

# ISO 27003 (SGSI) Ayuda y guía para implementar un SGSI

Ing. Fernando Moreno, CISM, Auditor 27001





### Evolución normativa del modelo SGSI



Código de práctica	1993		ISO/IEC 27002	2007
Norma BS 7799	1995		ISO/IEC 27006	2007
BS 7799 parte 2	1998		ISO/IEC 27005	2008
Revisión partes 1 y 2	1999		ISO/IEC 27000	2009
ISO/IEC 17799	2000		ISO/IEC 27004	2009
BS 7799-2:2002	2002		ISO/IEC 27003	2010
ISO/IEC 17799	2005	4	ISO/IEC 27005	2011
ISO/IEC 27001	2005		ISO/IEC 27008	2011

Familia normas ISO/IEC 27000







## ISO 27003 Guía de implementación de Sistemas de Gestión de Seguridad



- Hacia inicios de febrero de 2010 se publica la norma ISO/IEC 27003, con la finalidad de proporcionar una guía sobre de implementación del estandar ISO 27001.
- Esta publicación ayudará a las organizaciones a implementar un SGSI, principalmente enfocado en las clausulas 4,5 y 7 de estándar.
  - 4. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
    - **4.1 REQUISITOS GENERALES**
    - 4.2 ESTABLECIMIENTO Y GESTIÓN DEL SGSI
    - 4.3 REQUISITOS DE DOCUMENTACIÓN
  - 5. RESPONSABILIDAD DE LA DIRECCIÓN
    - 5.1 COMPROMISO DE LA DIRECCIÓN
    - **5.2 GESTIÓN DE RECURSOS**
  - 7. REVISIÓN DEL SGSI POR LA DIRECCIÓN
    - 7.1 GENERALIDADES
    - 7.2 INFORMACIÓN PARA LA REVISIÓN
    - 7.3 RESULTADOS DE LA REVISIÓN





#### ISO 27003 – Estructura General



- a) Obtaining management approval for initiating an ISMS project (Clause 5)
- b) Defining ISMS Scope and ISMS Policy (Clause 6)
- c) Conducting Organization Analysis (Clause 7)
- d) Conducting Risk Assessment and Risk Treatment planning (Clause 8)
- e) Designing the ISMS (Clause 9)

Obtaining management approval for initiating an ISMS project

Defining ISMS scope, boundaries and ISMS policy

security requirements analysis

Conducting information

Conducting risk assessment and planning risk treatment

Design the ISMS

Management approval for initiating ISMS Project

The ISMS Scope and boundaries

ISMS Policy

Information security requirements

Information assets

Results from information security assessment

Written notice of management approval for implementing the ISMS

Risk treatment plan

SoA, including the control objectives and the selected controls

Final ISMS project implementation plan

### Numeral 5 - Obtener la aprobación de la dirección para iniciar un proyecto SGSI



Clarify the organization's priorities to develop an ISMS

Objectives for an

Summarized

ISMS

5.2

Define the preliminary ISMS scope

5.3

Develop the preliminary ISMS scope

5.3.1

Outlined business characteristics

Define roles & responsibilities for the preliminary ISMS scope

5.3.2

Description of roles and responsibilities for implementing an ISMS

Create the business case and the project plan for management approval

5.4

Business case

ISMS Project Proposal

Approval of an ISMS Project

List of regulatory contractual and industry constraints relevant to the information security of the organization

