dit-upm

Seguridad de la Información organización

José A. Mañas < http://www.dit.upm.es/~pepe/>
Dep. de Ingeniería de Sistemas Telemáticos
E.T.S. Ingenieros de Telecomunicación
Universidad Politécnica de Madrid

7.2.2018

Seguridad

Seguridad de las redes y de la información:

la capacidad de las redes o de los sistemas de información
de resistir, con un determinado nivel de confianza,
los accidentes o acciones ilícitas o malintencionadas que
comprometan la disponibilidad, autenticidad, integridad y confidencialidad
de los datos almacenados o transmitidos y
de los servicios que dichas redes y sistemas ofrecen o hacen accesibles

REGULATION (EC) Not 460/2004 10 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of March 2004 establishing the European Network and Information Security Agency

Sistema de información

- Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento
- Los sistemas tienen una o dos misiones
  - custodiar datos
    para que puedan ser utilizados por quien debe cuando quiera
  - prestar servicios
    - administrativos
    - comerciales
    - industriales

ciberseguridad

- CIBERESPACIO
  nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información – incluida Internet–, las redes y los sistemas de información y de telecomunicaciones
  Estrategia de ciberseguridad nacional, 2013
- CIBERSEGURIDAD
  Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan
- (EN) CYBER SECURITY
  The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them. [CSS NZ:2011]

Resiliencia

- Resiliencia es la capacidad de los sistemas para seguir operando pese a estar sometidos a un ataque, aunque sea en un estado degradado o debilitado. Así mismo incluye la capacidad de restaurar con presteza sus funciones esenciales después de un ataque. Bajo la palabra ataque se incluyen tanto acciones deliberadas, como accidentes causados por personas o por el entorno.

- the ability of systems to operate while under attack, even in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack. The concept of information system resilience can also be applied to the other classes of threats, including threats from environmental disruptions and/or human errors of omission/commission.

Hablamos de seguridad

- La empresa necesita confiar en los sistemas
  - que la información está disponible cuando se necesita
  - que la información no se ve modificada sin control
  - que la información se mantiene reservada a los que necesitan conocerla
- ... y la seguridad aspira a dar confianza
  - en que los sistemas estarán listos para usarse
  - en las alteraciones son imposibles o se detectan
  - en que la información permanece confidencial

En la medida en que la seguridad proporciona confianza
empresa querrá seguridad

Los sistemas de información

- Antes
  - la informática era cosa de unos pocos profesionales
  - los sistemas eran complejos y muy suyos
  - la seguridad no era un problema
- La red
  - lo cambia todo
  - no hay equipos aislados
  - los malos saben lo mismo que los buenos
- Ahora
  - las amenazas incluyen la naturaleza, la industria y el hombre
  - los sistemas son excesivamente complejos para que alguien, en singular, comprenda absolutamente todos los detalles

dit

Generaciones de sistemas

	G.1	G.2	G.3
tecnología	*host*	cliente / servidor	en red
sistema	manejable	complejo	incierto
objetivo técnico	eficiencia	eficacia del sistema	eficacia para los usuarios
calidad	funciona	predecible	controlable
objetivo de negocio	manejar volumen	organizar	mejorar la productividad
información	herramienta	estrategia	recurso
amenazas	naturales	accidentales	deliberadas

atacantes y defensores

- el defensor tiene que proteger todos los frentes
  el atacante elige el punto más débil (para sus habilidades)
  - ¿qué hay que defender?
  - ¿cuáles son las prioridades?
- el defensor se defiende de ataques conocidos
  el atacante puede investigar
- el defensor no duerme
  el atacante elige el momento ideal
- el defensor debe ser legal (más o menos)
  el atacante puede jugar sucio

Gobierno de las TIC

- Las TIC son una oportunidad pero conllevan un riesgo
- Las decisiones deben equilibrar ambas caras
  - destinando recursos prudentes a los objetivos de negocio
  - destinando recursos prudentes a la protección
- Toda decisión de gobierno debe estar informada
  - la funcionalidad que queremos obtener
  - los riesgos en que incurrimos = su seguridad

