



Universidad de Oviedo

Departamento de Informática
Campus de Gijón

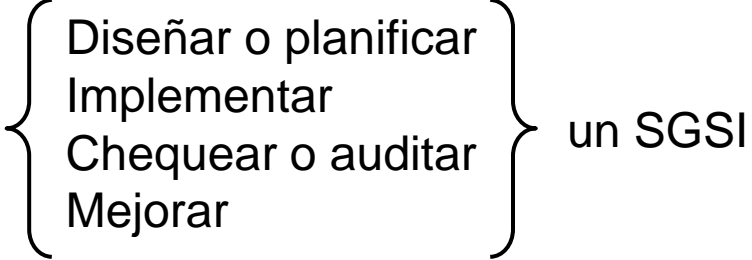
Normas y Estándares de Seguridad de la Información

Presentación

Daniel F. García

Objetivos 1

Objetivo primario de una norma (estándar):

Establecer un método para  un SGSI

Para una organización (empresa, hospital, banco, universidad, etc.)
Que sea AUDITABLE y CERTIFICABLE

Aspecto esencial

SGSI = **Sistema** de Gestión de la Seguridad de la Información



Concepto de sistema = **PROCESO** (Actividades Sistemáticas) necesario para garantizar la seguridad de la información

En este contexto Sistema \neq Conjunto de hardware y software

Sino que Sistema = Modo sistematizado de hacer las cosas

En algunos procesos se usará tecnología y sistemas informáticos (Hard & Soft)

Objetivos 2

Una visión MÁS amplia

Hay autores que usan el concepto de INFORMATION SECURITY GOVERNANCE

Governance == Gobierno, pero en un contexto empresarial

Corporate Governance == $\left\{ \begin{array}{l} \text{Dirección de Empresas} \\ \text{Gerencia Corporativa} \end{array} \right.$

En español se suele usar la palabra “gobernanza”

Objetivo similar → Desarrollar una estrategia para implementar la gobernanza de la seguridad de la información

Una estrategia para la gobernanza de la SI ...

- Suele trabajar a un nivel más alto que un SGSI
- Suele centrarse en integrar los procesos de gestión de la seguridad con otros procesos de gestión desarrollados en la organización

Uso de metodologías y estándares

Para diseñar, implementar, etc., un SGSI es muy conveniente utilizar Metodologías y Estándares ampliamente adoptados

ISO/IEC 27000 (o 27K)

Es el estándar más usado actualmente y está totalmente enfocado a la seguridad de la información

Desarrollado por la ISO: **International Organization for Standardization** <https://www.iso.org>

Una organización puede obtener el certificado ISO 27001

COBIT *Control Objectives for Information and Related Technology*

Proporciona un conjunto de buenas prácticas para la gestión de la información

Desarrollado por { **ISACA – Information Systems Audit & Control Association** <https://www.isaca.org>
ITGI – Information Technology Governance Institute

Uno de los aspectos de la gestión de la información es la gestión de su seguridad

