ISO 27001:2013 Todo lo que usted necesita saber acerca de los nuevos cambios

Cambios respecto a ISO 27001:2005

William Hálaby CISSP, PMP
(ISC)² Capitulo Colombia Board Member

Si usted asistió a esta charla agradecemos diligenciar la siguiente encuesta

http://goo.gl/rcNxUc

Objetivos de la Sesión

- Entender las diferencias claves
- Entender los nuevos requerimientos de la norma
- Entender los controles adicionados y los controles eliminados

BIG PICTURE

- La versión 2013 es una evolución, NO una revolución.
- Mucho del texto de la versión 2005 y sus requerimientos (debes) permanecen, pero algunos se han movido para ajustarse a las nuevas secciones.
- No es una migración mayor como lo fue de BS 7799 a ISO 17799.

+ 80 %

Se mantiene

Agenda

- **ISO 27000**
  - La familia ISO 27000
  - ¿Qué es ISO 27001:2013?
  - ¿Qué es un SGSI?
  - Por que seleccionar ISO 27001?

- **Principales cambios ISO 27001: 2013 Vs. ISO 27001:2005**
  - El ciclo PHVA
  - Los 5 principales cambios
  - Otros Cambios relevantes
  - Estructura del Documento
  - **Sección 3** Términos y definiciones
  - **Sección 4** Contexto de la organización
  - **Sección 5** Liderazgo
  - **Sección 6** Planeación
  - **Sección 7** Soporte
  - **Sección 8** Operaciones
  - **Sección 9** Evaluación del desempeño
  - **Sección 10** Mejora
  - **Anexo A** Cambios en los Controles
- **Tiempo de Transición**
- **Conclusiones**

Agenda

- **ISO 27000**
  - La familia ISO 27000
  - ¿Qué es ISO 27001:2013?
  - ¿Qué es un SGSI?
  - Por que seleccionar ISO 27001?

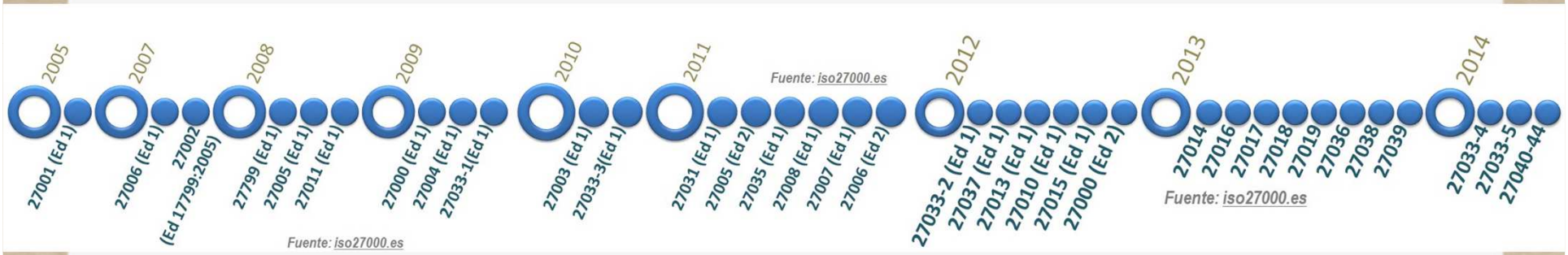
- **Principales cambios ISO 27001: 2013 Vs. ISO 27001:2005**
  - El ciclo PHVA
  - Los 5 principales cambios
  - Otros Cambios relevantes
  - Estructura del Documento
  - **Sección 3** Términos y definiciones
  - **Sección 4** Contexto de la organización
  - **Sección 5** Liderazgo
  - **Sección 6** Planeación
  - **Sección 7** Soporte
  - **Sección 8** Operaciones
  - **Sección 9** Evaluación del desempeño
  - **Sección 10** Mejora
  - **Anexo A** Cambios en los Controles
- **Tiempo de Transición**
- **Conclusiones**

La familia ISO 27000

More than 30 “ISO27k” standards are planned, more than half of which have been published and are on sale from various official ISO/IEC

- ISO/IEC 27000:2014 - provides an overview/introduction to the ISO27k standards plus a glossary for the specialist vocabulary.
- **ISO/IEC 27001:2013 is the Information Security Management System (ISMS) requirements standard, a formal specification for an ISMS.**
- ISO/IEC 27002:2013 is the code of practice for information security controls describing good practice information security control objectives and controls.
- ISO/IEC 27003:2010 provides guidance on implementing ISO/IEC 27001.
- ISO/IEC 27004:2009 covers information security management measurement (metrics).
- ISO/IEC 27005:2011 covers information security risk management.
- ISO/IEC 27006:2011 is a guide to the certification or registration process for accredited ISMS certification or registration bodies.
- ISO/IEC 27007:2011 is a guide to auditing Information Security Management Systems.
- ISO/IEC TR 27008:2011 concerns the auditing of technical security controls.
- ISO/IEC 27009 will advise those producing standards for sector-specific applications of ISO27k.
- ISO/IEC 27010:2012 provides guidance on information security management for
- inter-sector and inter-organisational communications.
- ISO/IEC 27011:2008 is the information security management guideline for telecommunications organizations (dual-numbered as ITU X.1051).
- ISO/IEC 27013:2012 provides guidance on the integrated/joint implementation of both ISO/IEC 27001 (ISMS) and ISO/IEC 20000-1 (service management/ITIL).
- ISO/IEC 27014:2013 offers guidance on the governance of information security.
- ISO/IEC TR 27015:2012 provides information security management guidelines for financial services.
- ISO/IEC TR 27016:2014 covers the economics of information security management.
- ISO/IEC 27017 will cover information security controls for cloud computing.
- ISO/IEC 27018 will cover privacy in public cloud computing services.
- ISO/IEC TR 27019:2013 covers information security for process control in the energy industry.
- ISO/IEC 27031:2011 is an ICT-focused standard on business continuity.
- ISO/IEC 27032:2012 covers cybersecurity.
- ISO/IEC 27033:2009+ is replacing the multi-part ISO/IEC 18028 standard on IT network security (parts 1, 2, 3, 4 & 5 are published, part 6 is in preparation).
- ISO/IEC 27034:2011+ is providing guidelines for application security (part 1 was released in 2011, the others are in preparation).
- ISO/IEC 27035:2011 on information security incident management.
- ISO/IEC 27036:2013+ is a multi-part security guideline for supplier relationships including the relationship management aspects of cloud computing (only part 3 has been published so far, but part 1 is in the process of being published).
- ISO/IEC 27037:2012 covers identifying, gathering and preserving digital evidence.
- ISO/IEC 27038 will be a specification for digital redaction.
- ISO/IEC 27039 will concern intrusion detection and prevention systems.
- ISO/IEC 27040 will offer guidance on storage security.
- ISO/IEC 27041 will offer guidance on assurance for digital evidence investigation methods.
- ISO/IEC 27042 will offer guidance on analysis and interpretation of digital evidence.
- ISO/IEC 27043 will offer guidance on digital evidence investigation principles and processes.
- ISO/IEC 27044 will offer guidance on SIEM (Security Incident and Event Management).
- ISO/IEC 27050 will offer guidance on electronic discovery.
- ISO 27799:2008 provides health sector specific ISMS implementation guidance based on ISO/IEC 27002:2005.

La familia ISO 27000



Qué es ISO 27001:2013?

ISO 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

Qué es ISO 27001:2013?

¿Para quién es significativo?

ISO 27001 es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo. La norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sanidad, sector público y tecnología de la información (TI).

ISO 27001 también es muy eficaz para organizaciones que gestionan la información por encargo de otros, por ejemplo, empresas de subcontratación de TI. Puede utilizarse para garantizar a los clientes que su información está protegida

Qué es ISO 27001:2013?

Timeline

¿Qué es un SGSI?

El concepto clave de un SGSI es el **diseño, implantación y mantenimiento de un conjunto de procesos** para gestionar eficientemente la accesibilidad de la información, buscando **asegurar la confidencialidad, integridad y disponibilidad** de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un **SGSI** debe seguir siendo eficiente durante un largo tiempo **adaptándose** a los cambios internos de la organización así como los externos del entorno

¿Qué es un SGSI?

UN SGSI, ¿QUÉ BENEFICIOS APORTA?

- Un **análisis de riesgos**, identificando amenazas, vulnerabilidades e impactos en la actividad empresarial.
- Una **mejora continua** en la gestión de la seguridad.
- Una garantía de continuidad y **disponibilidad del negocio**.
- **Reducción de los costos** vinculados a los incidentes.
- El **incremento de los niveles de confianza** de clientes y partners.
- El aumento del valor comercial y **mejora de la imagen** de la organización.
- Voluntad de **cumplir con la legislación vigente** de protección de datos de carácter personal, servicios de la sociedad e la información, comercio electrónico, propiedad intelectual y en general, aquella relacionada con la seguridad de la información.

¿Por que seleccionar ISO 27001?

¿Por qué necesitamos un SGSI?