Outlined business characteristics

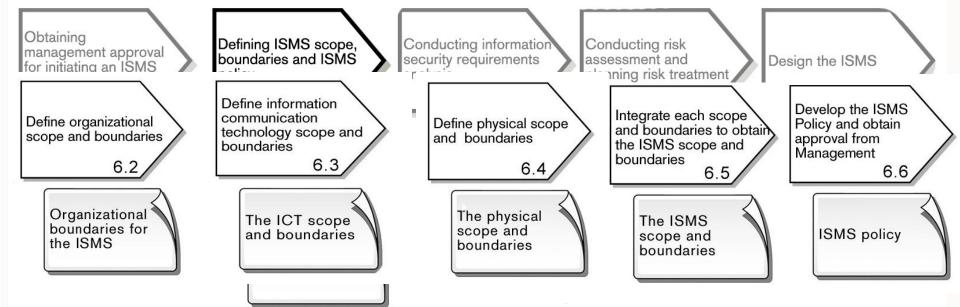


www.globalteksecurity.com

### Numeral 6 - Definir el alcance, límites y política del SGSI



Timeline

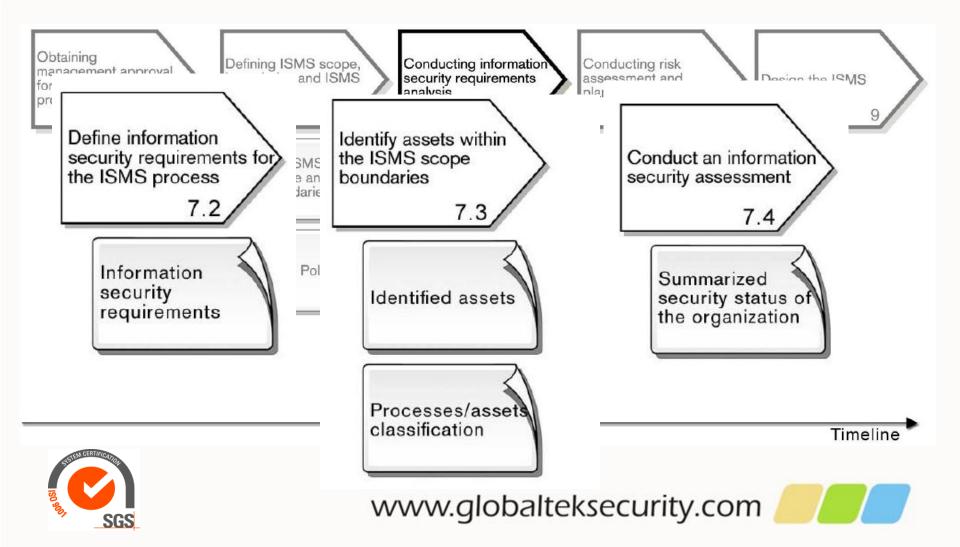






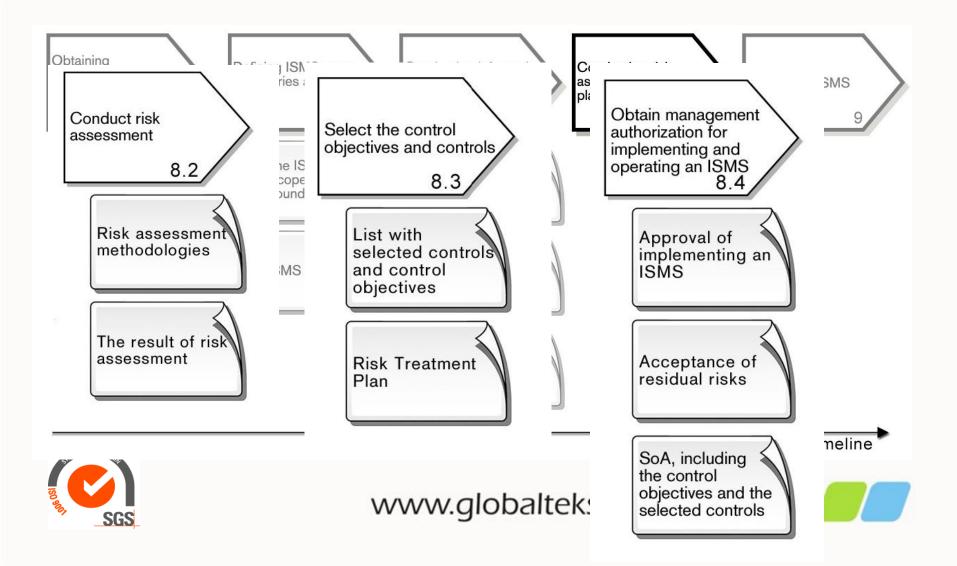
## Numeral 7 - Realizar un análisis de requisitos de seguridad de la información





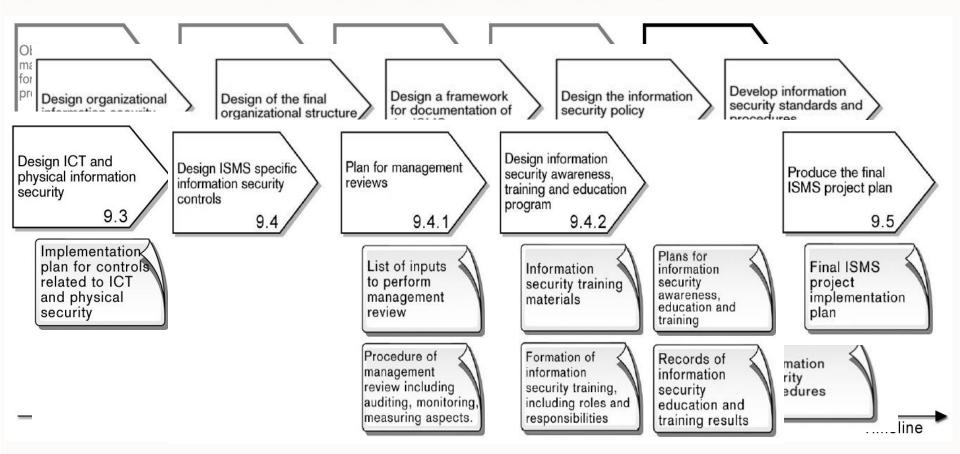
## Numeral 8 - Realizar la valoración de riesgos y planificar el tratamiento de los riesgos