órganos de gobierno

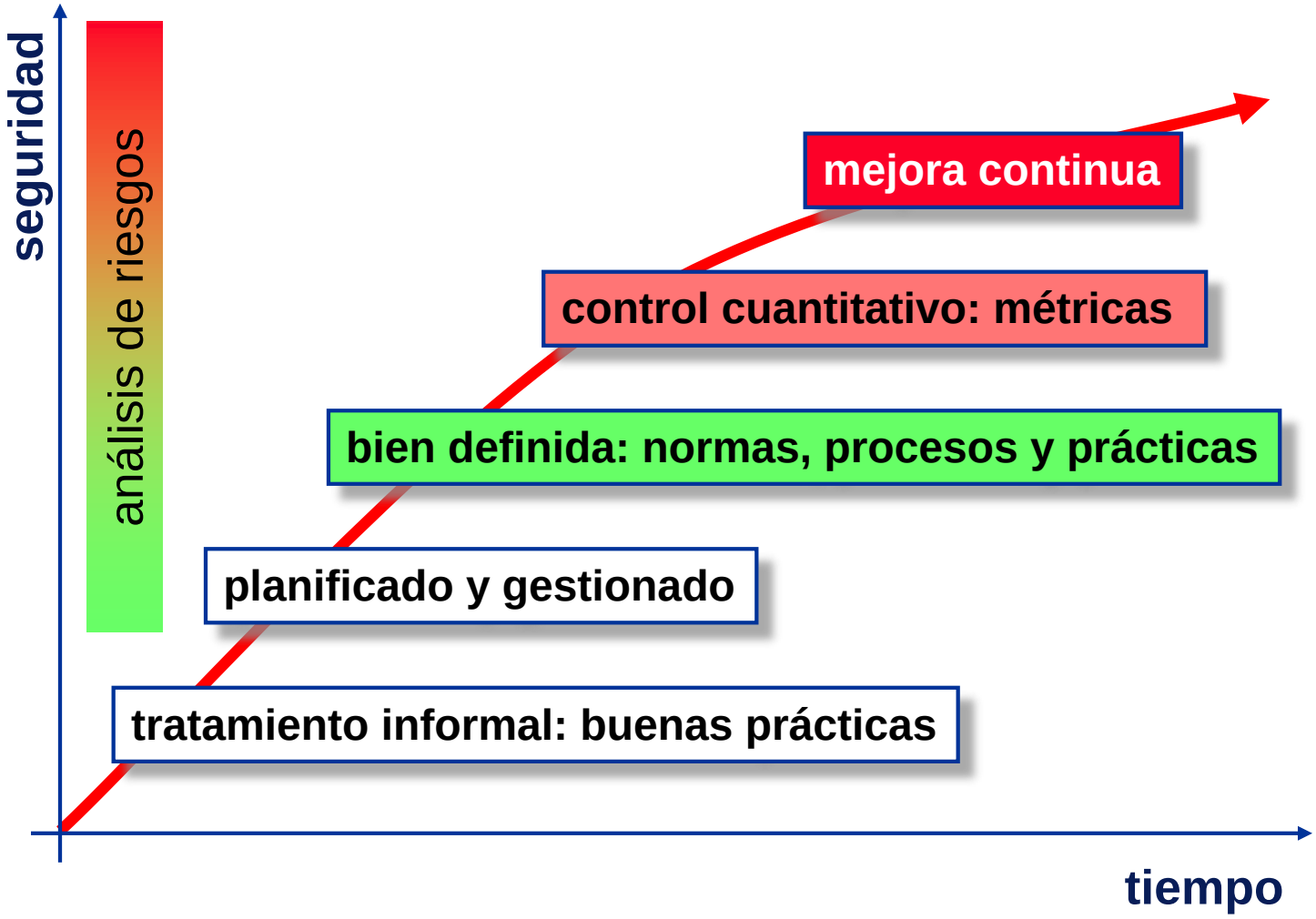
gestores

técnicos TIC

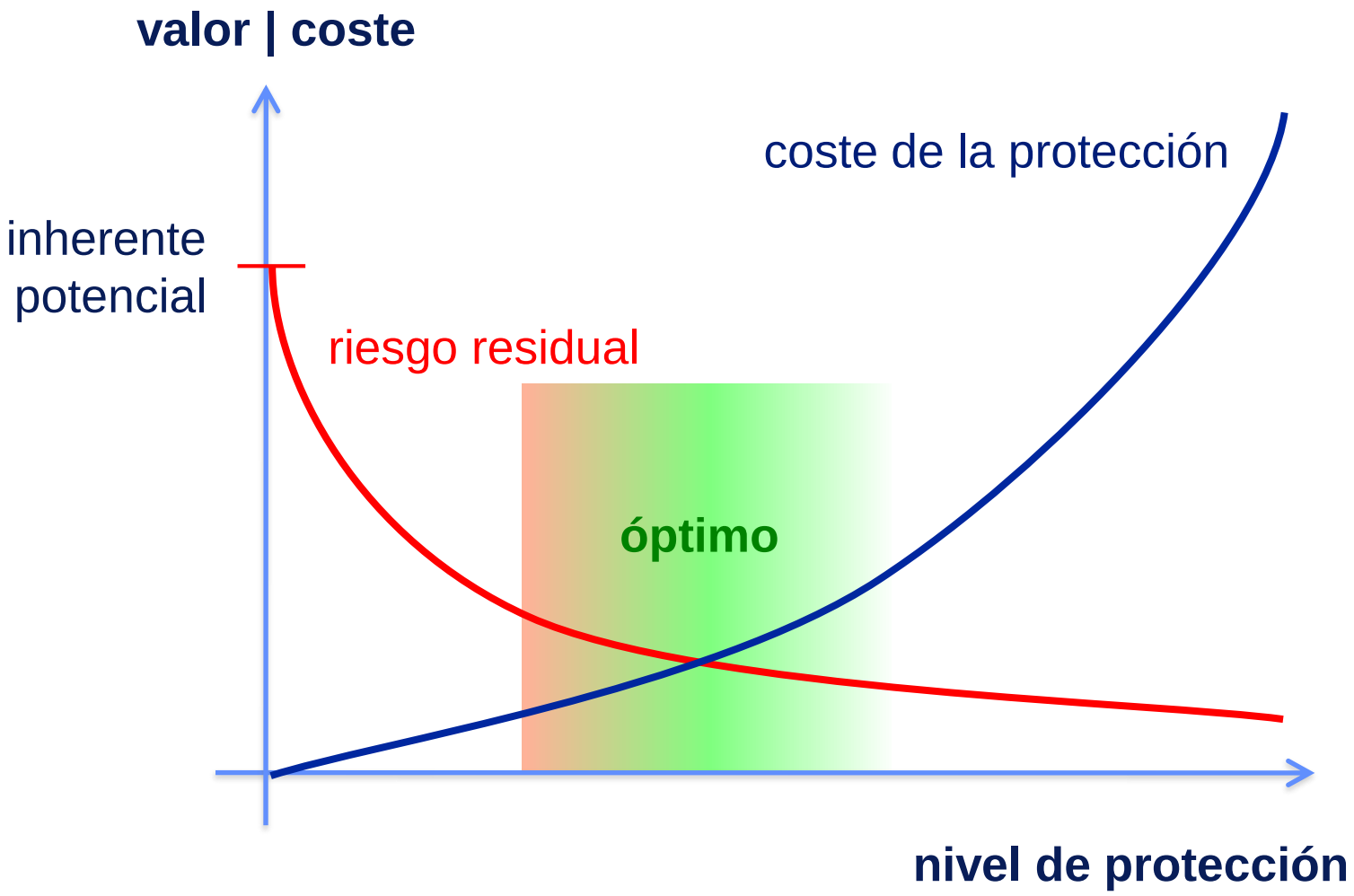
equipamiento TIC

Madurez

International Systems Security Engineering Association



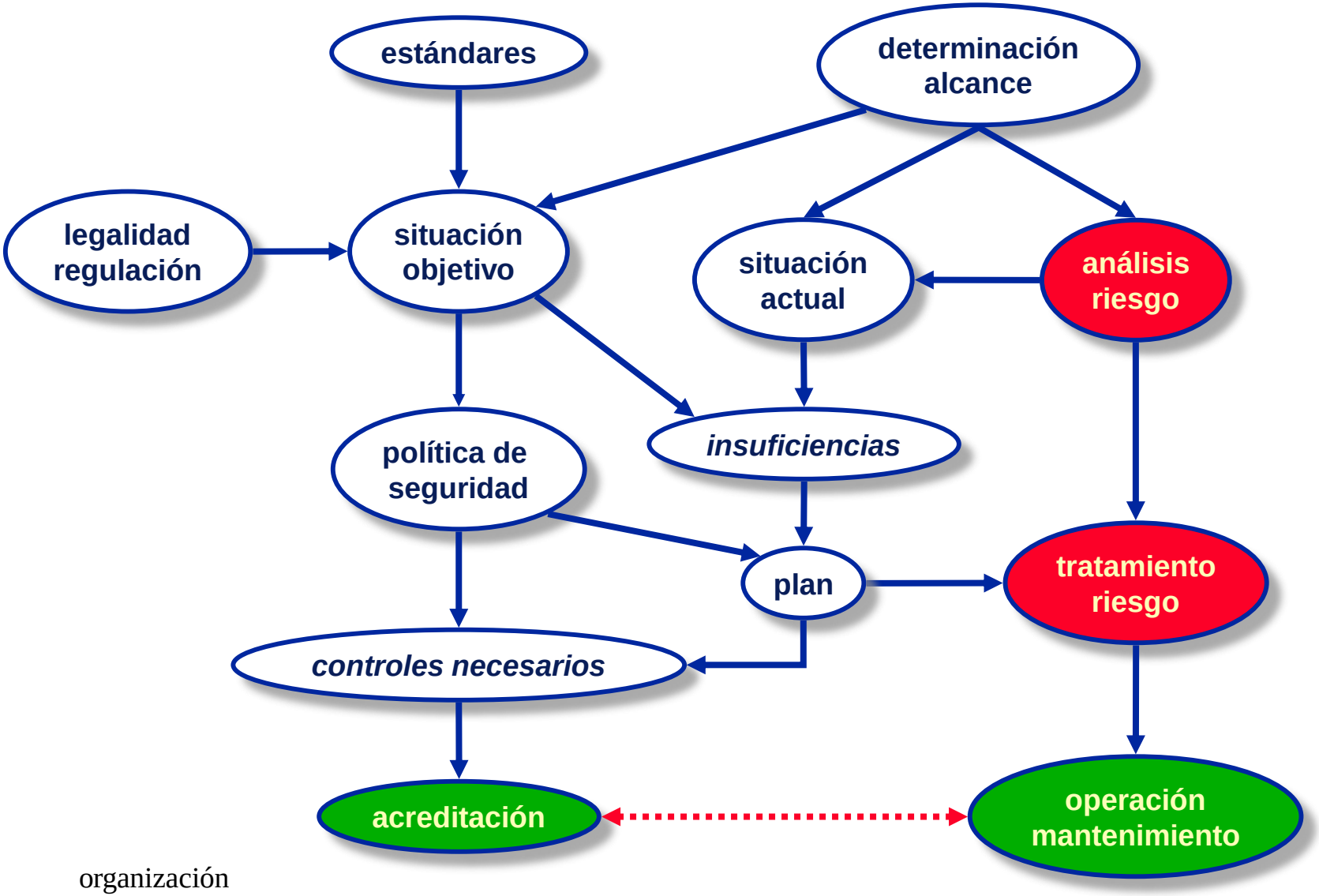
equilibrio valor-coste



Riesgo

- Riesgo
  - el arte de vivir con una razonable seguridad
- Análisis de impacto
  - el arte de estimar las consecuencias de una amenaza potencial
- Análisis de riesgos
  - el arte de estimar las consecuencias recurrentes de la inseguridad residual
- Análisis de riesgos y análisis de impacto
  - proporcionan información para tomar decisiones
- Gestión de riesgos
  - Risk management involves managing to achieve an appropriate balance between realizing opportunities for gains while minimizing losses. [AS/NZS 4360:2004]

Roadmap


estándares
determinación alcance
legalidad regulación
situación objetivo
situación actual
análisis riesgo
política de seguridad
insuficiencias
plan
tratamiento riesgo
controles necesarios
acreditación
operación mantenimiento

ISMS - management system

- set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives
  - Note 1: A management system can address a single discipline or several disciplines.
  - Note 2: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.
  - Note 3: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

SGSI

ISMS – Information Security Management System

SGSI – Sistema de Gestión de la Seguridad de la Información

- Protecting information assets through defining, achieving, maintaining, and improving information security effectively is essential to enable an organization to achieve its objectives, and maintain and enhance its legal compliance and image. These coordinated activities directing the implementation of suitable controls and treating unacceptable information security risks are generally known as elements of information security management.

términos

sistema de gestión de la seguridad de la información (SGSI)

- la parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, hacer funcionar, supervisar, revisar, supervisar, mantener y mejorar la seguridad de la información
- NOTA
  - el sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos

Roles

CISO
Responsable de la Información y de los servicios

Responsable de la seguridad

Responsable de operaciones

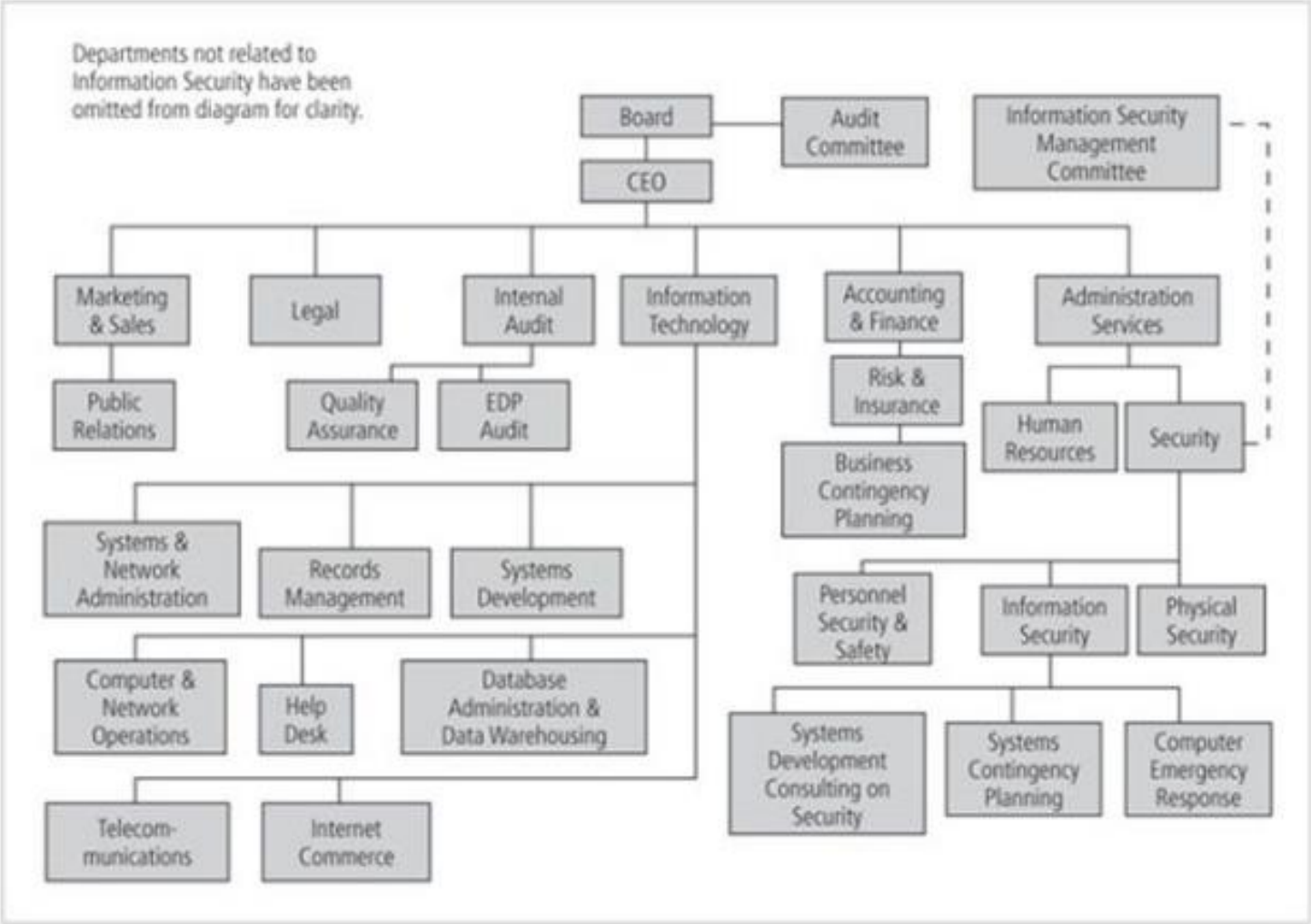
administradores de seguridad

administradores de sistemas

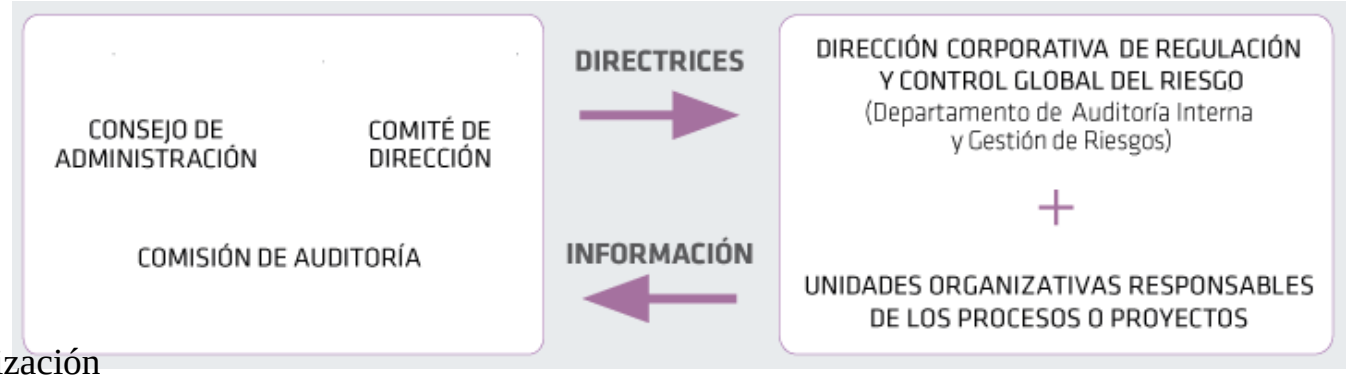
desarrolladores

proveedores

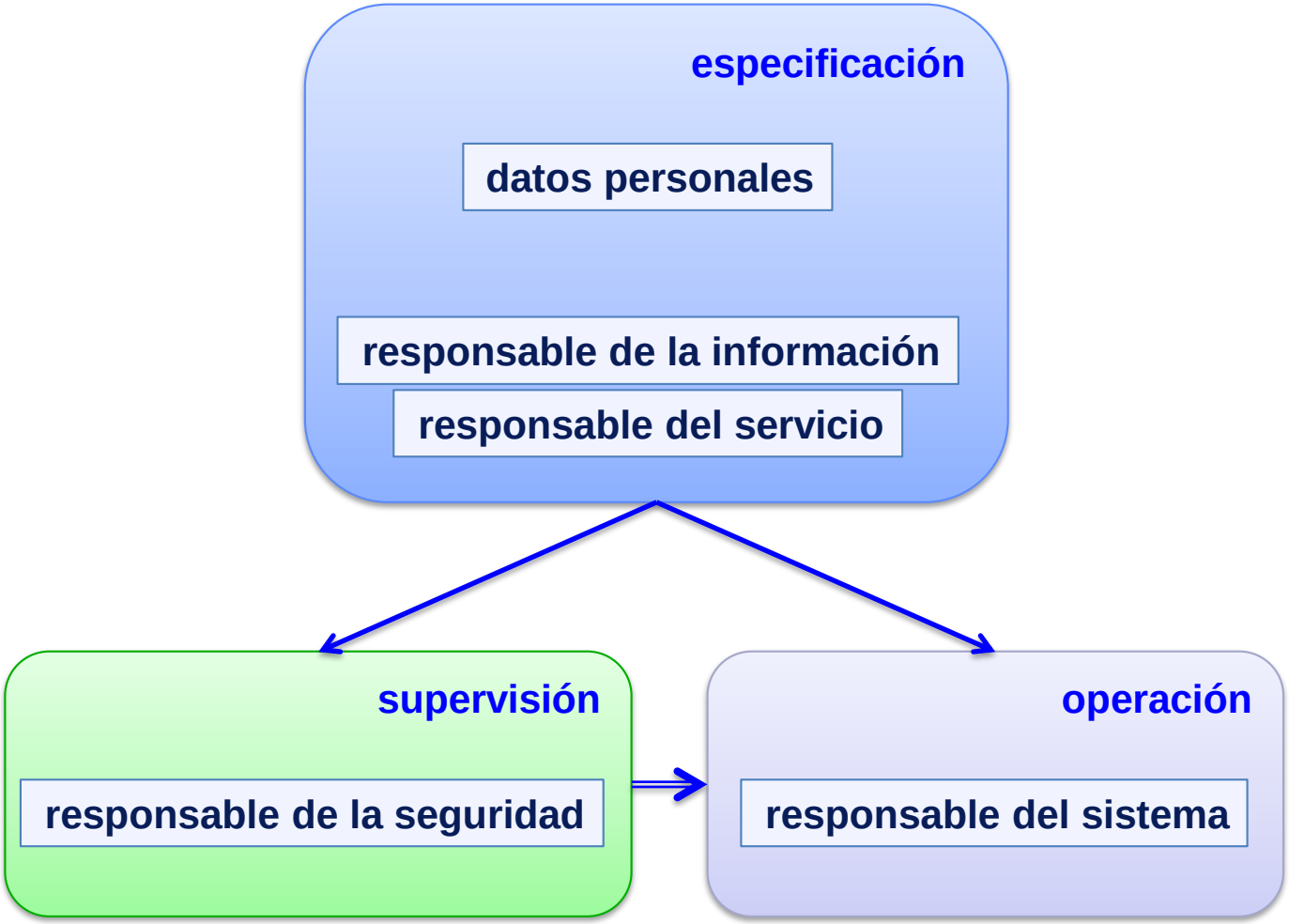
Hay muchas formas de organizarse



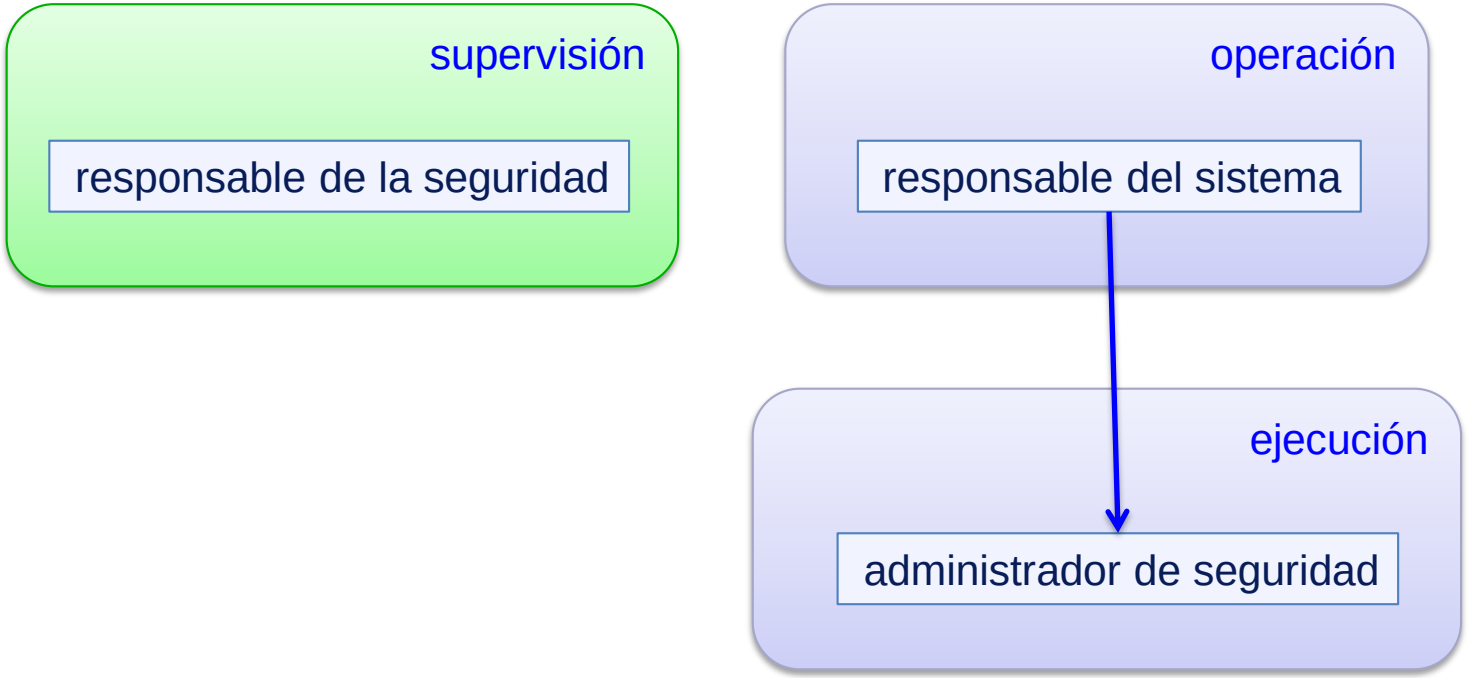
Identificación de Roles



dit


especificación
datos personales
responsable de la información
responsable del servicio
supervisión
responsable de la seguridad
operación
responsable del sistema

dit


supervisión
responsable de la seguridad
operación
responsable del sistema
ejecución
administrador de seguridad

dit

supervisión
responsable de la seguridad
operación
responsable del sistema
ejecución
administrador de seguridad