Las organizaciones y sus sistemas y redes de información están expuestos a las **AMENAZAS** de seguridad tales como el fraude, espionaje, incendios, inundaciones y el sabotaje proveniente de una amplia gama de fuentes. El creciente número de fallos de seguridad ha llevado a una mayor preocupación por la seguridad de la información entre las organizaciones de todo el mundo.

LOGRAR AVANCES EN SEGURIDAD DE LA INFORMACIÓN es un gran desafío para la organización ya que **NO PUEDE LOGRARSE SOLO A TRAVÉS DE MEDIOS TECNOLÓGICOS** y nunca debe ser implementado de una manera que no este alineado con el enfoque de la organización a los riesgos o de forma tal que se creen dificultades para sus operaciones comerciales.

Por lo tanto hay una necesidad de mirar a seguridad de la información desde una **PERSPECTIVA HOLÍSTICA** lo que hace necesario tener una metodología de gestión de seguridad de la información para proteger la información de manera sistemática. S aquí donde el SGSI entra en juego.

Agenda

- **La familia ISO 27000**
  - ¿Qué es ISO 27001:2013?
  - ¿Qué es un SGSI?
  - Por que seleccionar ISO 27001?

- **Principales cambios ISO 27001: 2013 Vs. ISO 27001:2005**
  - El ciclo PHVA
  - Los 5 principales cambios
  - Otros Cambios relevantes
  - Estructura del Documento
  - **Sección 3** Términos y definiciones
  - **Sección 4** Contexto de la organización
  - **Sección 5** Liderazgo
  - **Sección 6** Planeación
  - **Sección 7** Soporte
  - **Sección 8** Operaciones
  - **Sección 9** Evaluación del desempeño
  - **Sección 10** Mejora
  - **Anexo A** Cambios en los Controles
- **Tiempo de Transición**
- **Conclusiones**

Cambios: marco central

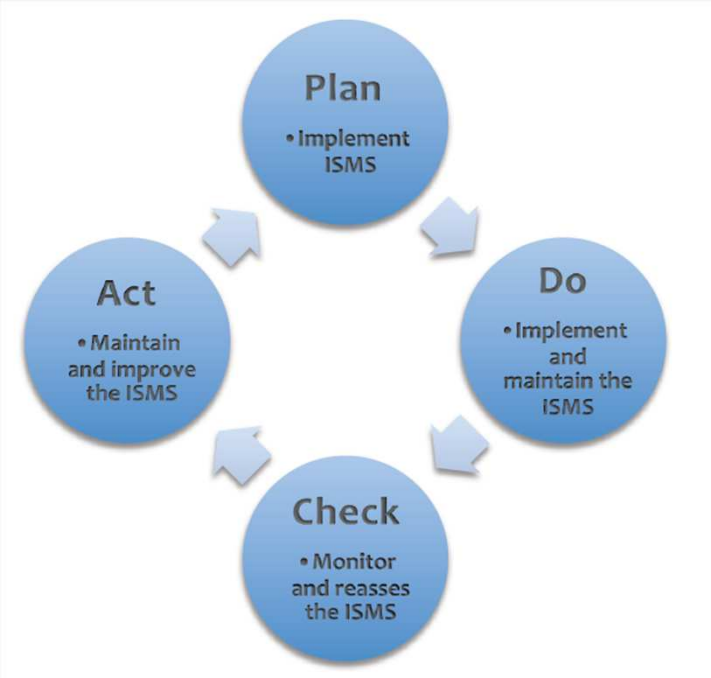
Para tener en cuenta sobre los cambios:

- La norma ahora es menos descriptiva y prescriptiva
- Da mayores libertades en la implementación
- Propone un periodo de transición para las organizaciones ya certificadas

Cambios: El ciclo PHVA

El modelo **PHVA** no se referencia explícitamente en la nueva norma, sin embargo, está allí como un modelo de mejora subyacente pero ..

- Los diferentes elementos de **PHVA** se distribuyen ahora dentro de la estructura común de la norma.
- Por ejemplo **ACTUAR** se puede interpretar como la cláusula **10 MEJORA**



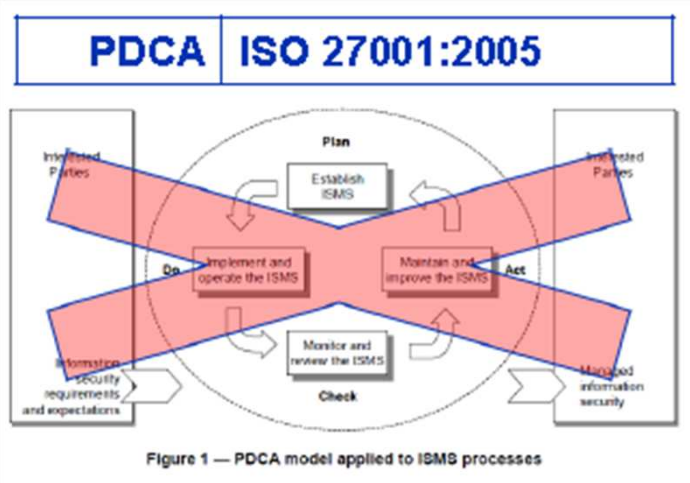
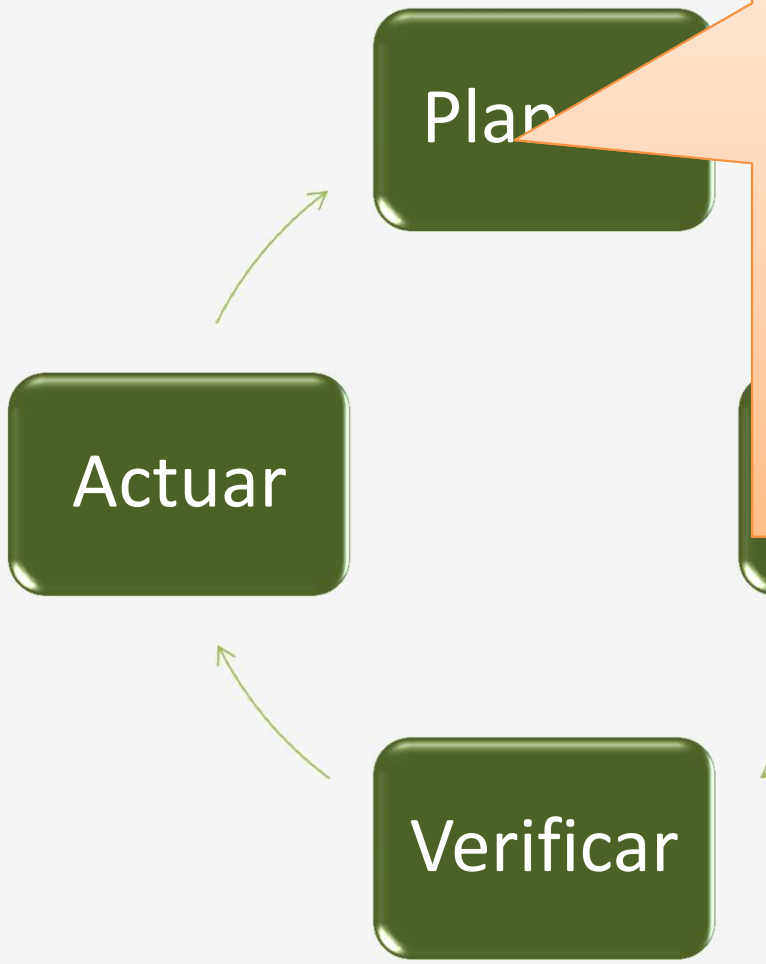