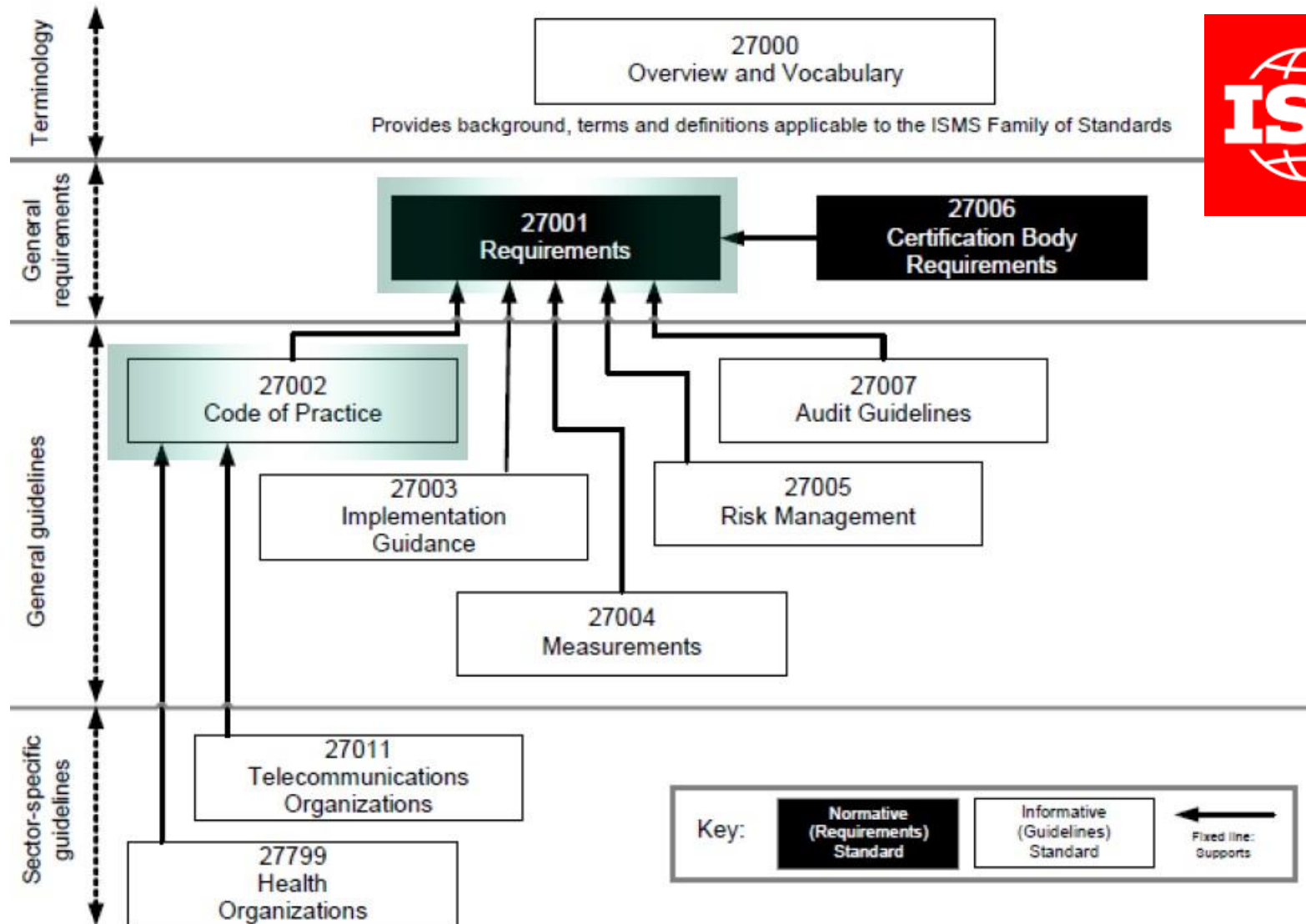
ITIL *Information Technology Infrastructure Library*