modelo PDCA

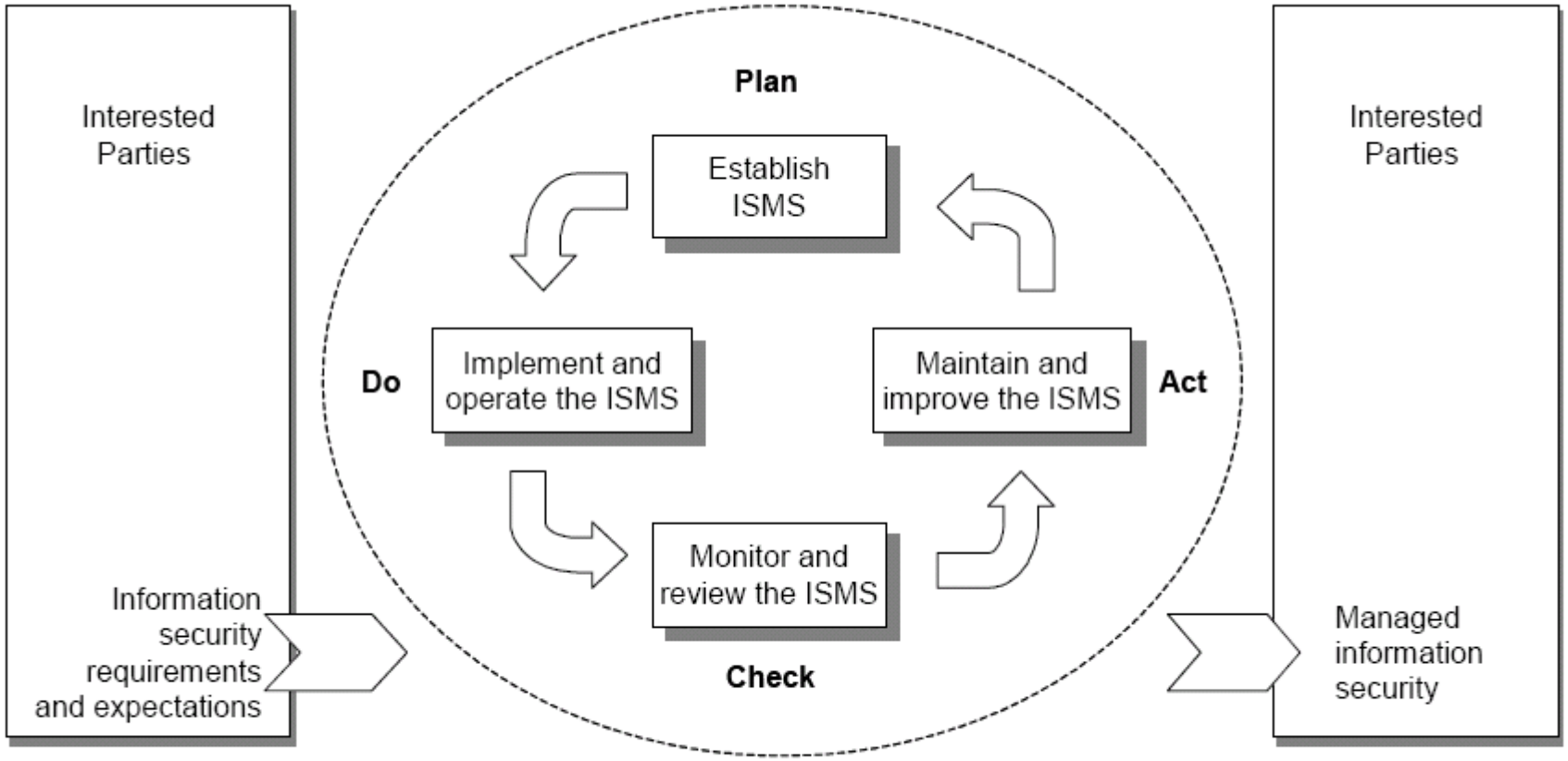


Figure 1 — PDCA model applied to ISMS processes

plan

PLANIFICAR

- administrativo
  - política de seguridad, específica y encajada en la empresa
  - se definen roles y funciones
- “técnico”
  - se define el alcance y el contexto
  - se identifican los riesgos y opciones de tratamiento
  - se decide cómo gestionar los riesgos

dit do

HACER

- se implantan y se operan las medidas de seguridad decididas
- plan de concienciación y formación
- gestión de incidencias
  - detección de incidentes
  - gestión de incidentes