Figure 1 — PDCA model applied to ISMS processes

El ciclo PHVA

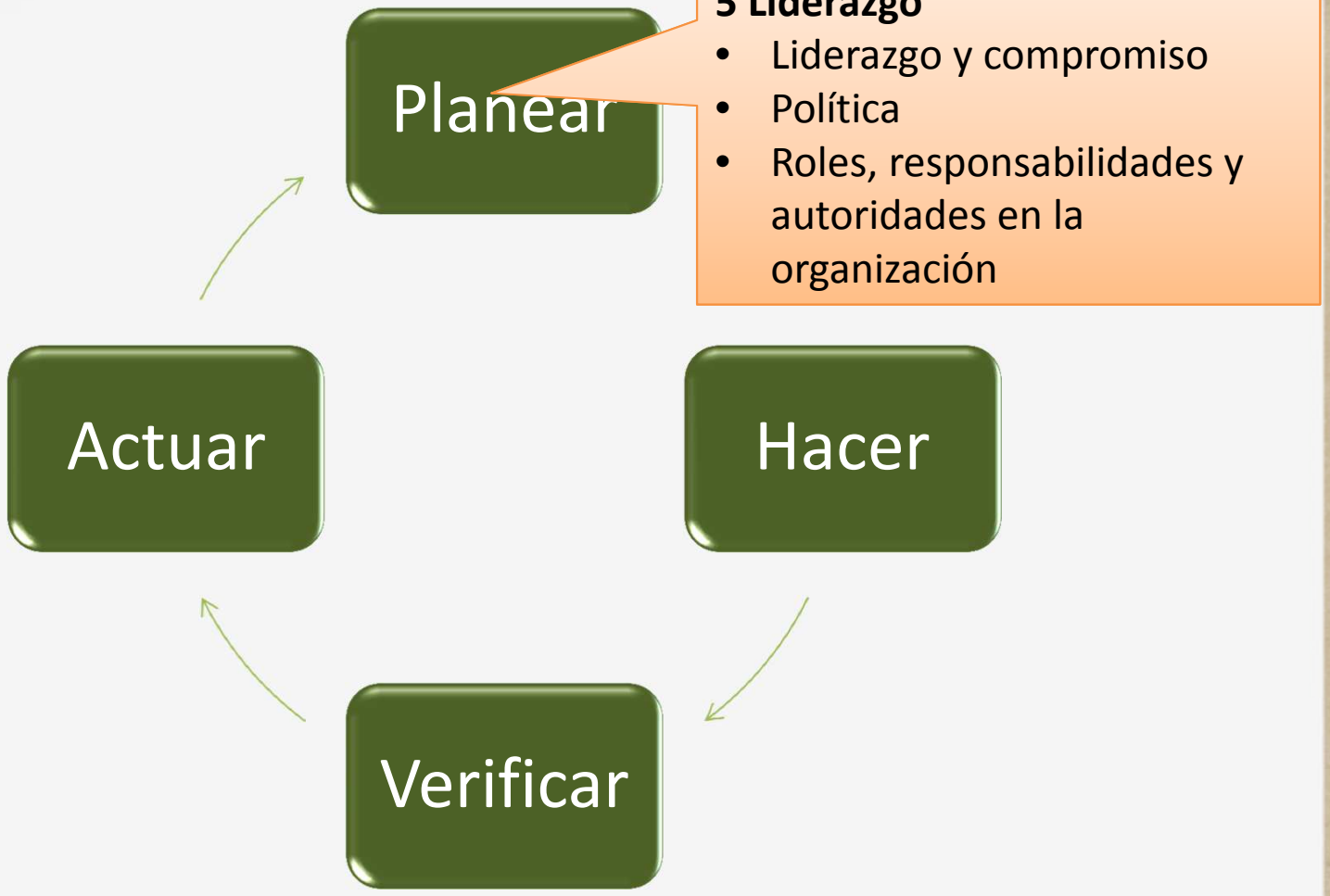
El ciclo PHVA



4 Contexto de la organización

- Conocimiento de la organización y su contexto
- Comprensión de las necesidades y expectativas de las partes interesadas
- Determinación del alcance del SGSI
- SGSI

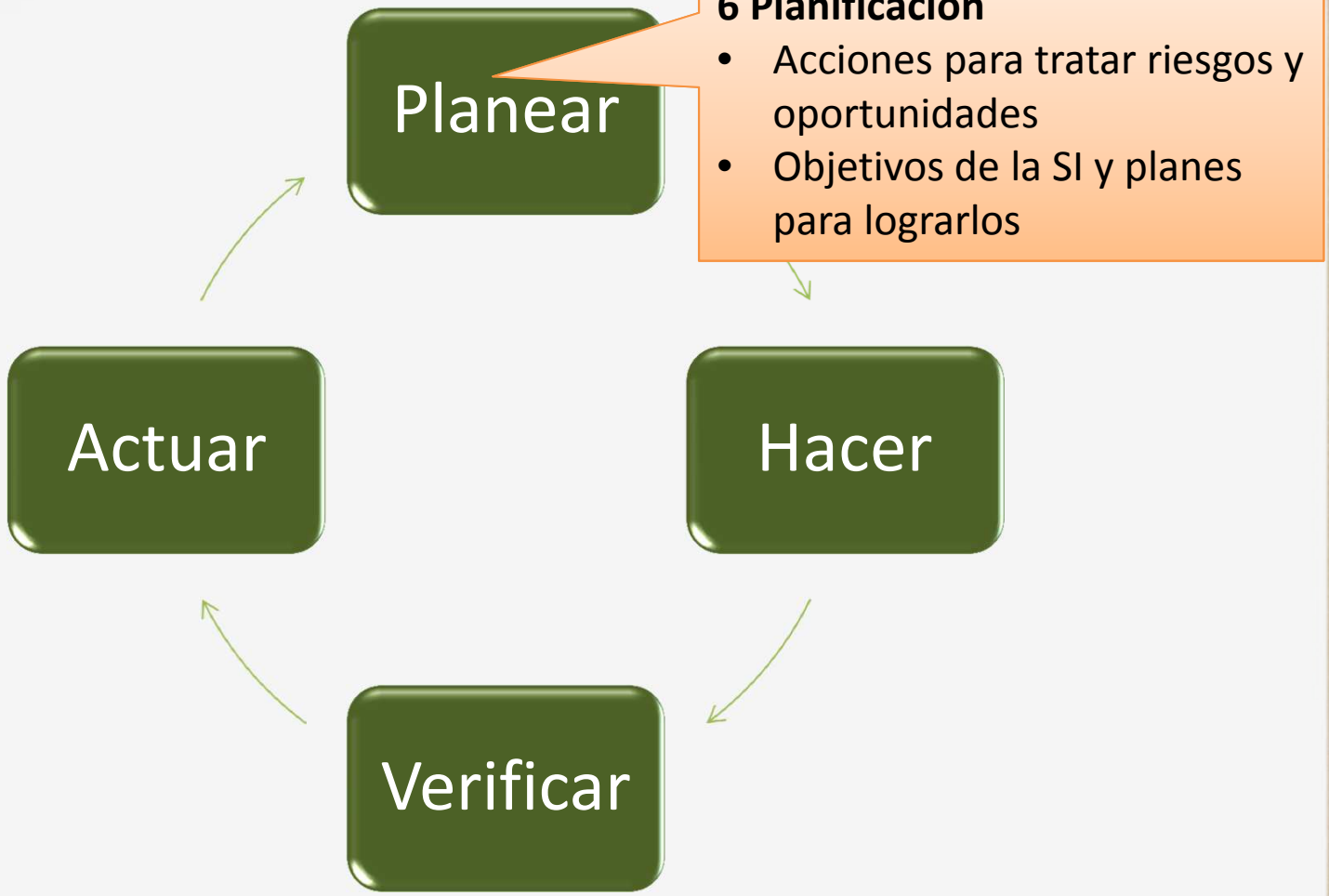
El ciclo PHVA



5 Liderazgo

- Liderazgo y compromiso
- Política
- Roles, responsabilidades y autoridades en la organización