Proporciona un conjunto de buenas prácticas para la gestión de servicios de TI

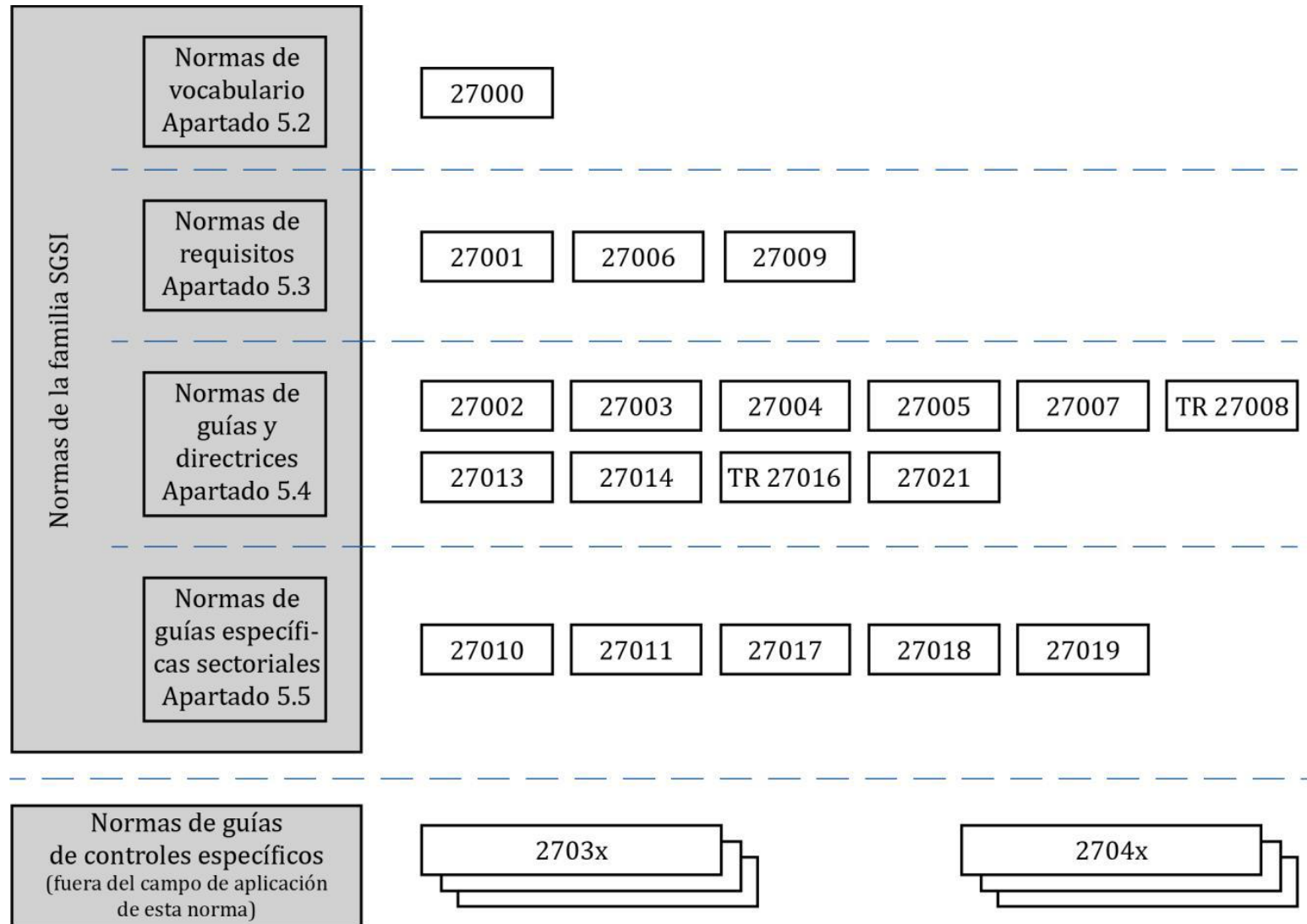
Desarrollado por el itSMF: **IT Service Management Forum** <https://www.itsmf.es>

Como uno de los aspectos de los servicios hay que considerar su seguridad

ISO 2700x Visión general (Año 2009)



ISO 2700x Visión general (Año 2021)



UNE-EN ISO/IEC 27000:2021 Figura 1

Estándares ISO 27xxx (1)

El estándar 27000 Última versión: Febrero-2018

Proporciona una introducción a la serie de estándares ISO 27xxx incluyendo:

- Un **glosario** de los términos y definiciones que se emplean en toda la serie 27xxx
- Una **introducción** a los Sistemas de Gestión de Seguridad de la Información
- Una **visión** general de la familia de **estándares** integrados en la serie 27xxx

El estándar 27001 Última versión: Octubre-2022

Contiene los **requisitos** generales del SGSI

Cubre el establecimiento, implementación, operación, monitorización, revisión y mejora del SGSI

Indica los requisitos de **documentación**

Establece las **responsabilidades** de gestión

Anexo A: Incluye un conjunto de objetivos de control y los controles correspondientes
Se desarrollan en el estándar 27002 y deben implementarlos las organizaciones
(Una organización debe argumentar por que no ha implementado ciertos controles)

¡El ISO 27001 es el único estándar certificable de la serie 27xxx!