dit

check

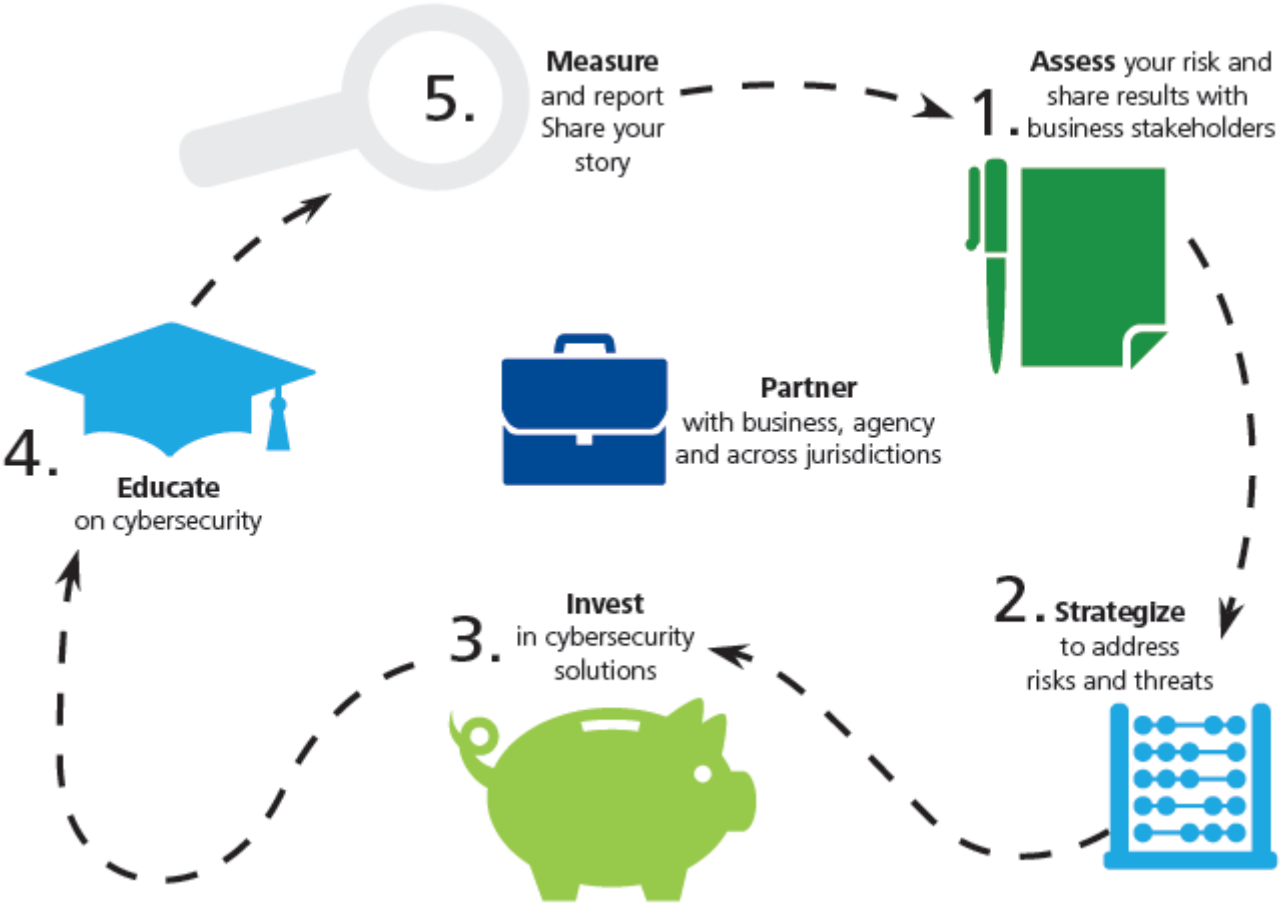
MONITORIZAR

- se revisa la efectividad y eficiencia del sistema implantado
- métricas
- auditorías

ACTUAR

- nos adaptamos a las circunstancias
- nos comunicamos con las partes interesadas
- mejora continua
  - se aprende de los errores
  - se destinan recursos
    - económicos
    - humanos
    - tiempo

te mueves, o caducas



2012 Deloitte-NASCIO Cybersecurity Study

ISO 27000 et al.

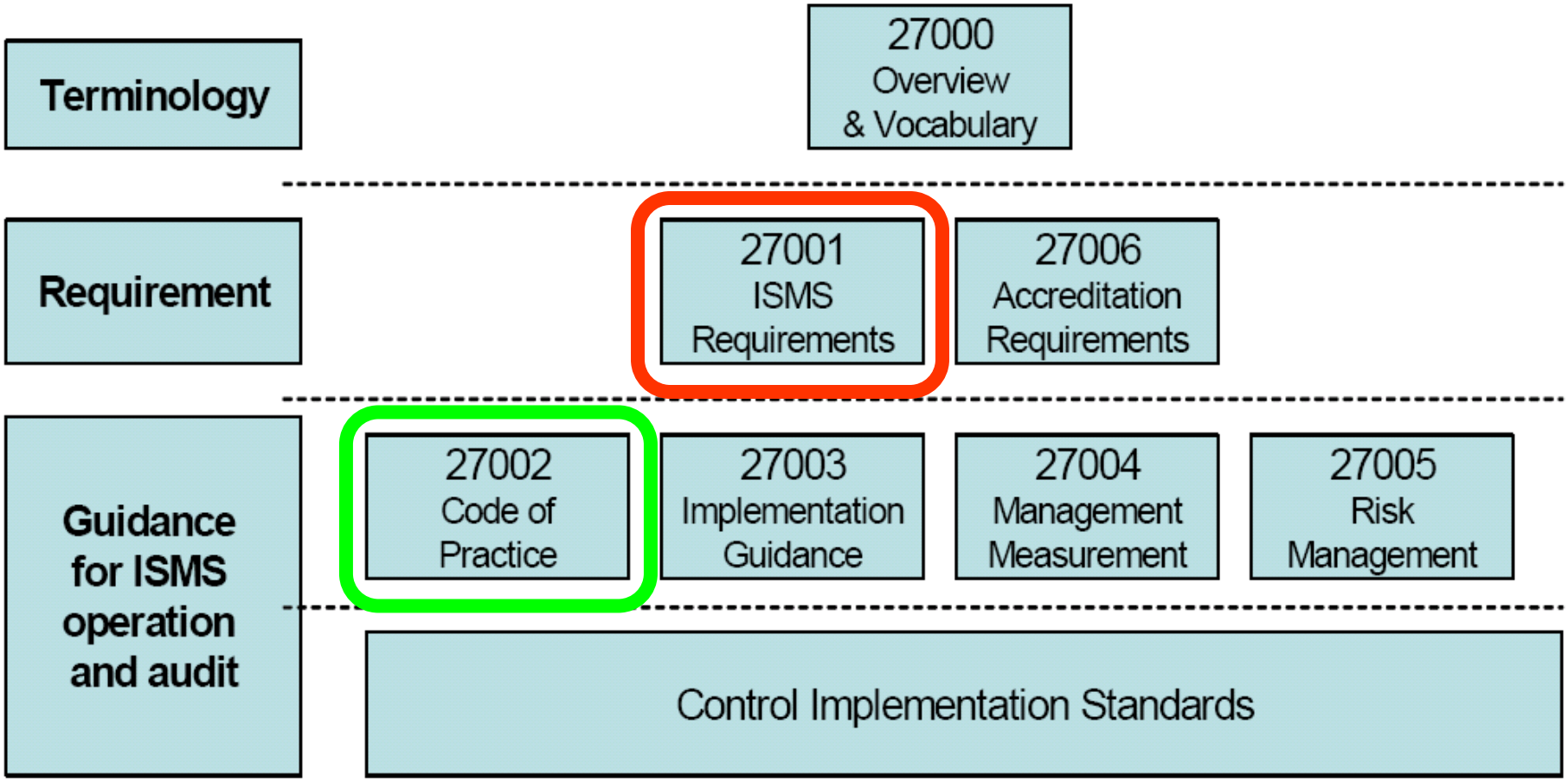


Figure 1: Information Security Standards Structure

ISO 27002:2013

[27002:2013] Código de prácticas para los controles de seguridad de la información
[5] Políticas de seguridad de la información
[6] Organización de la seguridad de la información
[7] Seguridad relativa a los recursos humanos
[8] Gestión de activos
[9] Control de acceso
[10] Criptografía
[11] Seguridad física y del entorno
[12] Seguridad de las operaciones
[13] Seguridad de las comunicaciones
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información
[15] Relación con proveedores
[16] Gestión de incidentes de seguridad de la información
[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio
[18] Cumplimiento