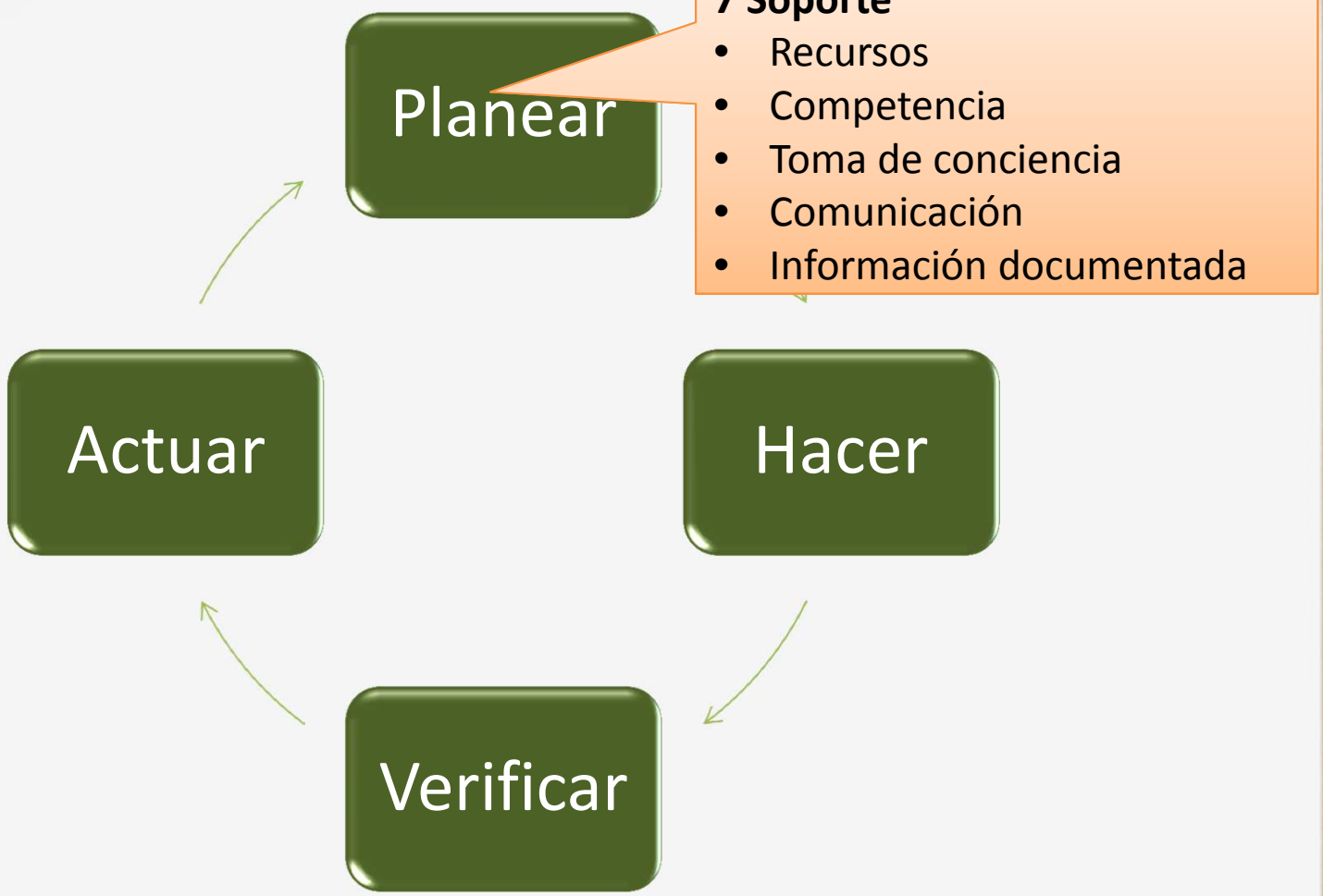
El ciclo PHVA



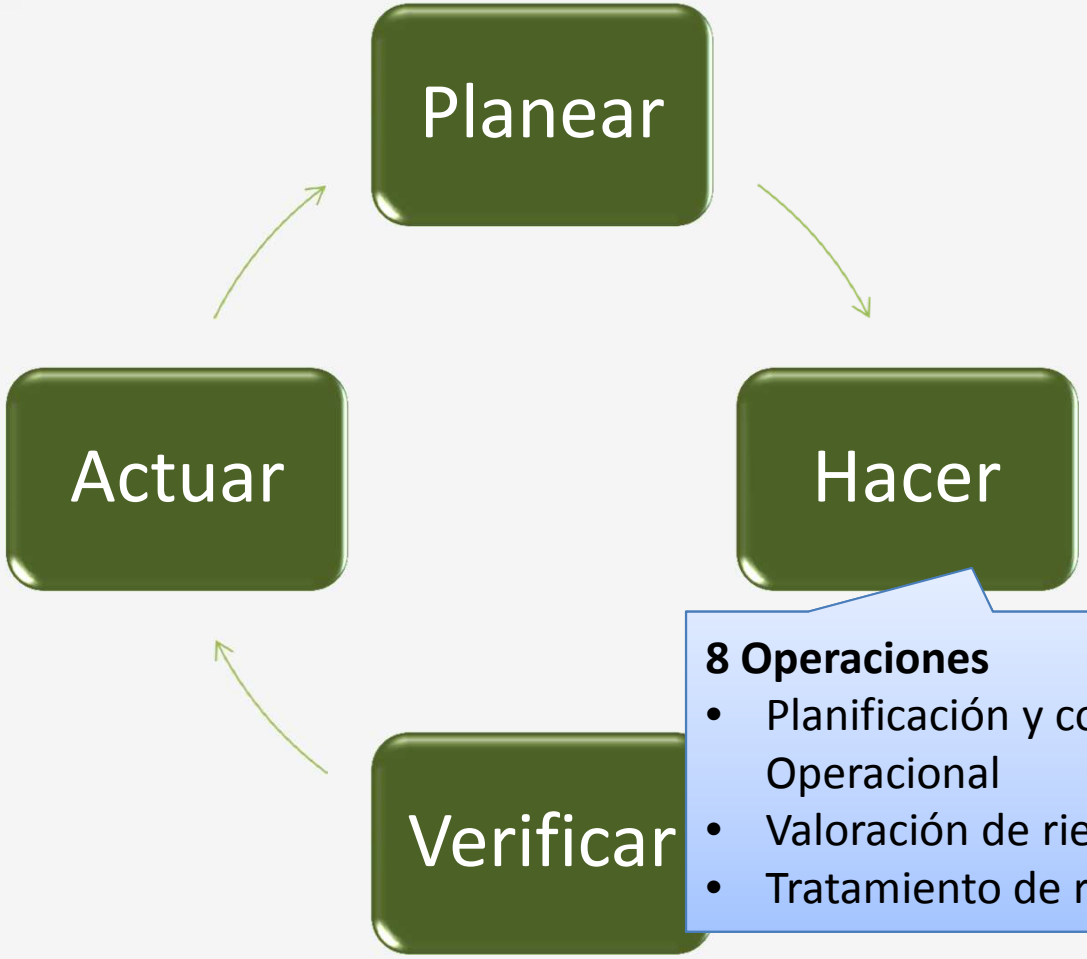
6 Planificación

- Acciones para tratar riesgos y oportunidades
- Objetivos de la SI y planes para lograrlos

El ciclo PHVA



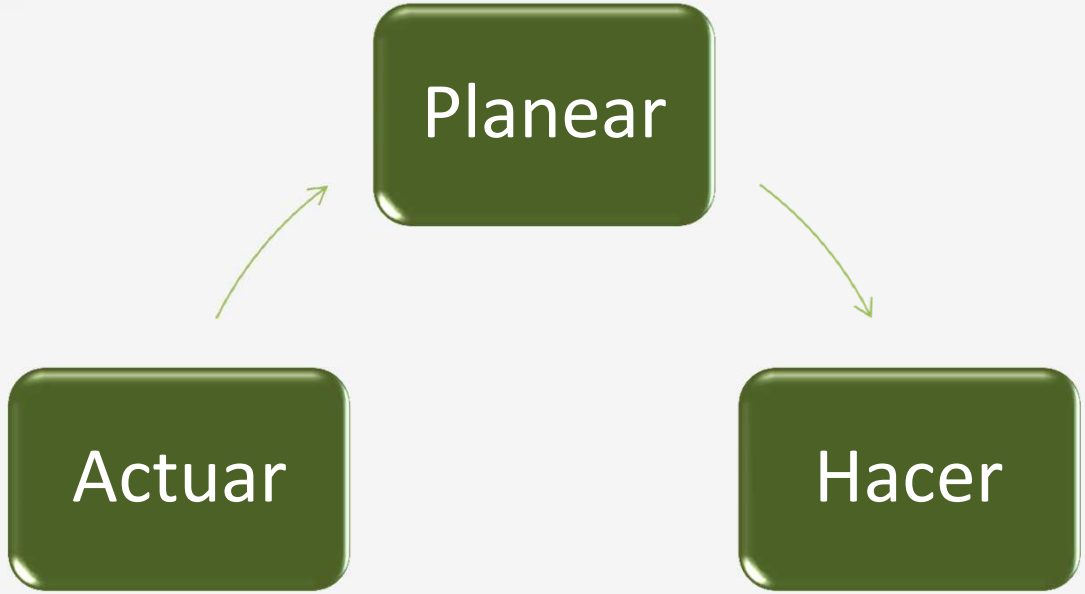
El ciclo PHVA



8 Operaciones

- Planificación y control Operacional
- Valoración de riesgos de la SI
- Tratamiento de riesgos de la SI

