#gigatic15

gigaTIC 2015

Congrés de la Governança i la Gestió avançada de les TIC

16 abril - Barcelona

Torre Telefónica - Diagonal 00

ISACA Barcelona Chapter

itSMF España Catalunya

COBIT 5: Transforming Cybersecuriry

Xavier Rubiralta Costa

Sessió 13:05-13:40

#gigaTIC15

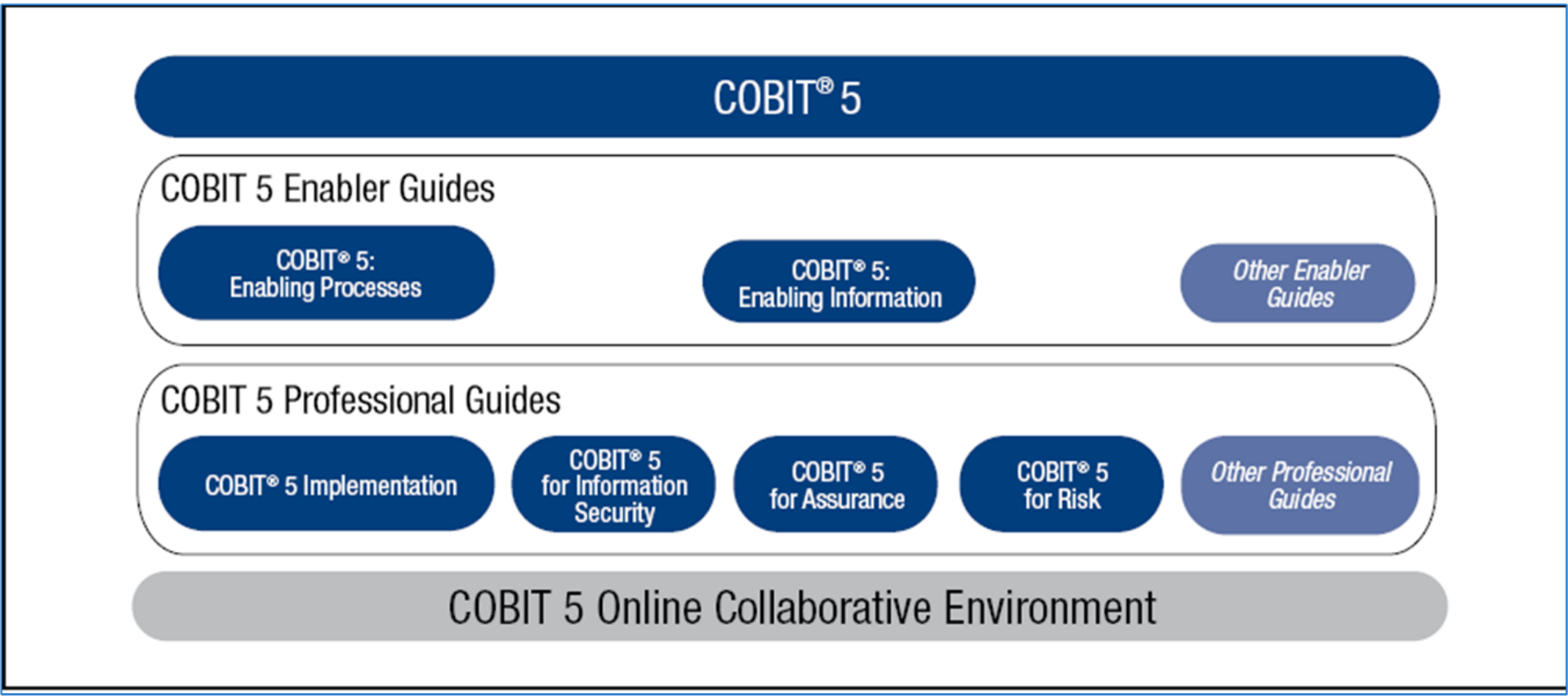
Contenido

- COBIT5 y ciberseguridad
- Amenazas, vulnerabilidades y riesgo
- Gobierno de la ciberseguridad
- Gestión de la ciberseguridad
- Aseguramiento de la ciberseguridad
- Principios para la transformación de la ciberseguridad

