SEGURIDAD DE LA INFORMACIÓN

Paloma Llaneza

II Jornada sobre certificación acreditada en España

28 de noviembre de 2006

llaneza a+a
llaneza abogados asociados

ISO JTC 1/SC 57

- El funcionamiento del Subcomité 27, en el ámbito nacional y en el internacional, se ha venido articulando alrededor de tres Grupos de Trabajo (WGs)
  - Gestión de la seguridad (WG1)
  - Criptografía (WG2)
  - Certificación y evaluación de la seguridad de las tecnologías de la información (WG3).

- A partir de la reunión de Madrid de mayo de 2006 del SC27 internacional, entran en funcionamiento dos nuevos WG
  - WG4 se dedicará a la normalización de servicios y aplicaciones que apoyen la implantación de los controles de la ISO/IEC 27002 (actual 17799:2005)
  - WG5 se dedicará a la normalización de los aspectos técnicos en materia de privacidad y gestión de identidad.

Proyectos de la familia 27000-SGSI

- ISO ha asignado a la Familia 27000 de Sistemas de Gestión SI (ISMS en inglés) los números 27000 al 27019 y del 27030 al 27044.

- Se incluirán en la familia ISMS aquellas normas internacionales que estén relacionadas con los requerimientos de la ISO/IEC 27001 siempre que establezcan guías para su implantación, por ejemplo
  - El análisis de riesgos SI
  - Medidas de la eficacia de los controles SI
  - Auditoría del ISMS
  - Cuando establezcan requerimientos específicos sectoriales o requerimientos de evaluación de conformidad para el ISMS

Proyectos de la familia 27000-SGSI

- Quedan excluidas de la familia 27000 las normas que únicamente tiene por objeto el detalle técnico para la implantación de controles de la ISO/IEC 27002 (actual 17799:2005).

Proyectos actuales de la familia 27000

Serie 27000-27009 (proyectos en tramitación):

- **27000:** Aspectos fundamentales y vocabulario SGSI
- **27003:** Guías de implantación SGSI
- **27004:** Medidas (*métricas*) del SGSI
- **27005:** Gestión de riesgos de seguridad de la información
- **27006:** Requisitos para la acreditación de entidades que certifiquen ISMS

Estado de tramitación

Octubre 2004	Abril 2005	Noviembre 2006	Abril 2007
ISO/IEC 13335-1 MICTS* Part 1: Concepts and models for Information and Communications Technology security management		**27000** 1st CD Information security management – Overview and vocabulary	
24743 Information security management systems - Requirements	**27001** Information security management systems – Requirements **27001-2005** Publicada		
ISO/IEC 17799:2005			**27002**
		27003 WD Implementation Guidance	
24742 Information security management metrics and measurements	**27004** Information security management metrics and measurements	**27004** 1st CD Information security management measurements	
ISO/IEC 13555-2 MICTS* Part 2: Information security risk management * Management of information and communications technology security		**27005 FCD** Information security risk management	
		27006 FDIS Information security risk management	