El ciclo PHVA

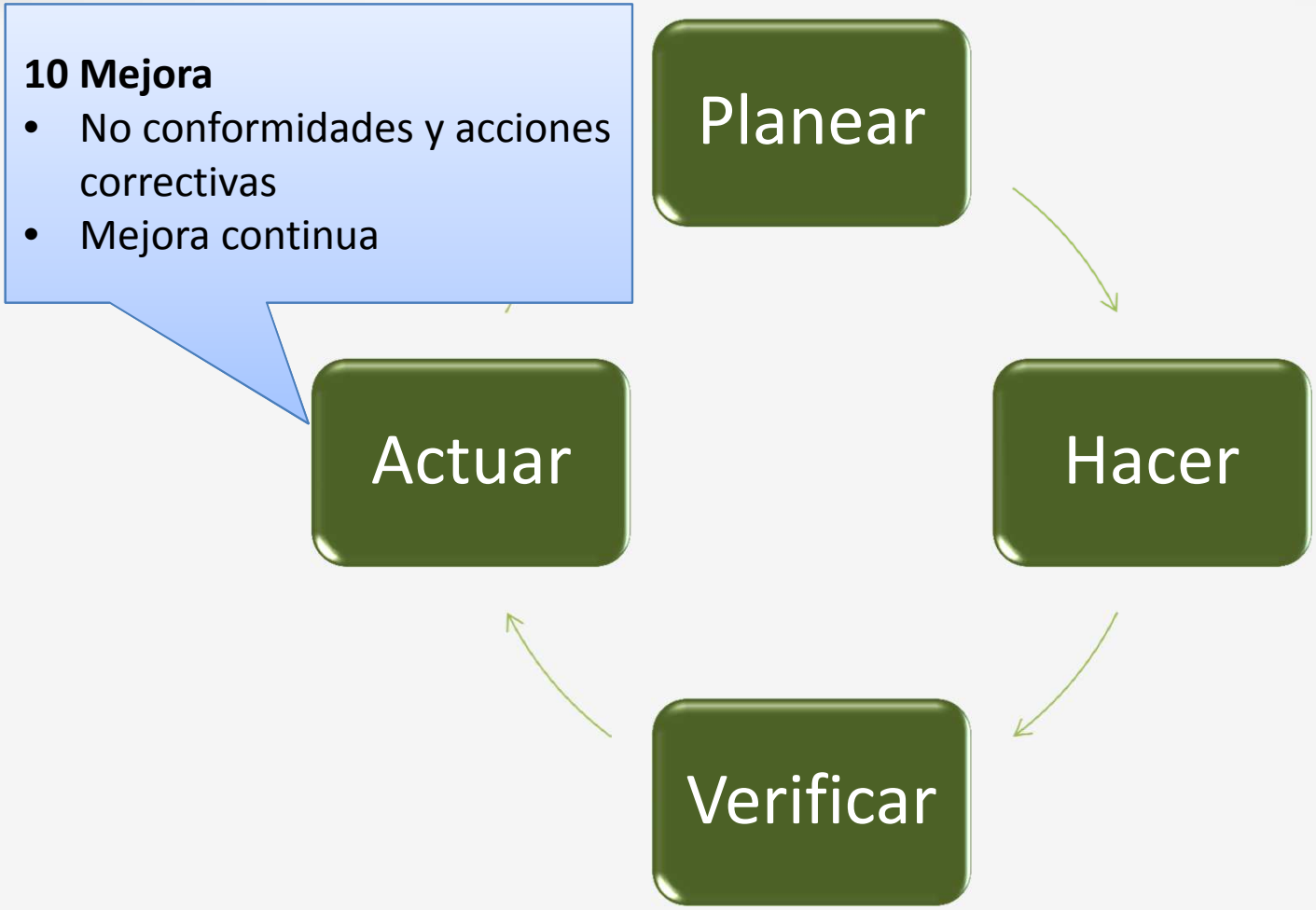


9. **Evaluación del Desempeño**
- Seguimiento, medición, análisis y evaluación
- Auditoria Interna
- Revisión por la dirección

El ciclo PHVA

10 Mejora

- No conformidades y acciones correctivas
- Mejora continua



Cambios: 5 Diferencias fundamentales

- La nueva norma esta escrita de conformidad con el Anexo SL
- lSO 27002 ya no es una normativa de referencia
- Las definiciones fueron removidas y reubicadas en la norma ISO 27000
- Cambios en la terminología: por ejemplo, “Política de SI” es usada en lugar de “Política del SGSI”
- Los requisitos para el compromiso de la Alta Dirección fueron revisados y ahora están presentes en la Cláusula de Liderazgo

Cambios: 4 diferencias adicionales

- Las acciones preventivas se reemplazaron por "acciones para abordar los riesgos y oportunidades
- Los requisitos de evaluación de riesgos son ahora más generales y se alinean con la norma ISO 31000
- Los requisitos de la declaración de aplicabilidad (SoA) son similares pero se da mayor claridad en la determinación de los controles del proceso de tratamiento de riesgos
- Mayor énfasis en el establecimiento de los objetivos, el seguimiento del desempeño y métricas

Cambios: Nueva Estructura documental

- Desarrollado usando el Anexo SL
  - Para estandarizar a los redactores de normas
  - Proporciona texto estándar bien conocido entre los Sistemas de gestión.
- Nueva estructura para convertirse en común para todas las normas de Sistemas de Gestión.
- Se desea estandarizar terminología y requisitos fundamentales para sistemas de gestión

Cambios: Nueva Estructura documental

High Level Structure – Main clauses

Introduction

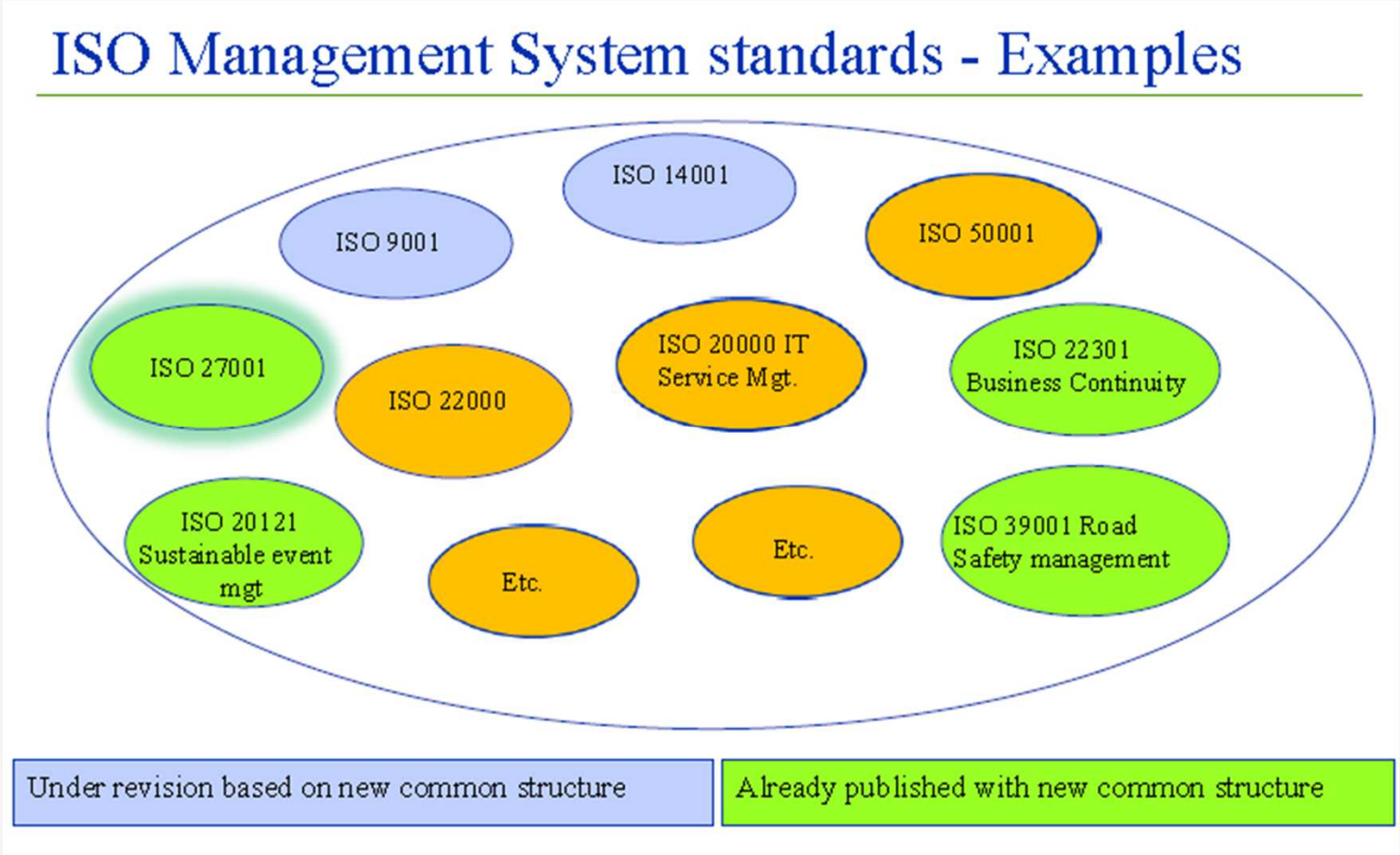
1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