COBIT 5 Y CIBERSEGURIDAD

COBIT 5 y Ciberseguridad

- Familia de publicaciones

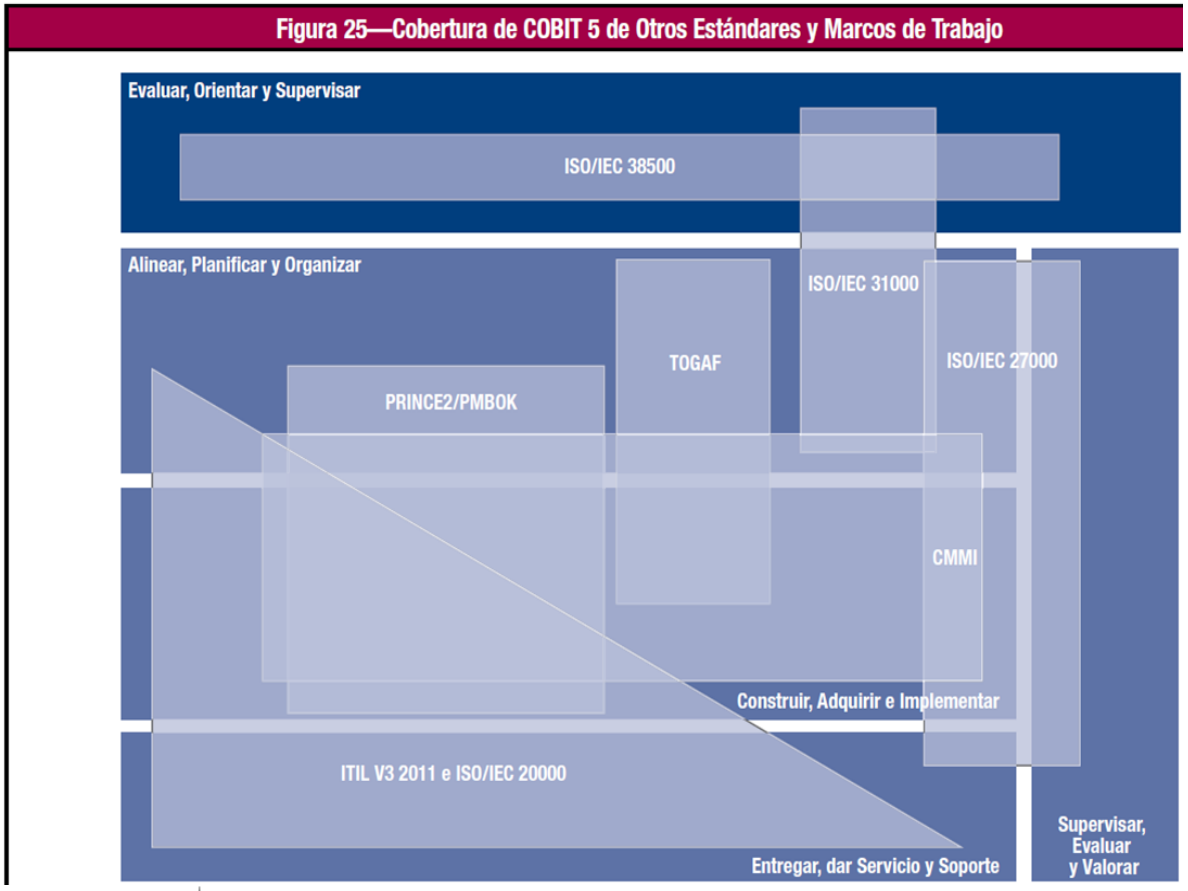


COBIT 5 y Ciberseguridad

- COBIT 5 Transforming Cybersecurity

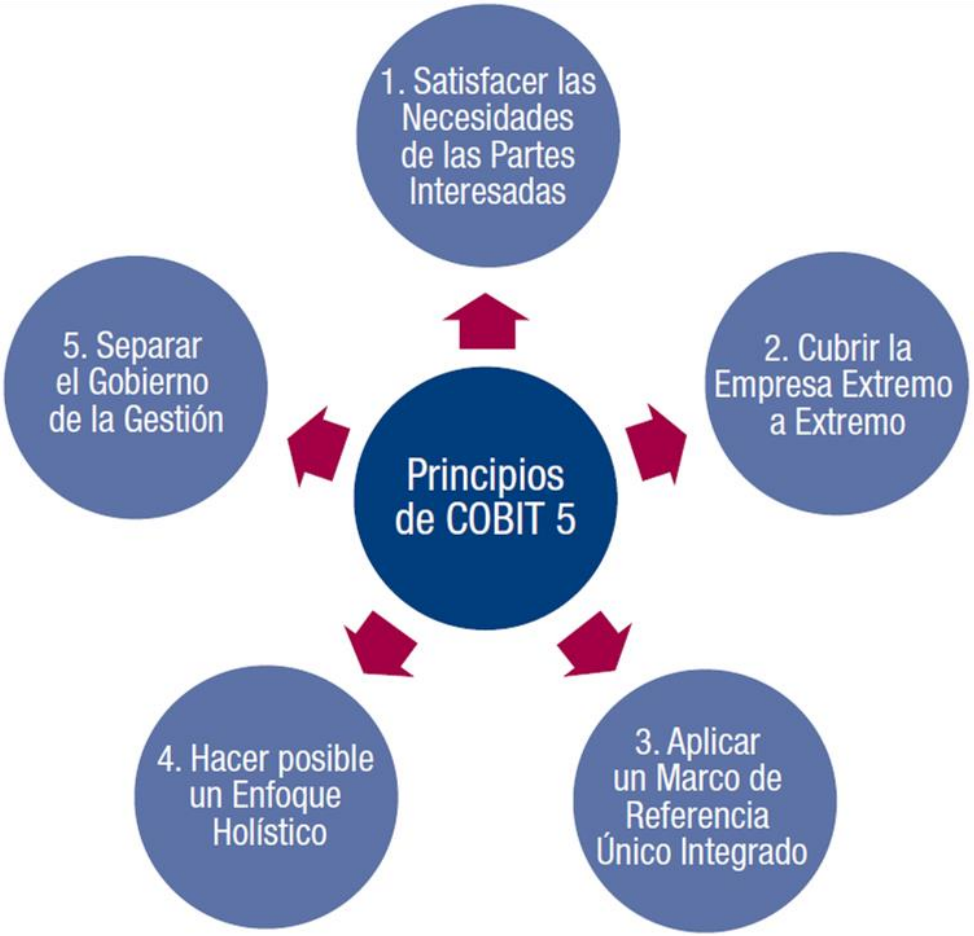
COBIT 5 y Ciberseguridad

- COBIT 5 y otros estándares



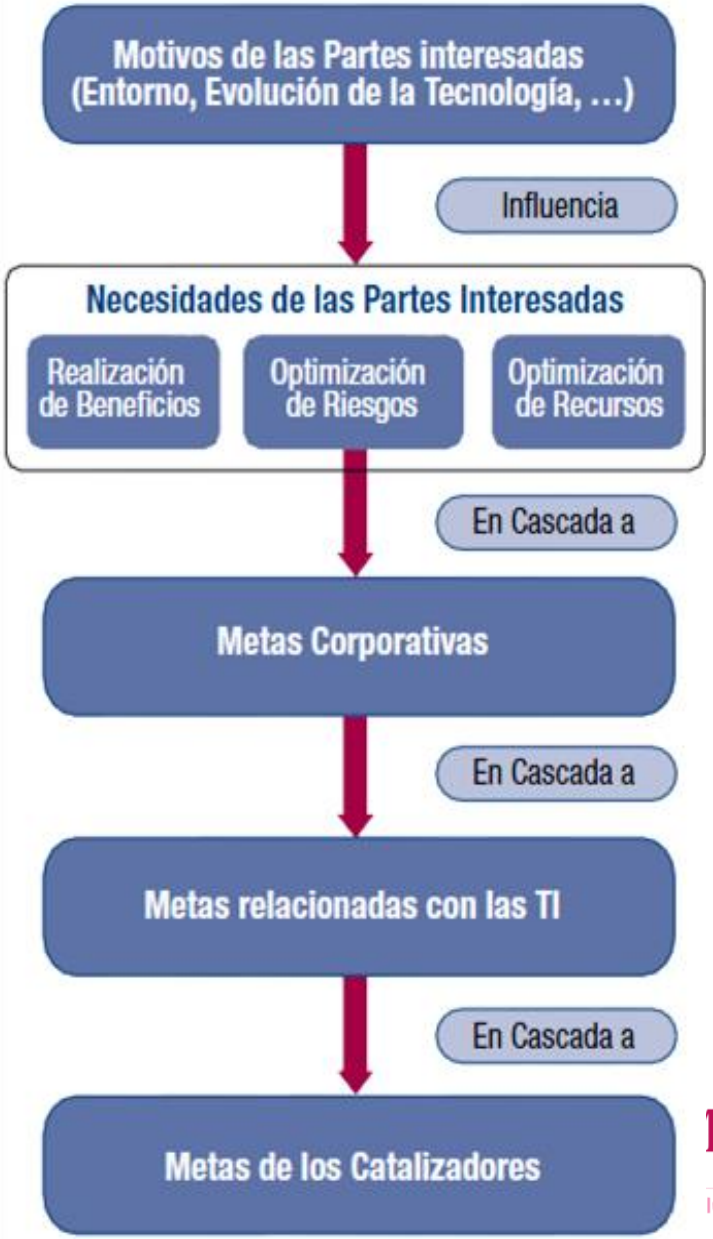
COBIT 5 y Ciberseguridad