### Numeral 9 - Diseñar el SGSI











### Anexo A - Cheklist de las actividades requeridas para implementar un SGSI

	Implementation Phase ISO/IEC 27003	Step number	Activity, reference ISO/IEC 27003	Step Pre- Requisite	Documented Output	Reference to ISO/IEC 27001
	5 Obtaining Management Approval for the implementation of ISMS	1.	Gather corporation business objectives	None	List of corporation business objectives	N/A
		2.	Gain understanding of existing management systems	None	Description of existing management systems	N/A
		3.	5.2 Define objectives, information security needs, business requirements for ISMS	1, 2	Summary of the objectives, information security needs and business requirements for the ISMS	N/A
		4.	Gather relevant regulatory, compliance, and industry standards applicable to the corporation	None	Summary of regulatory, compliance, and industry standards that are applicable to the corporation	N/A
		5.	5.3 Define preliminary ISMS scope	3, 4	Description of preliminary scope of ISMS (5.3.1)	N/A
					Definition of ISMS	N/A



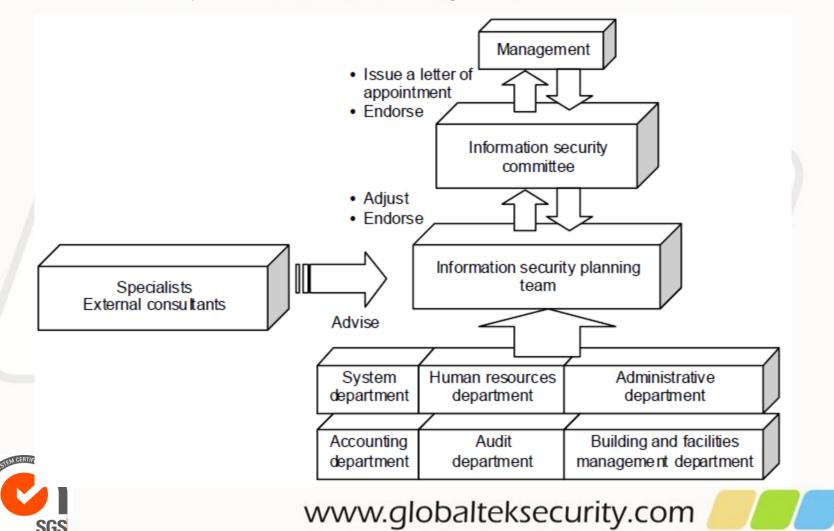


roles and

responsibilities (5.3.2)



Anexo B – Roles y responsabilidad de Seguridad de la información





Anexo C – Información acerca de Auditorias Internas

**Anexo D** – Estructura de la Documentación

#### **High Level General Policies**

e.g. security policy, privacy policy, marketing policy, product development policy

High Level Topic-specific Policies e.g. information security policy

#### **Detailed Policies**

e.g. access control policy, clear desk and clear screen policy use of network services policy use of cryptographic controls policy

Figure D.1 — Policy hierarchy

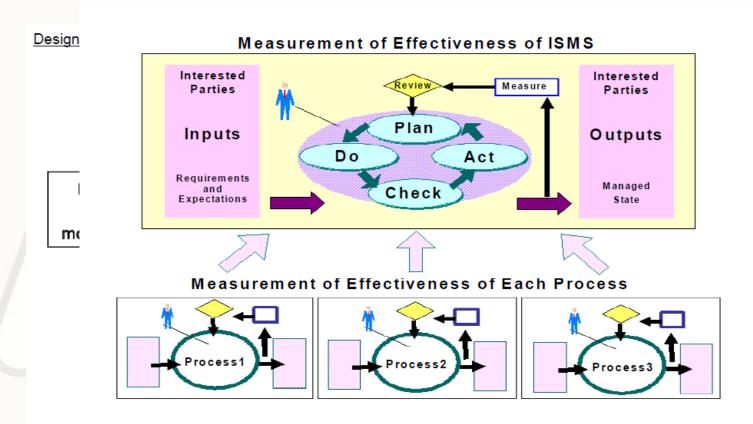


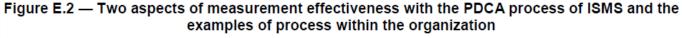






#### **Anexo E** – Monitoreo y medición







#### Conclusiones



La ISO 27003, se constituye en una guía de implementación de controles relacionados con la gestión de un SGSI, el cual nos permite realizar una planeación clara para de como implementar la ISO 27001 en sus numeral 4,5, y 7, y definir las estrategias de seguridad relacionadas con el negocio acorde con los requisitos de ISO 27001.

Cabe resaltar, la importancia que tiene incluir dentro del proceso de implementación de un SGSI, los lineamientos de otras normas de la familia 27000, como son la gestión de riesgos ISO 27005, la medición y métricas del sistema ISO 27004, el código de práctica ISO 27002, y las definiciones y conceptos enumerados en la ISO 27000, para la implementación de un correcto y apropiado SGSI en las organizaciones.