ISO ANNEX SL

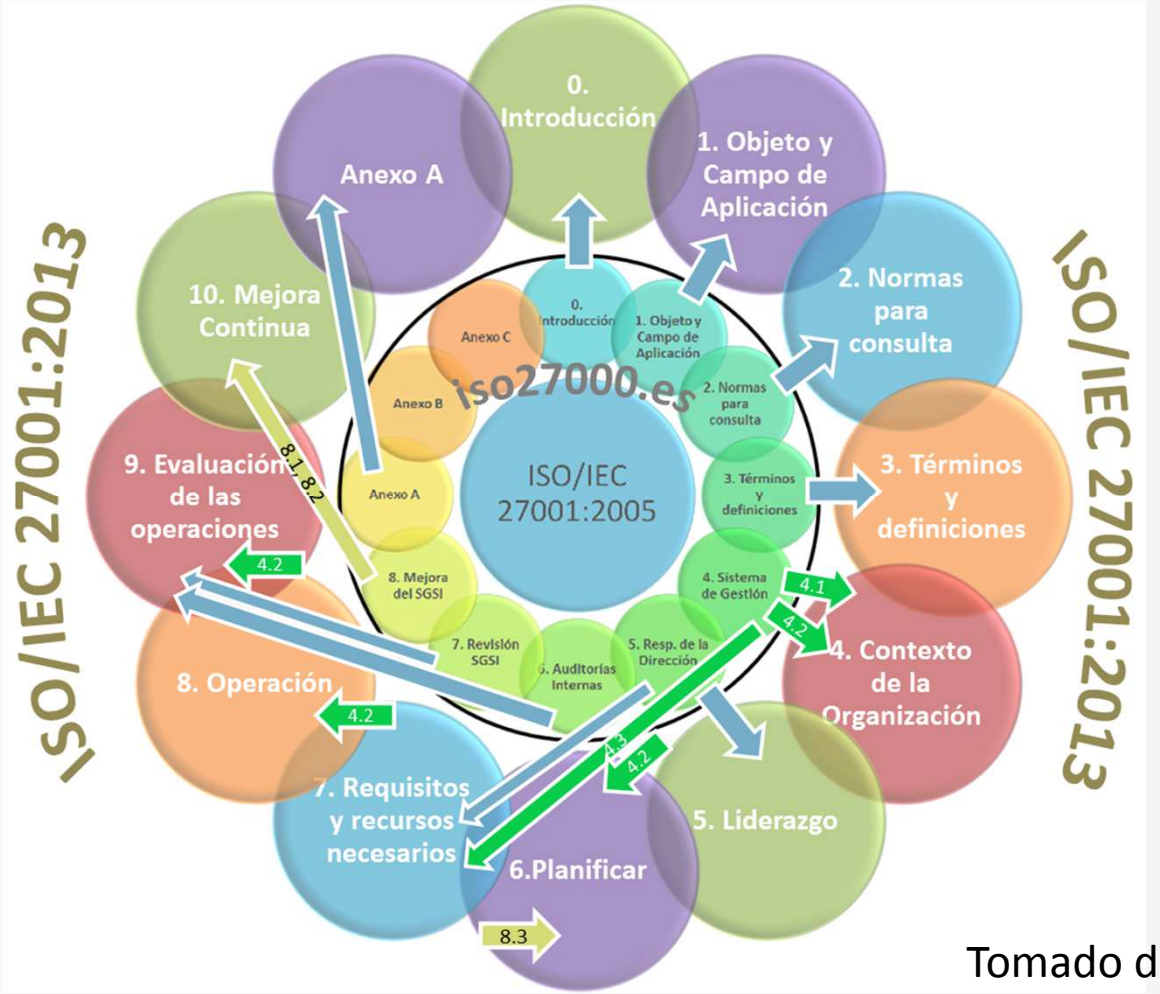
Identical core text For clauses 4-10 there are also sub-clauses, and identical core text (requirements) is provided (refer Appendix 3 in Annex SL).

The common framework is defined in Appendix 3 of ISO/IEC Directives, Part 1 Annex SL (pp 143-152)

Cambios: Nueva Estructura documental



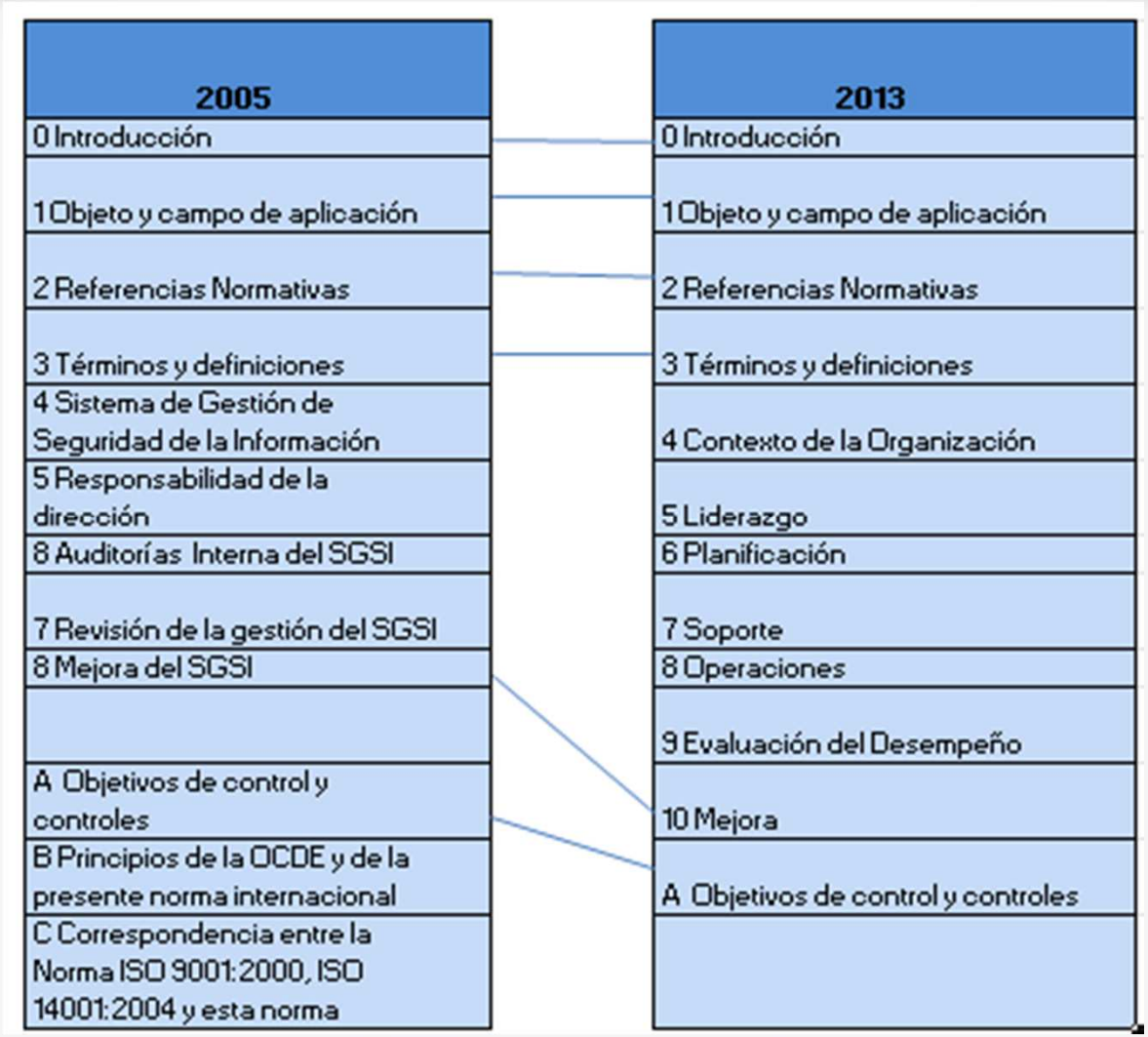
Principales Diferencias



Tomado de iso27000.es

Principales Diferencias

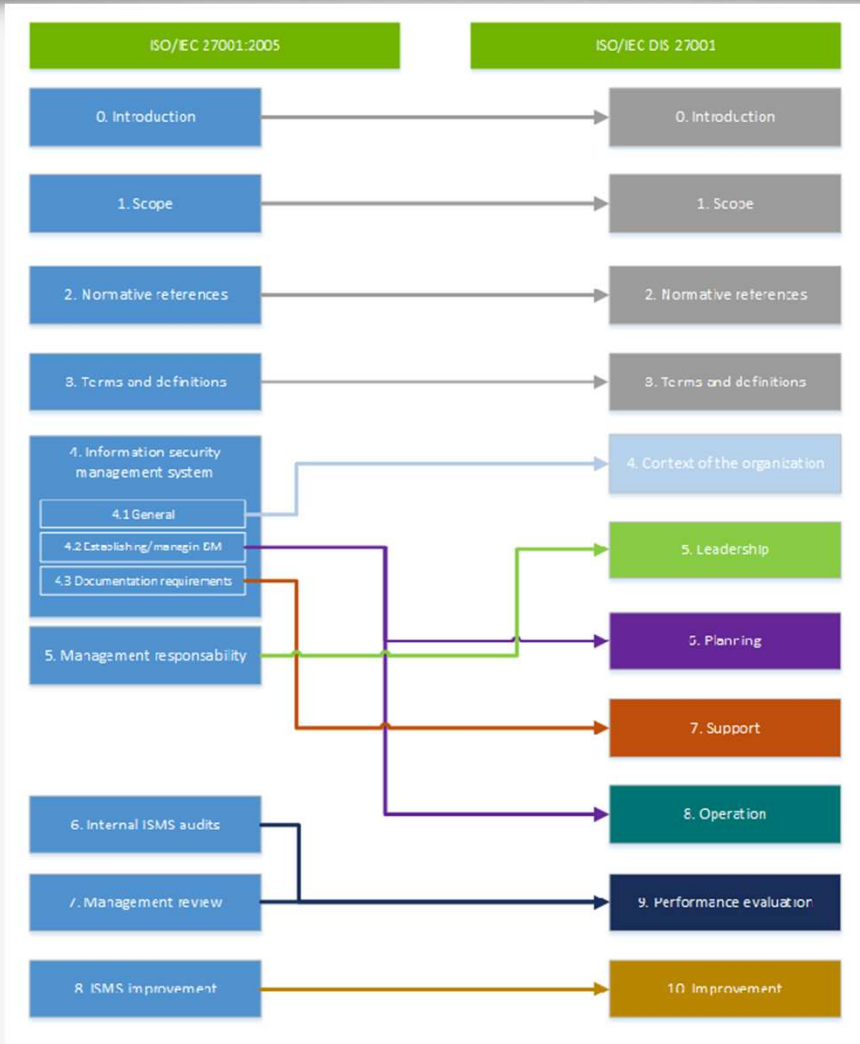
Tabla de contenido



2005	2013
0 Introducción	0 Introducción
1 Objeto y campo de aplicación	1 Objeto y campo de aplicación
2 Referencias Normativas	2 Referencias Normativas
3 Términos y definiciones	3 Términos y definiciones
4 Sistema de Gestión de Seguridad de la Información	4 Contexto de la Organización
5 Responsabilidad de la dirección	5 Liderazgo
8 Auditorías Interna del SGSI	6 Planificación
7 Revisión de la gestión del SGSI	7 Soporte
8 Mejora del SGSI	8 Operaciones
	9 Evaluación del Desempeño
A Objetivos de control y controles	10 Mejora
B Principios de la OCDE y de la presente norma internacional	A Objetivos de control y controles
C Correspondencia entre la Norma ISO 9001:2000, ISO 14001:2004 y esta norma	