- Principios de COBIT 5



COBIT 5 y Ciberseguridad

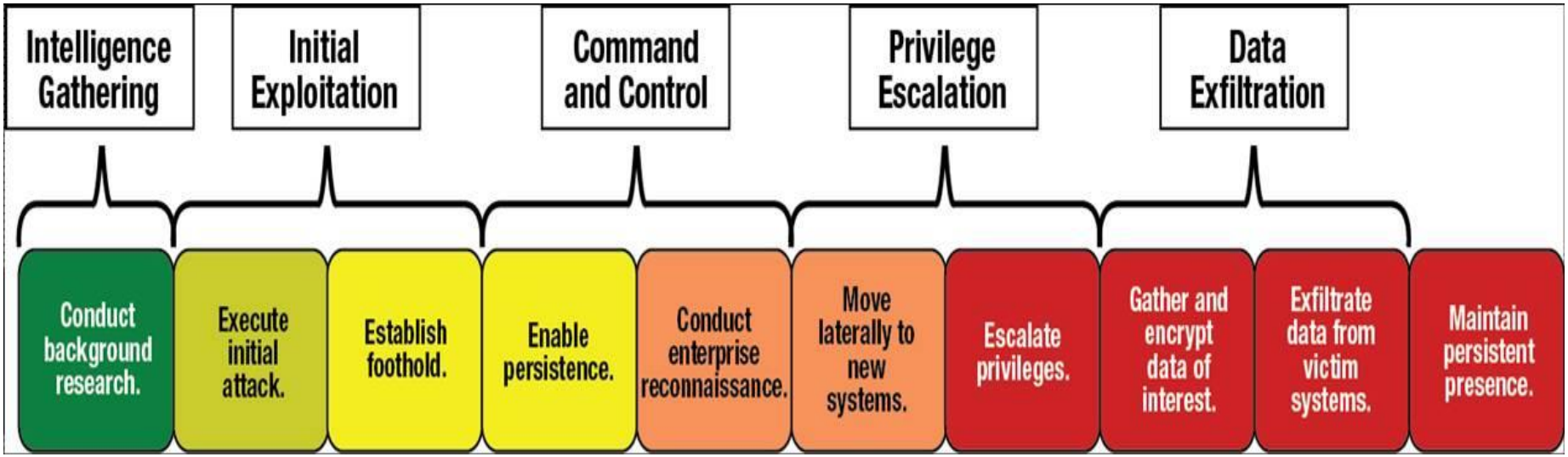
- Cascading



AMANEZAS, VULNERABILIDADES Y RIESGO ASOCIADO

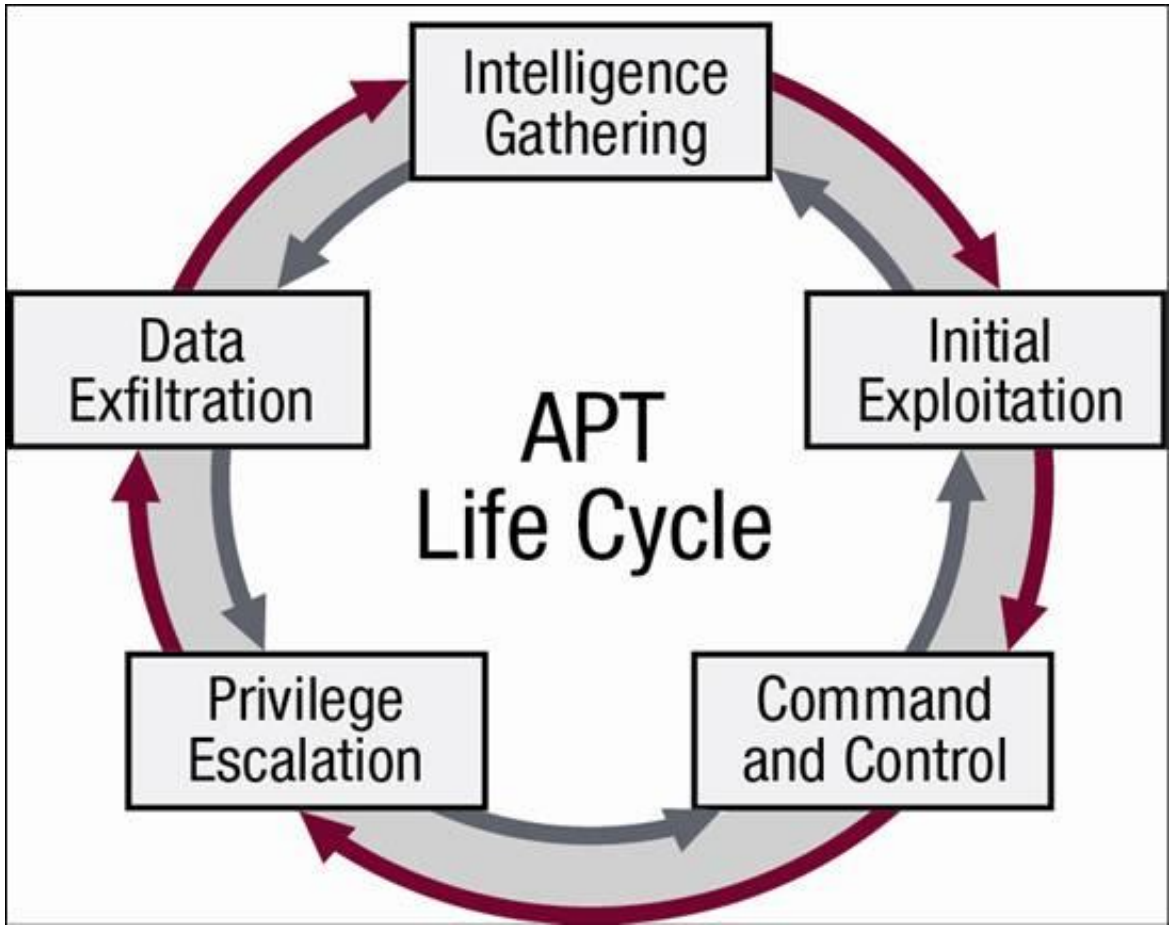
Amenazas, vulnerabilidades y riesgo asociado

- Ciclo de vida de una APT



Amenazas, vulnerabilidades y riesgo asociado

- Ciclo de vida de una APT



Amenazas, vulnerabilidades y riesgo asociado

- Categorización de amenazas y vulnerabilidades
- Identificación de debilidades sistémicas
- Integración de ataques e historia de incidentes
- Riesgo organizacional
  - Diseño organizacional y riesgo estructural
  - Gobierno corporativo, cumplimiento y control del riesgo
  - Riesgo cultural