Estándares ISO 27xxx (2)

El estándar 27002 Última versión: Febrero-2022

Es una guía de **buenas prácticas** que describe **93 controles de seguridad** que son recomendados para garantizar la seguridad de la información (208 páginas)

Contiene 4 capítulos dedicados a los controles de la seguridad:

Cap.5 Controles organizacionales (37)

Cap.6 Controles de personas (8)

Cap.7 Controles físicos (14)

Cap.8 Controles tecnológicos (34)

El estándar 27003 Última versión: Marzo-2017

Es una guía para la **implementación** de un SGSI que considera estos aspectos:

Contexto de la organización

Liderazgo

Planificación

Soporte

Operación

Evaluación de prestaciones

Mejoras

En los **anexos** (informativos) incluye un aspecto adicional:

A. Marco de desarrollo de políticas

Estándares ISO 27xxx (3)

El estándar 27004 Última versión: Diciembre-2016

Proporciona una guía para usar métricas y técnicas de medida de la eficacia de un SGSI (y de los controles implementados siguiendo el estándar ISO/IEC 27001) Incluye:

- Visión general sobre la medición de la seguridad de la información
- Selección de medidas y desarrollo del sistema de medición
- Funcionamiento del sistema de medición
- Análisis de datos e informes
- Evaluación y mejora del sistema de medición

El estándar 27005 Última versión: Octubre-2022

Provee directrices para gestionar riesgos de seguridad considerando estos aspectos:

Valoración, tratamiento, aceptación, comunicación, monitorización y revisión de riesgos

En los anexos:
(informativos)

- A. Alcance y límites del proceso de gestión de riesgos
- B. Identificación-valoración de activos y valoración de impactos
- C. Ejemplos de amenazas
- D. Vulnerabilidades y métodos de valoración de vulnerabilidades
- E. Enfoques para la valoración de riesgos
- F. Restricciones para la reducción de riesgos

Estándares ISO 27xxx (4)

El estándar 27006 Última versión: Octubre-2022

Especifica los requisitos para la acreditación de los organismos que auditan y certifican SGSIs
PERO NO ES UN ESTÁNDAR DE ACREDITACIÓN EN SI MISMO

El estándar considera los siguientes tipos de requisitos:

Generales, estructurales, de recursos, de información, de procesos, y del sistema de gestión

En los anexos (informativos) proporciona guía adicional:

- A. Análisis de una organización cliente y los aspectos específicos de un sector
- B. Ejemplos de áreas de competencia de un auditor
- C. Períodos de auditoría
- D. Guía para revisar los controles implementados siguiendo el Anexo A de ISO/IEC 27001

El estándar 27007 Última versión: Enero-2020

Consiste en una guía de auditoría de los controles seleccionados en la implantación de un SGSI