Principales Diferencias

Tabla de contenido



Principales Diferencias

- **3 Términos y definiciones**
  - Todas las definiciones fueron removidas
  - Las definiciones relevantes fueron movidas a ISO27000
  - Promueve la consistencia de términos y definiciones en toda la familia ISO270XX

Principales Diferencias

4 Contexto de la Organización

- Relacionados con el contexto de la Organización - determinar los problemas externos e internos
- Requisito claros para considerar las partes interesadas
- El contexto determina la política de SI, los objetivos y la forma en que la organización tendrá en cuenta el riesgo y el efecto del riesgo en su negocio
- Requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios y las obligaciones contractuales

Principales Diferencias

Contexto Externo

- social, cultural, político, jurídico, normativo, financiero, tecnológico, económico, natural y ambiente competitivo (internacional, nacional, regional o local)

- Factores clave y tendencias que tienen impacto en los objetivos de la organización

- Relaciones percepciones y valores de los actores externos

Principales Diferencias

Contexto Interno

- Cultura de la organización
- Estructura de gobierno, roles y responsabilidades
- Políticas, objetivos y las estrategias en marcha para alcanzarlos
- Capitales en términos de recursos y de conocimientos (procesos ej., Dinero, tiempo, gente, sistemas y tecnologías)
- sistemas de información Informales y formales y flujos de procesos para toma de decisiones
- Normas adoptadas, Guias y modelos
- Forma y alcance de las relaciones contractuales
- Relaciones, percepciones y valores de los actores internos

Principales Diferencias

5 Liderazgo

- Resume los requisitos específicos para el papel de la alta dirección en el SGSI
- Delinea formas específicas para demostrar la gestión y su compromiso con el sistema. Ejemplos incluyen:
  - asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles;
  - comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información;
- Aunque se renombro la Política del SGSI, los requisitos de política originales permanecen
- La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.

Principales Diferencias

6 Planificación

- Establecimiento de objetivos y principios rectores para el SGSI
- Al planificar el SGSI. el contexto de la organización debe ser tenido en cuenta a través de la consideración de los riesgos y oportunidades
- Los objetivos de la organización deben estar claramente definidos junto con los planes para alcanzarlos
- Requisitos de evaluación de riesgos más general y alineados con la norma ISO 31000
- Requisitos de la declaración de aplicabilidad (SoA) prácticamente sin cambios.

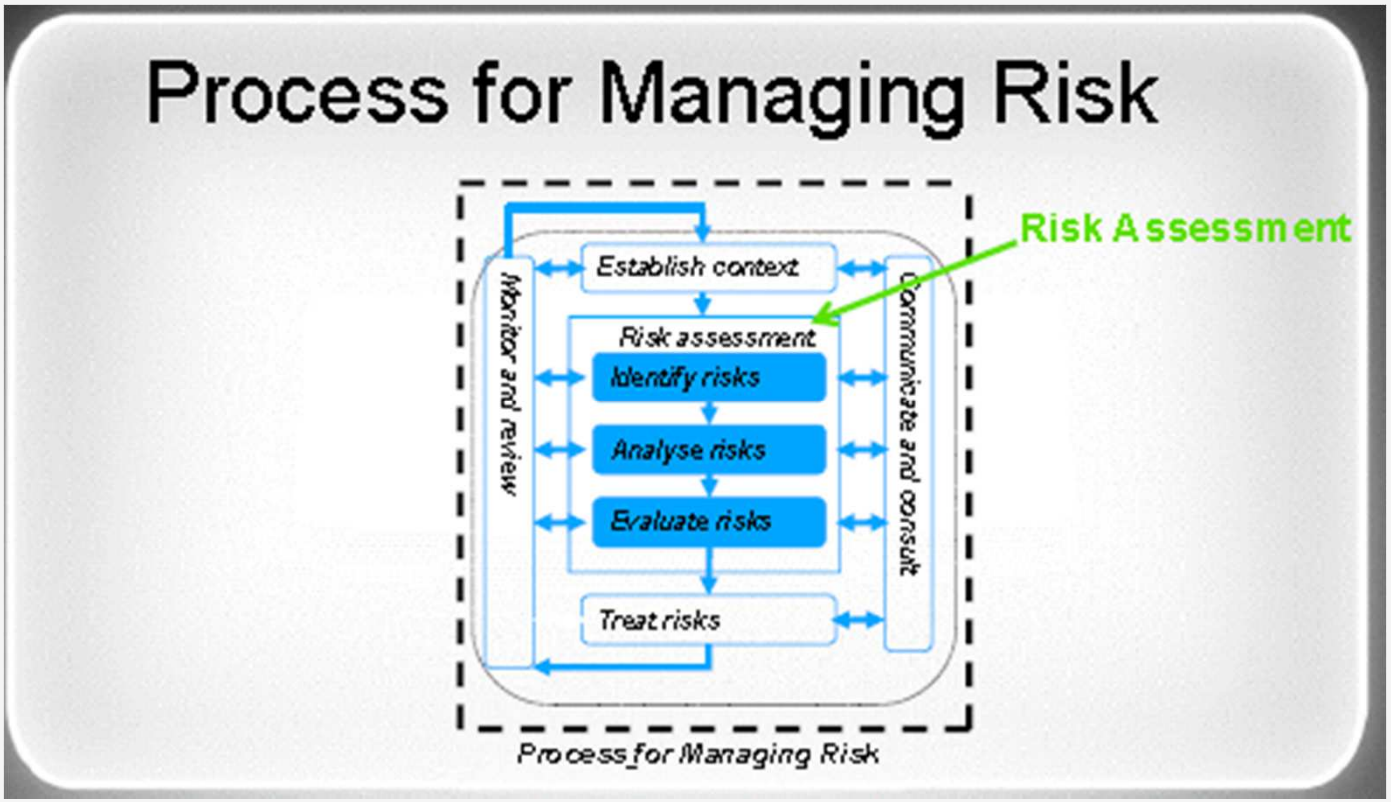
Principales Diferencias

Riesgo

- Propietario del Riesgo en lugar de propietario del activo
- Sólo es necesario para identificar los riesgos con respecto a Confidencialidad, Integridad y Disponibilidad
- incluye "riesgos positivos" también conocidos como Oportunidades
- Plan de tratamiento de riesgos usado para crear la declaración de aplicabilidad

Principales Diferencias

Riesgo



Principales Diferencias

Plan de Tratamiento del Riesgo

- La cláusula 6.1.3 describe cómo una organización puede responder a los riesgos con un Plan de Tratamiento de Riesgos, una parte importante de esto es la elección de los controles adecuados
- Estos controles y objetivos de control, figuran en el Anexo A, aunque también es posible, en principio que las organizaciones implementen controles tomados de cualquier otra fuente

Principales Diferencias

7 Soporte

- Lo necesario para establecer, implementar y mantener y mejorar continuamente un SGSI efectivo incluye:
  - Requerimientos de recursos o
  - competencias de las personas involucradas
  - Conocimiento y comunicación con las partes interesadas
  - Requisitos para la gestión de documentos
- Se refiere a la "información documentada" en lugar de "documentos y registros“
- Ya no es una lista de los documentos que se necesitan o nombres particulares que se les debe dar
- Más énfasis en el contenido en lugar del nombre.