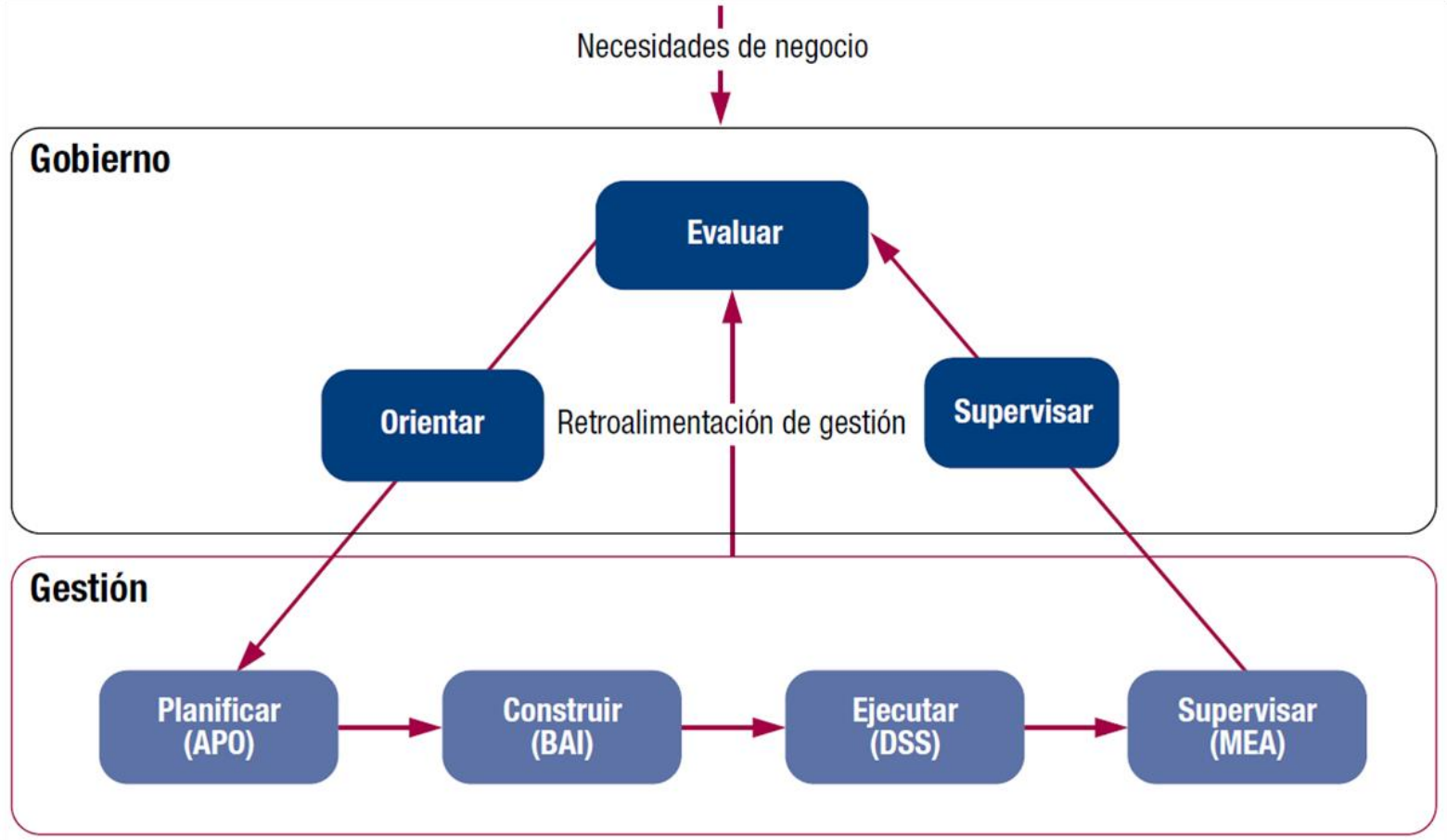
Amenazas, vulnerabilidades y riesgo asociado

- Riesgo social
  - Riesgo en las personas
  - Cultura individual del riesgo
  - Riesgos emergentes
- Riesgo tecnológico
  - Arquitectura
  - Aplicaciones
  - Operaciones
  - Infraestructura