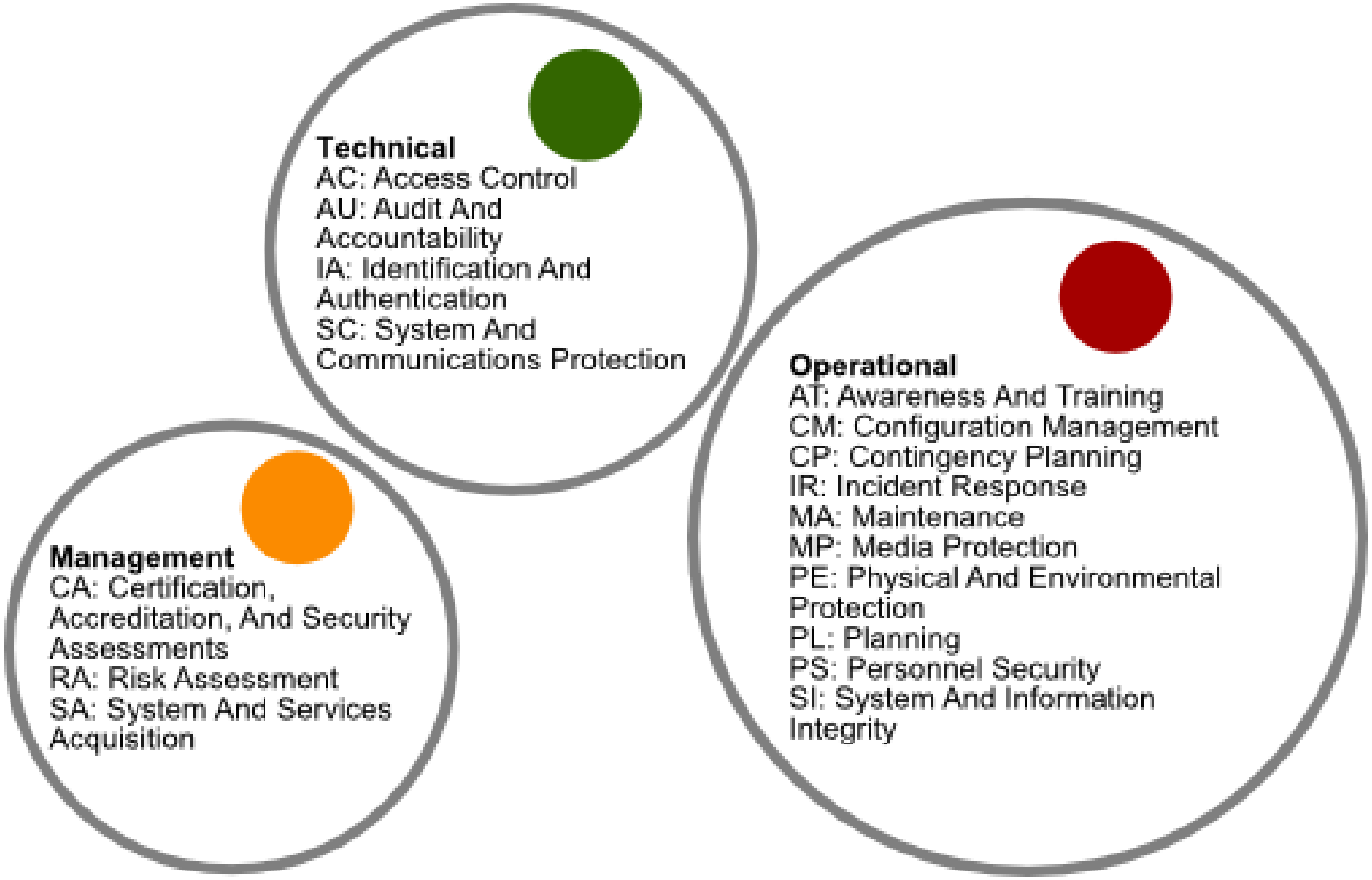
ENS:2015

[ens:2010] Esquema Nacional de Seguridad (10.6.2011)
[org] Marco organizativo
[op] Marco operacional
[op.pl] Planificación
[op.acc] Control de acceso
[op.exp] Explotación
[op.ext] Servicios externos
[op.cont] Continuidad del servicio
[op.mon] Monitorización del sistema
[mp] Medidas de protección
[mp.if] Protección de las instalaciones e infraestructuras
[mp.per] Gestión del personal
[mp.eq] Protección de los equipos
[mp.com] Protección de las comunicaciones
[mp.si] Protección de los soportes de información
[mp.sw] Protección de las aplicaciones informáticas (SW)
[mp.info] Protección de la información
[mp.s] Protección de los servicios

www.pilar-tools.com/doc/ens

SP-800-53

- NIST SP-800-53 rev. 4



Conclusiones

- El SGSI es un proceso formal para gestionar las actividades relacionadas con la seguridad de la información
  - análisis de riesgos
  - flujo de toma de decisiones
  - mantenimiento continuo
  - formalizado y verificable
- Una certificación 27001 es la corroboración oficial de un tercero de que todo lo anterior
  - se hace
  - y es verificable

Conclusiones

- Una certificación 27001
  - no asegura que el sistema es ‘seguro’
  - asegura que la Dirección sabe exactamente el riesgo residual que asume
- Un sistema incapaz de alcanzar la certificación probablemente denota un sistema de comportamiento incierto