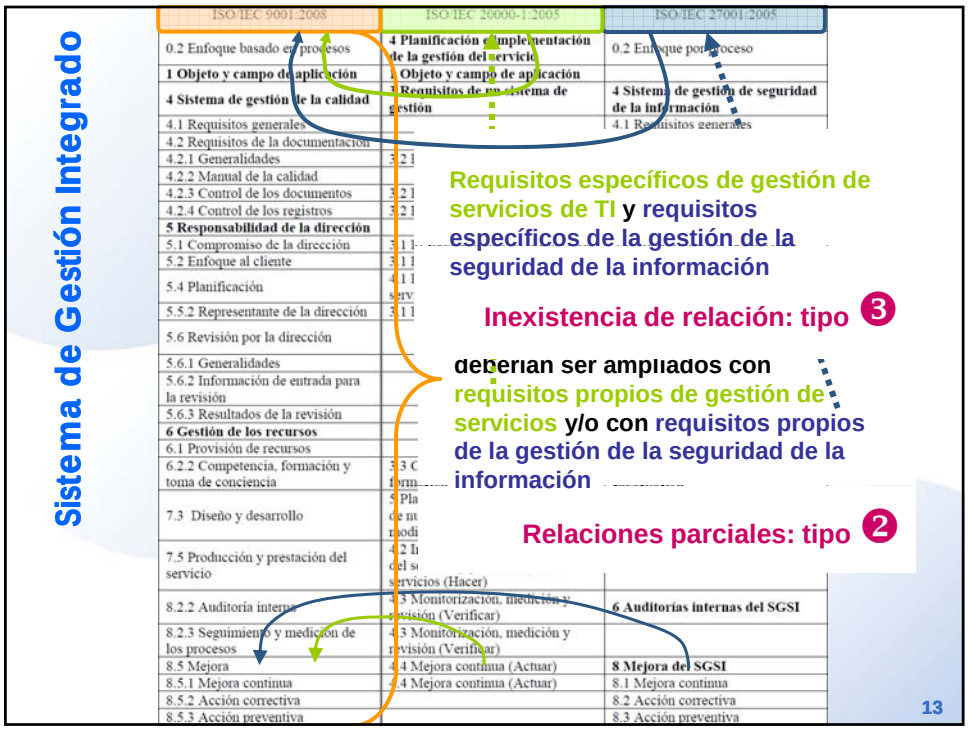
11

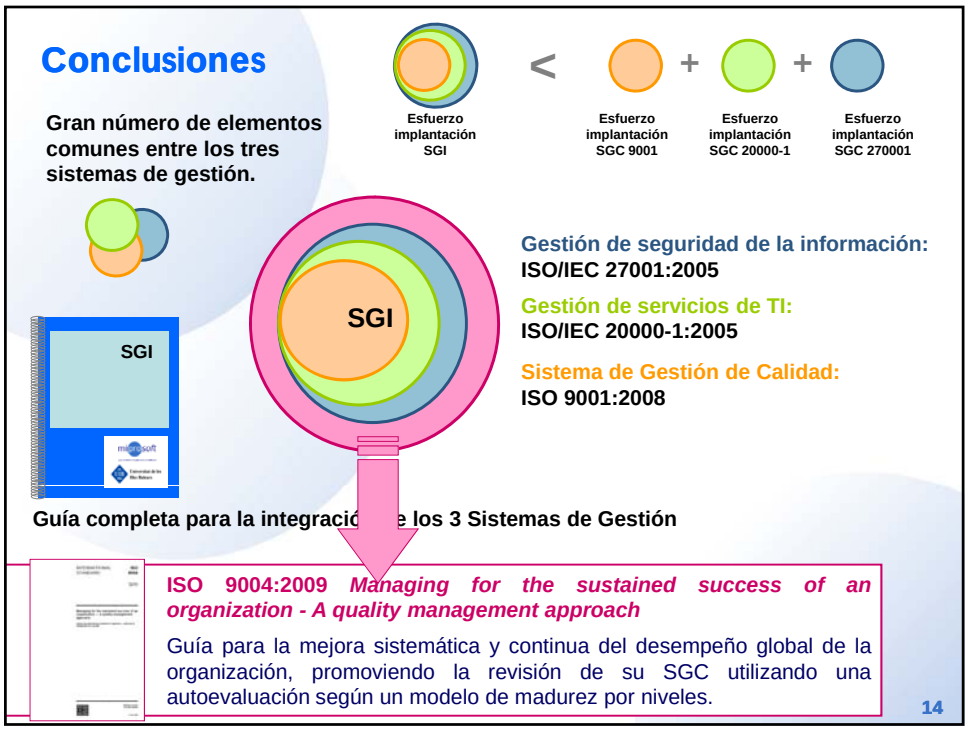
Elaboración de guías de aplicación



Guardan el mismo formato que las guías de aplicación de ISO 9001: ISO/IEC 90003, ISO/IEC TR 90005, ISO/IEC NP 90006

12


Sistema de Gestión Integrado
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 la calidad
4 Requisitos de un sistema de gestión
4 Sistema de gestión de seguridad de la información
4.1 Requisitos generales
4.1 Requisitos generales
4.2 Requisitos de la documentación
4.2.1 Generalidades
4.2.2 Manual de la calidad
4.2.3 Control de los documentos
4.2.4 Control de los registros
5 Responsabilidad de la dirección
5.1 Compromiso de la dirección
5.2 Enfoque al cliente
5.4 Planificación
5.5.2 Representante de la dirección
5.6 Revisión por la dirección
5.6.1 Generalidades
5.6.2 Información de entrada para la revisión
5.6.3 Resultados de la revisión
6 Gestión de los recursos
6.1 Provisión de recursos
6.2.2 Competencia, formación y toma de conciencia
7.3 Diseño y desarrollo
7.5 Producción y prestación del servicio
8.2.2 Auditoría interna
6 Auditorías internas del SGSI
8.2.3 Seguimiento y medición de los procesos
8.5 Mejora
8.5.1 Mejora continua
8.5.2 Acción correctiva
8.5.3 Acción preventiva
8 Mejora del SGSI
8.1 Mejora continua
8.2 Acción correctiva
8.3 Acción preventiva
Requisitos específicos de gestión de servicios de TI y requisitos específicos de la gestión de la seguridad de la información
Inexistencia de relación: tipo 3
deberían ser ampliados con requisitos propios de gestión de servicios y/o con requisitos propios de la gestión de la seguridad de la información
Relaciones parciales: tipo 2
13


Conclusiones
Gran número de elementos comunes entre los tres sistemas de gestión.
Esfuerzo implantación SGI
<
Esfuerzo implantación SGC 9001
+
Esfuerzo implantación SGC 20000-1
+
Esfuerzo implantación SGC 270001
SGI
SGI
Gestión de seguridad de la información:
ISO/IEC 27001:2005
Gestión de servicios de TI:
ISO/IEC 20000-1:2005
Sistema de Gestión de Calidad:
ISO 9001:2008
Guía completa para la integración de los 3 Sistemas de Gestión
ISO 9004:2009 Managing for the sustained success of an organization - A quality management approach
Guía 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.
14


miprosoft
grup de millora de processos de software
UIB
Universitat de les Illes Balears
Antoni Lluís Mesquida
antoni.mesquida@uib.es
+34 971 17 29 91
+34 971 17 30 03
http://miprosoft.uib.es
miprosoft@uib.es
XII Jornadas de Innovación y Calidad del Software (JICS)
Grupo de calidad del software de ATI
Madrid, 25-26 de Noviembre de 2010
15