GOBIERNO DE LA CIBERSEGURIDAD

Gobierno de la ciberseguridad

- Diferenciación entre gobierno y gestión



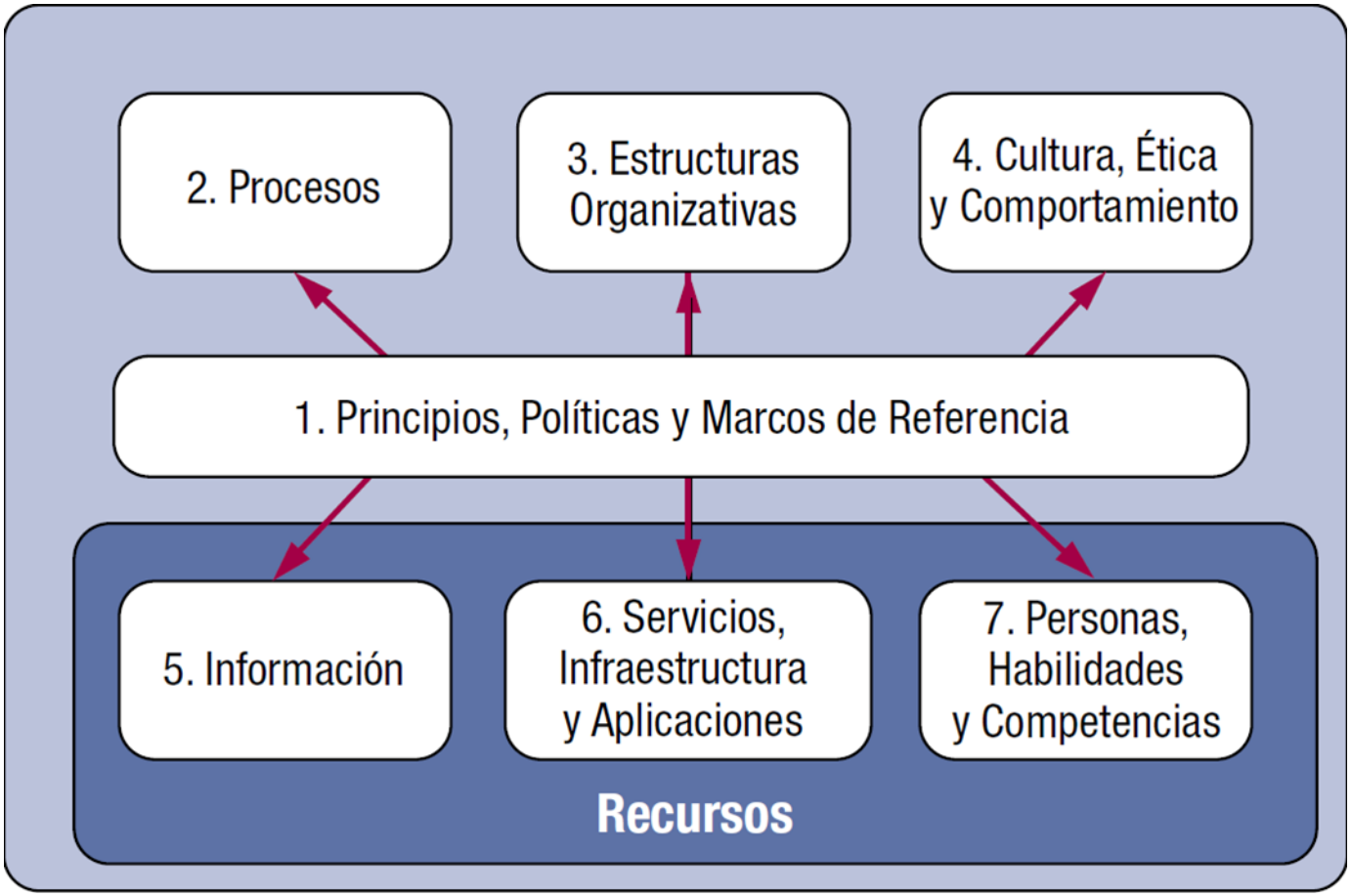
Gobierno de la ciberseguridad

- “Business case”
- Gobernando la transformación de la ciberseguridad
  - Establecer el estado actual y el objetivo
  - Transformación estratégica y sistémica
- Aplicando COBIT5 al gobierno de la ciberseguridad
  - Evaluar, Dirigir y Monitorear (EDM)
  - Alinear, Planificar y organizar (APO)