Es un complemento del estándar ISO 19011:2018

Directrices para la auditoría de los sistemas de gestión

ISO 27001 – Introducción al estándar

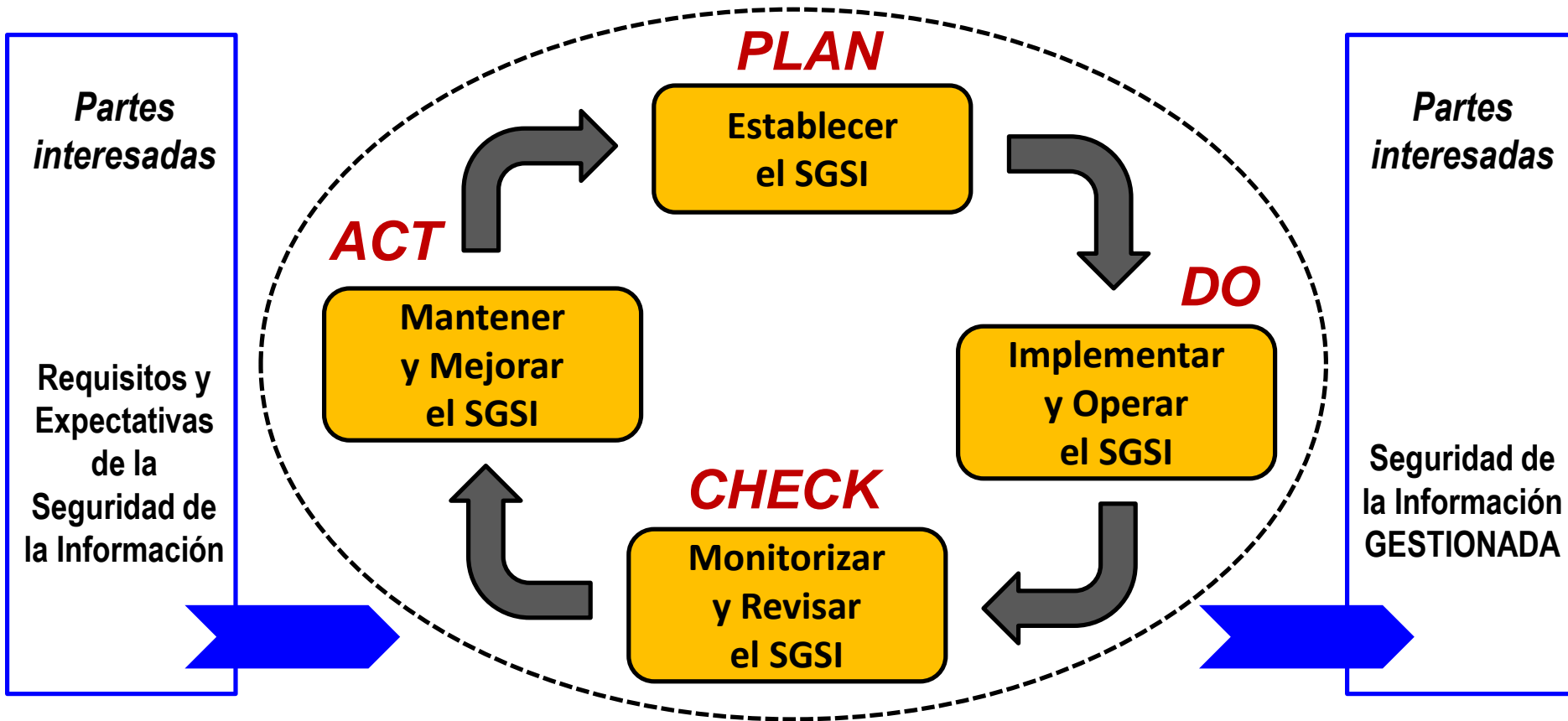
El estándar adopta un enfoque de procesos para establecer, implantar, revisar y mejorar un SGSI

Proceso == Actividad gestionada adecuadamente para transformar entradas en salidas

Enfoque de Procesos → Aplicar un sistema de procesos dentro de una organización

(Hay que identificar los procesos, las interacciones entre ellos, y gestionarlos)

El estándar adopta el modelo PDCA (*Plan-Do-Check-Act*) para estructurar los procesos



PLAN Establecer el SGSI

Establecer la **política y los objetivos** del SGSI

Establecer los procesos y procedimientos necesarios para

	{	Gestionar los riesgos y
		Mejorar la seguridad de la información

Para obtener resultados acordes con la **política y objetivos** globales de una organización

DO Implementar y operar el SGSI

Implementar y aplicar la política, los controles, los procesos y procedimientos del SGSI

CHECK Monitorizar y revisar el SGSI

Evaluar y medir la eficacia de los procesos en relación con la política y los objetivos del SGSI