Principales Diferencias

8 Operaciones

- Las organizaciones deben planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información
- Se incluye:
  - Llevar a cabo valoraciones de riesgo de SI a intervalos planificados
  - La implementación de un Plan de Tratamiento de Riesgos de SI

Principales Diferencias

9 Evaluaciones del desempeño

- Auditorías internas y revisión por la dirección métodos clave de la revisión del rendimiento del SGSI y herramientas para su mejora continua
- Requisitos más específicos para la medición de la efectividad

Principales Diferencias

10 Mejora

- Las no conformidades de los SGSI tienen que ser tratadas junto con las acciones correctivas para asegurarse de que no vuelvan a ocurrir
- Al igual que con todos los estándares de sistemas de gestión, la mejora continua es un requisito básico de la norma

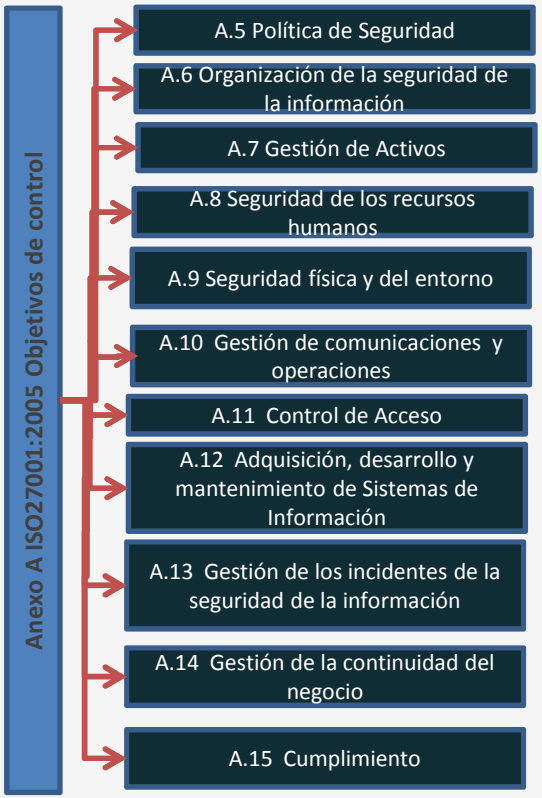
Principales Diferencias

Dominios y Controles

- Ahora se tienen 14 dominios (2005: 11 dominios)
- El número de controles se redujo de 133 a 113 controles
- Se han eliminado o fusionado algunos controles
- Algunos controles nuevos se han añadido
- Algunos de los controles que permanecen han sido han sido reformulados

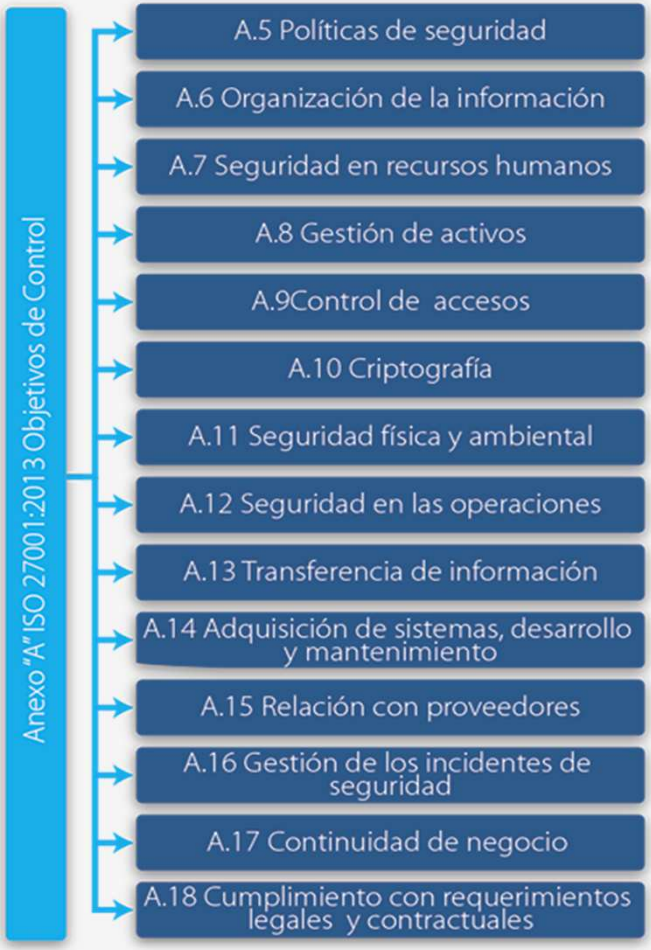
ISO27001/2005	ISO27001/2013
Total dominios de los controles 11	Total dominios de los controles 14
Número de controles 133	Número de controles 113

Principales Diferencias



El número de dominios del anexo aumenta de 11 a 14

Dominios de la norma ISO/IEC 27001:2013



Principales Diferencias

Controles del Anexo A

Lista de controles que ya no forman parte del estándar:

Control	Descripción	Cambia por	Incluye los controles de la ISO 27001:2005
A.6.1.1	Comité de gestión para la seguridad de la información	Roles de la seguridad de la información y sus responsabilidades	A.6.1.3 y A.8.1.1
A.6.1.2	Coordinación de seguridad de la información	Contacto con autoridades	A.6.1.6
A.6.1.4	Procesos de autorización para instalaciones para procesamiento de información	Seguridad de la información en la gestión de proyectos	
A.6.2.1	Identificación de riesgos relacionados con agentes externos	Política de dispositivo móvil	A.11.7.1
A.6.2.2	Direccionamiento de seguridad al tratar con clientes	Trabajo a distancia	A.11.7.2
A.10.2.1	Entrega del servicio		
A.10.7.4	Seguridad del sistema de documentos		
A.10.8.5	Sistema de información de negocios		
A.10.10.2	Seguimiento al uso de sistema		
A.10.10.5	Falla en el registro		
A.11.4.2	Autenticación de usuarios para conexiones externas		

Principales Diferencias

Controles del Anexo A

Lista de controles que ya no forman parte del estándar:

A.11.4.3	Identificación de equipos		
A.11.4.4	Puerto remoto de diagnóstico y configuración de protección		
A.11.4.6	Control para la conexión de redes		
A.11.6.2	Aislamiento del sistema sensible		
A.12.2.1	Validación de datos de entrada	Controles contra *malware*	A.10.4.1
A.12.2.2	Control de procesamiento interno		
A.12.2.3	Integridad de mensaje		
A.12.2.4	Validación de datos de salida		
A.12.5.4	Filtración de la información		
A.15.1.5	Prevención del uso indebido de las instalaciones para el procesamiento de información		
A.15.3.2	Protección de las herramientas de auditoría de sistemas de información		

Principales Diferencias

Controles del Anexo A

Nuevos controles propuestos

Control	Descripción	Absorbe los controles de la ISO 27001:2005
A.6.1.4	Seguridad de la información en la gestión de proyectos	
A.12.6.2	Restricciones en la instalación de software	
A.14.2.1	Política de desarrollo de seguridad	
A.14.2.5	Desarrollo de procedimientos para el sistema	
A.14.2.6	Desarrollo de un entorno seguro	
A.14.2.8	Sistema de prueba de seguridad	
A.15.1.1	Información de seguridad para las relaciones de proveedores	A.6.2.3
A.15.1.3	Cadena de suministro ICT	
A.16.1.4	Evaluación y decisión de los eventos de seguridad de la información	
A.16.1.5	Respuesta a incidentes de seguridad de la información	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	
A.17.2.1	Disponibilidad de las instalaciones para procesamiento de	

Agenda

- **ISO 27000**
  - La familia ISO 27000
  - ¿Qué es ISO 27001:2013?
  - ¿Qué es un SGSI?
  - Por que seleccionar ISO 27001?

- **Principales cambios ISO 27001: 2013 Vs. ISO 27001:2005**
  - El ciclo PHVA
  - Los 5 principales cambios
  - Otros Cambios relevantes
  - Estructura del Documento
  - **Sección 3** Términos y definiciones
  - **Sección 4** Contexto de la organización
  - **Sección 5** Liderazgo
  - **Sección 6** Planeación
  - **Sección 7** Soporte
  - **Sección 8** Operaciones
  - **Sección 9** Evaluación del desempeño
  - **Sección 10** Mejora
  - **Anexo A** Cambios en los Controles
- **Tiempo de Transición**
- **Conclusiones**

Principales Diferencias

Tiempo de transición

Según lo especificado por el Foro Internacional de Acreditación (IAF), todos los **certificados vigentes** bajo los requisitos **de la norma ISO/IEC 27001:2005** deberán ser **actualizado**s en un periodo máximo de dos (2) años, el cual finalizará en **2015-10-01**,

Principales Diferencias

Tiempo de transición

Lineamientos aplicables para la transición de las certificaciones a la nueva versión:

1. Organizaciones certificadas con la ISO/IEC 27001 versión 2005 antes del día 2013-10-01

Las auditorías de seguimientos, reactivaciones y renovaciones de certificados emitidos con la norma ISO/IEC 27001 versión 2005, se podrán realizar hasta el 2015-04-01.

2. Organizaciones que aún no están certificadas con la ISO/IEC 27001

Las auditorías de otorgamiento de certificados con la norma ISO/IEC 27001 con la versión 2005 solo serán permitidas hasta el día 2014-10-01, después de esta fecha las auditorías de otorgamiento se realizarán solamente con ISO/IEC 27001 versión 2013.

Principales Diferencias

Conclusiones

Esta nueva versión refleja una **mayor flexibilidad** para su implementación dentro de las empresas sin importar su tamaño, así como la necesidad de **adaptarse a la evolución de las tecnologías**, lo que para muchos ya era inminente desde hace algunos años.

La recomendación para quienes ya poseen un SGSI implementado es considerar el apoyo de consultores con experiencia para llevar a cabo las modificaciones y dirigir los esfuerzos hacia una actualización exitosa de la norma, conforme lo dictan los requisitos. Después de todo, **con la actualización de la norma el cumplimiento** será más fácil de implementar con mejor flexibilidad para las empresas de cualquier tamaño.

Si usted asistió a esta charla agradecemos diligenciar la siguiente encuesta

http://goo.gl/rcNxUc

Preguntas