GESTIÓN DE LA CIBERSEGURIDAD

Gestión de la ciberseguridad

- Facilitadores



Gestión de la ciberseguridad

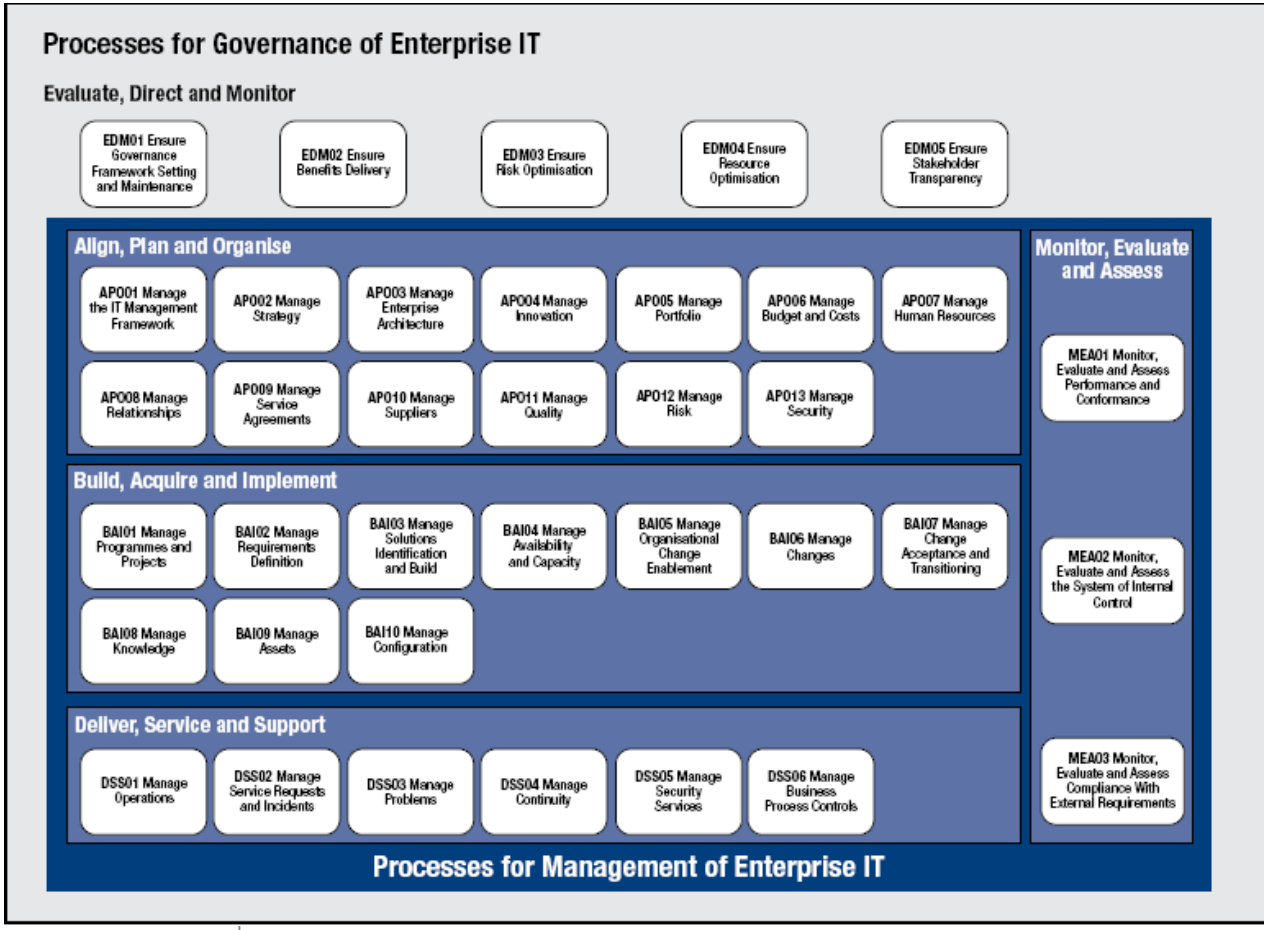
- Principios, políticas y “frameworks”
  - Principios de seguridad de la información
  - Política de seguridad de la información
  - Política de ciberseguridad
  - Norma de gestión de la ciberseguridad
  - Procedimientos clave de operación de ciberseguridad (Key Operation Procedures – KOP)

Gestión de la ciberseguridad

- Procesos
  - Procesos de gestión de seguridad
  - Procesos de monitorización de seguridad
  - Procesos relacionados con la continuidad