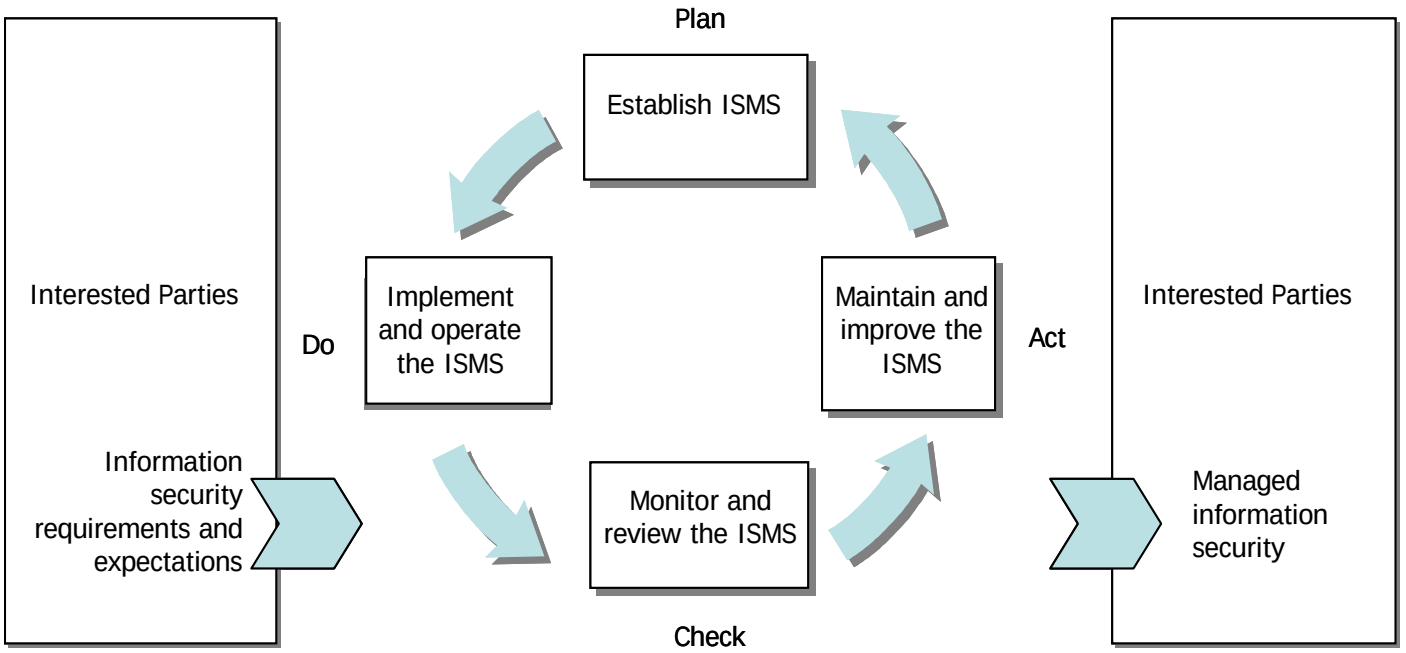
llaneza a+a
llaneza abogados asociados

Proyectos futuros del WG1

- Information security management guidelines for telecommunications (X.1051/27031).
- ISMS Auditor Guidelines (posible 27007)
- Sector-Specific ISMS Standards for the World Lottery Association
- Sector-Specific ISMS Standards for the Automotive Industry

llaneza a+a
llaneza abogados asociados

Sistema de gestión SGSI-ISMS



llaneza a+a
llaneza abogados asociados

Esquema de acreditación 27006

27006- Requirements for accreditation of certification bodies

- Versión revisada de EA-7/03 (Requisitos para la Acreditación de Entidades que operan Certificación / Registro)
- Basada en la ISO/IEC 17021 (Certificación de Sistemas de Gestión de Seguridad de la Información basados en la norma de Evaluación de Conformidad)
- Proporciona una interpretación de los requisitos de acreditación ajustados a ISMS.

Auditoría ISMS-SGSI

- Un nuevo documento está en estudio que complementaría la norma ISO/IEC 27006 así como la guía de auditoría general contenida en la norma ISO/IEC 19011.
- Se evitará la repetición en este documento de información ya contenida en la ISO/IEC 19011 y se elaborará con base en los requerimientos de la ISO/IEC 27001 y la ISO/IEC 27006.
- Tampoco incluirá requerimientos nuevos que no aparezcan en los antedichos documentos.

Auditoría ISMS-SGSI

- En la reunión del ISO JTC 1/SC27 en de Sudáfrica (noviembre 2006) se ha decidido incluir en este documento, al menos, las siguientes materias:
- Métodos y técnicas de auditoría.
- Análisis de "Audit trail"
- Audit forensics
- Confirmación del scope del ISMS
- Comprobación de la documentación del ISMS y en concreto:
  - El informe de análisis de riesgos (Risk assessment report)
  - El plan de gestión de riesgos (Risk treatment plan)
  - Y el "statement of Applicability"
- Comprobación de los sistemas y procedimientos de monitoreo y revisión
- Sampling de sites
- Conexiones externas, outsourcing y prestación de servicios por terceros

llaneza a+a
llaneza abogados asociados

GRACIAS
POR SU ATENCIÓN

Paloma Llaneza González
pll@palomallaneza.com

llaneza a+a
llaneza abogados asociados