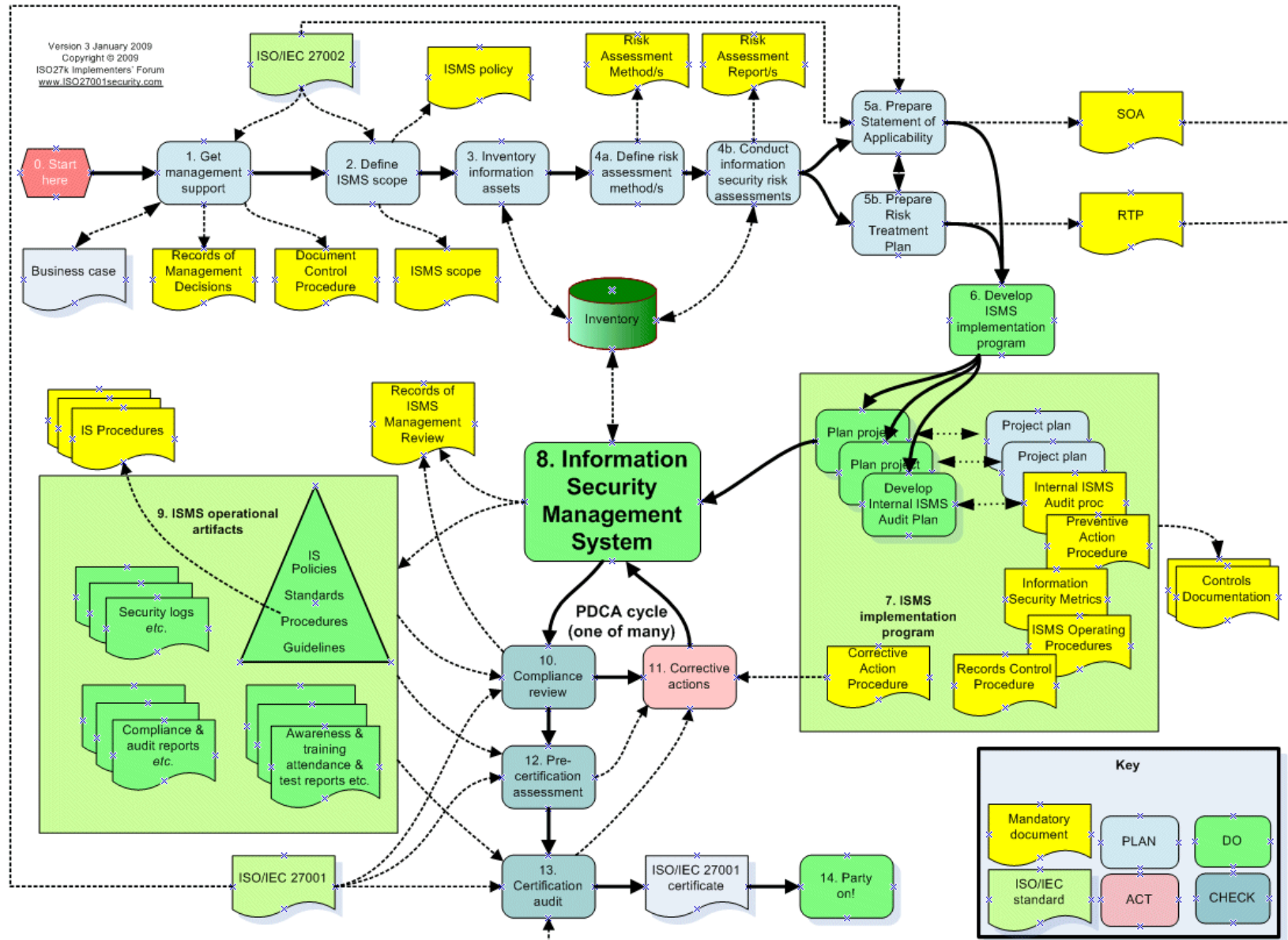
Informar de los resultados a la dirección de la organización para su revisión

ACT Mantener y mejorar el SGSI

Tomar acciones correctivas y preventivas basadas en la auditoría y la revisión del SGSI