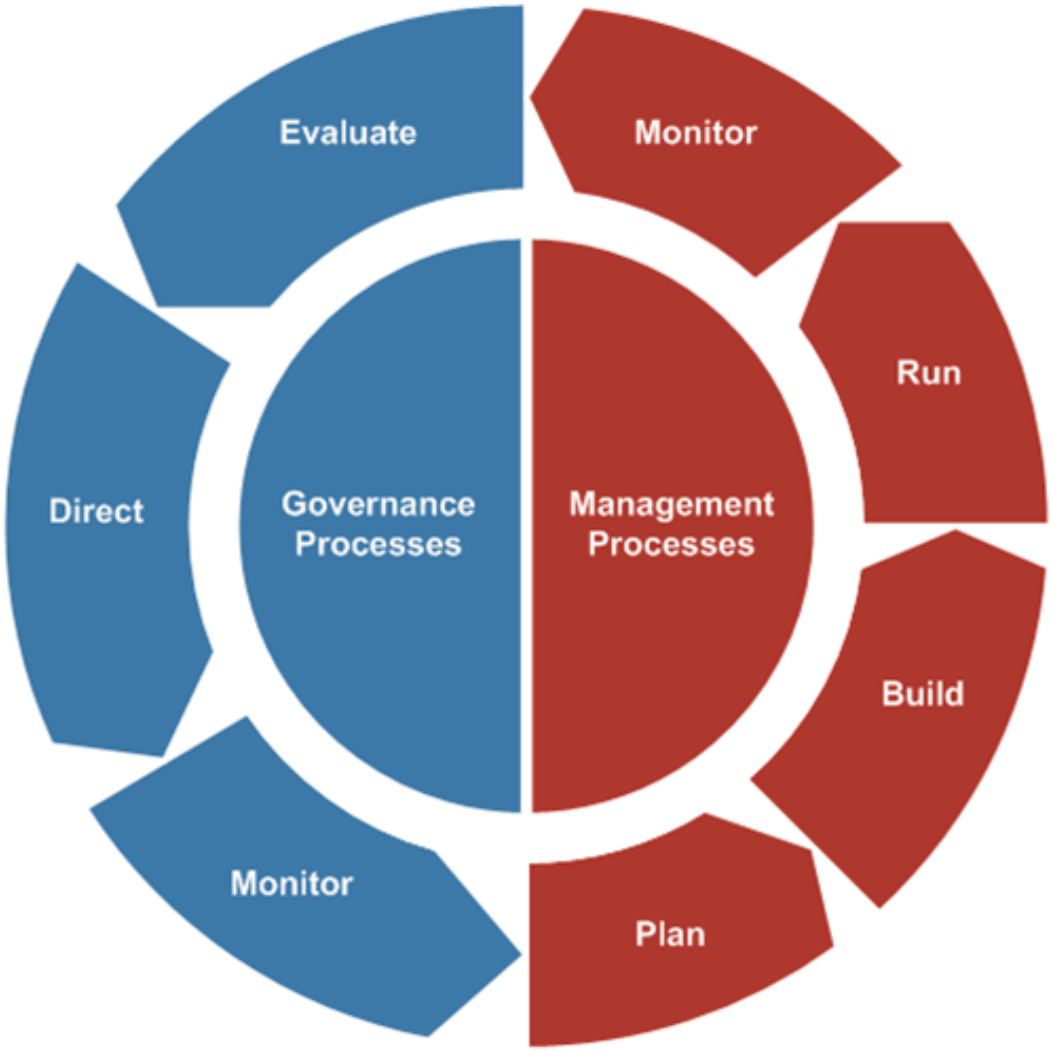
Gestión de la ciberseguridad

- Mapa de procesos



Gestión de la ciberseguridad

- Mapa



Gestión de la ciberseguridad

- Estructuras organizacionales
  - Dependencia de la función
  - Rol de Gestor de seguridad de la información
  - Rol de especialista en ciberseguridad
  - Interconexión entre ciberseguridad y otras funciones de la organización

Gestión de la ciberseguridad

- Cultura, ética y comportamiento
  - Defínción de modelos de comportamiento
  - Operación diaria
  - Importancia de principios y políticas
  - Guía suficiente y detallada
  - Responsabilidad
  - Concienciación sobre amenazas de los diferentes grupos de interés (stakeholders)
  - Soporte a la innovación
  - Reconocimiento de la Dirección Ejecutiva

Gestión de la ciberseguridad

- Información
  - Protección de la información sensible
  - Protección de la información personal
  - Protección de la información en la nube

Gestión de la ciberseguridad

- Servicios, infraestructura y aplicaciones
  - Arquitectura de seguridad
  - Concienciación en seguridad
  - Desarrollo seguro
  - Configuración y securización de sistemas
  - Accesos alineados con las funciones
  - Protección ante malware y ataques
  - Respuesta a incidentes adecuada
  - Monitorización de eventos de seguridad

Gestión de la ciberseguridad

- Personas, habilidades y competencias
  - Capacitación en gestión de la seguridad
  - Capacitación de los usuarios finales
  - Formación en ciberseguridad

ASEGURAMIENTO DE LA CIBERSEGURIDAD

Aseguramiento de la ciberseguridad

- Auditoría y revisión de la ciberseguridad:
  - Universo de la auditoría
  - Objetivos de la auditoría
  - Planificación y alcance
  - Consideraciones legales
  - Privacidad y protección de datos
  - “Logging”, retención de datos y archivo
  - Almacenamiento de los datos de auditoría

Aseguramiento de la ciberseguridad

- Investigaciones en ciberseguridad y "Forensics":
  - Requerimientos de investigación
  - Conflictos con la privacidad
  - Enfoque de investigación: Ex Post
  - Enfoque de investigación: Tiempo real
  - Cadena de custodia
  - "E-discovery"

PRINCIPIOS PARA LA TRANSFORMACIÓN DE LA CIBERSEGURIDAD

gigaTIC 15

itSMF ESPAÑA Catalunya

ISACA Barcelona Chapter

Principios para la transformación de la ciberseguridad

- Principios (I):
  1. Conocer el impacto potencial del cibercrimen
  2. Entender a los usuarios finales, sus valores culturales y sus patrones de comportamiento
  3. Enunciar el “business case” para la ciberseguridad y el “apetito” de riesgo de la organización
  4. Establecer el gobierno de la ciberseguridad

Principios para la transformación de la ciberseguridad

- Principios (II):
  5. Gestionar la ciberseguridad utilizando los principios y los catalizadores
  6. Conocer el universo y los objetivos de aseguramiento de la ciberseguridad
  7. Proveer un aseguramiento razonable sobre la ciberseguridad
  8. Establecer y evolucionar una ciberseguridad sistémica

Sessió 13:05-13:40

COBIT 5: Transforming Cybersecurity

Detalls Contacte

ISACA
Trust in, and value from, information systems
Barcelona Chapter

Nom del ponent

Xavier Rubiralta Costa

Adreça Correu

xavier.rubiralta@isacabcn.org

Telèfon Contacte

Twitter