Para lograr la mejora continua del SGSI

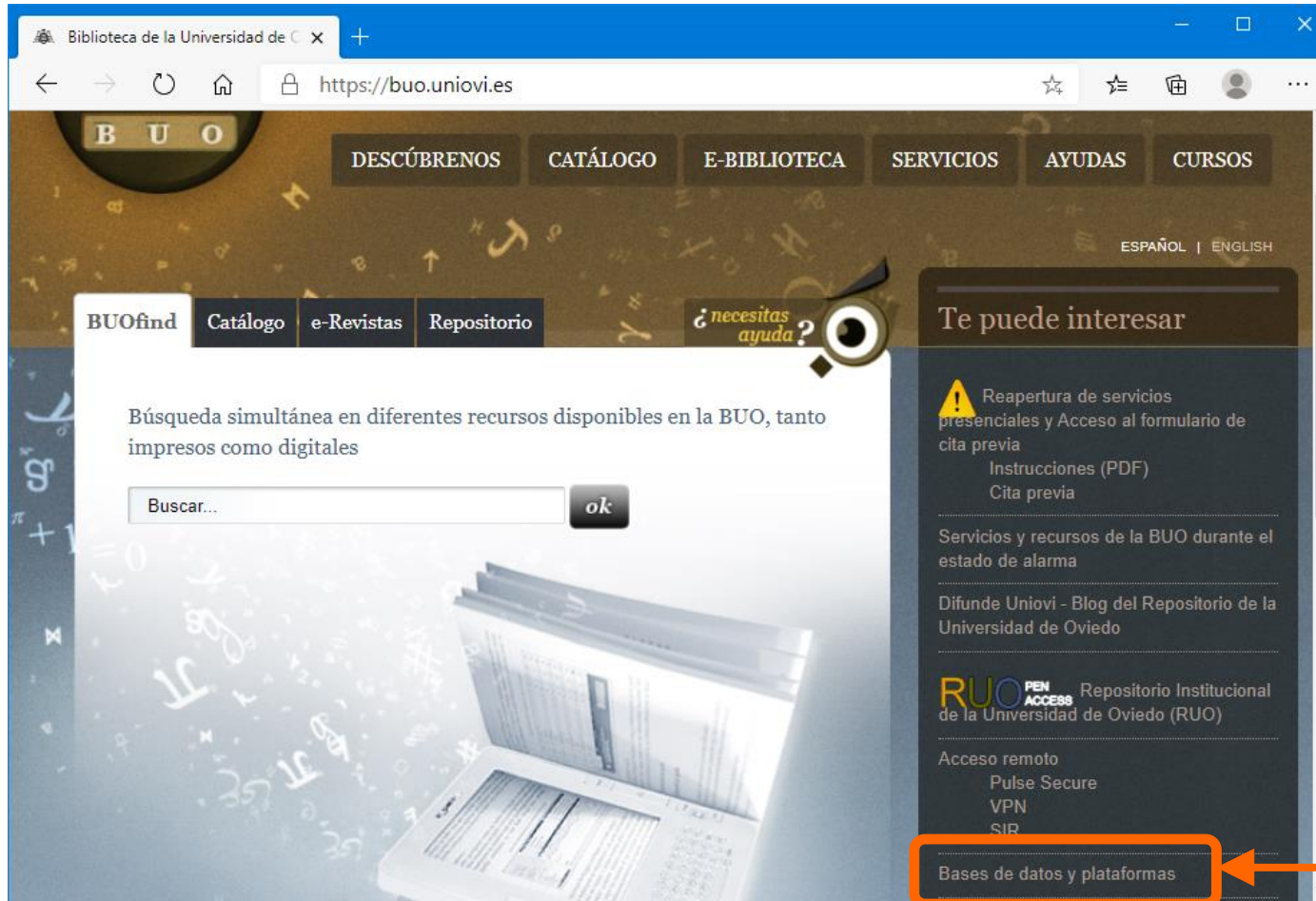
ISO 27001 y 27002 Visión general



Acceso a algunas normas ISO 27xxx (1)

AENOR proporciona versiones en español de algunas normas ISO 27xxx <https://www.aenor.com>

Acceder a la web de la biblioteca de la Universidad de Oviedo:



En el listado ordenado de BD y plataformas buscar AENOR y pulsar el botón de acceso AENORmas

Acceso a algunas normas ISO 27xxx (2)

Dentro de la web de AENOR usar el buscador

The screenshot shows a web browser window with the AENORMás search interface. The search term '27000' has been entered, resulting in 4 search results. The results are listed in a table with columns for the standard number, its status, and download/view options. The standards shown are UNE-ISO/IEC 27000:2014, UNE-ISO/IEC 27000:2012, UNE-EN ISO/IEC 27000:2019, and UNE-EN ISO/IEC 27000:2021. The first three are marked as 'Anulada' (Annulled) and the last one as 'Vigente' (Valid).

Norma	Estado	Acciones
UNE-ISO/IEC 27000:2014	Anulada 20 / 02 / 2019	Descargar Leer
UNE-ISO/IEC 27000:2012	Anulada 20 / 02 / 2019	Descargar Leer
UNE-EN ISO/IEC 27000:2019	Anulada 15 / 12 / 2021	Descargar Leer
UNE-EN ISO/IEC 27000:2021	Vigente 15 / 12 / 2021	Descargar Leer