



Seguridad, Riesgo Tecnológico e IT Governance

Nuevos retos y nuevos roles

Contenido



- ▶ Historia de la función de Seguridad
- ▶ Seguridad en Riesgo tecnológico
- ▶ Seguridad en Gobierno de IT
- ▶ Conclusiones



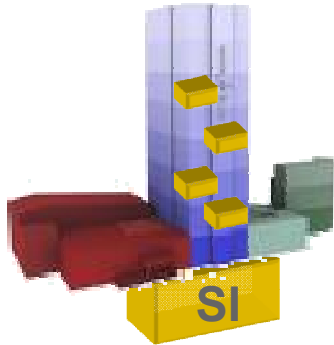
Historia de la función de Seguridad

Algo de historia el comienzo



- ▶ **Los Sótanos (antes 90's)**
 - ▶ Entorno
 - ▶ Centralizado
 - ▶ Ubicación
 - ▶ Explotación de sistemas centrales
 - ▶ Reporte
 - ▶ Bajo el área de TI
 - ▶ Funciones
 - ▶ Política de seguridad (?)
 - ▶ Administración de usuarios y contraseñas
 - ▶ Perfil
 - ▶ Técnicos especializados

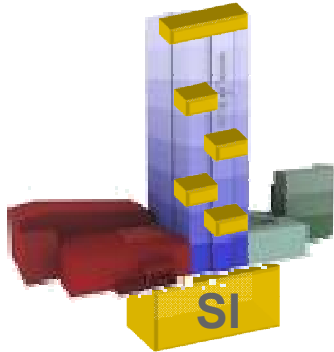
Algo de historia la luz



▶ La plantas de oficina (1995)

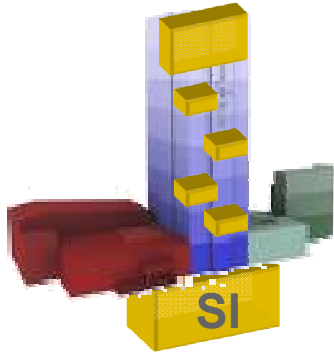
- ▶ Entorno
 - ▶ Distribuido: entorno cliente – servidor. Internet
 - ▶ Dependencia del negocio en los sistemas
- ▶ Ubicación
 - ▶ Seguridad Informática
- ▶ Reporte
 - ▶ Área de TI – Staff de Dirección TI
- ▶ Funciones
 - ▶ Política de seguridad
 - ▶ Análisis de riesgos
 - ▶ Administración de usuarios y contraseñas
 - ▶ Gestión de amenazas y vulnerabilidades
- ▶ Perfil
 - ▶ Técnicos

Algo de historia la presión



- ▶ **Los pisos altos (2000 - 2004)**
 - ▶ Entorno
 - ▶ Distribuido: entorno cliente – servidor. Internet. Intranet
 - ▶ Incrementa dependencia del negocio en los sistemas
 - ▶ Presión regulatoria (protección de datos y privacidad)
 - ▶ Ubicación
 - ▶ Seguridad Informática
 - ▶ Reporte
 - ▶ Área de TI – Staff de Dirección TI
 - ▶ Interlocución áreas de negocio
 - ▶ Funciones
 - ▶ Política de seguridad
 - ▶ Análisis y gestión de riesgos
 - ▶ Administración de usuarios y contraseñas
 - ▶ Gestión de amenazas y vulnerabilidades
 - ▶ Protección de datos y privacidad. Auditoría
 - ▶ Perfil
 - ▶ Técnicos. Gestión.

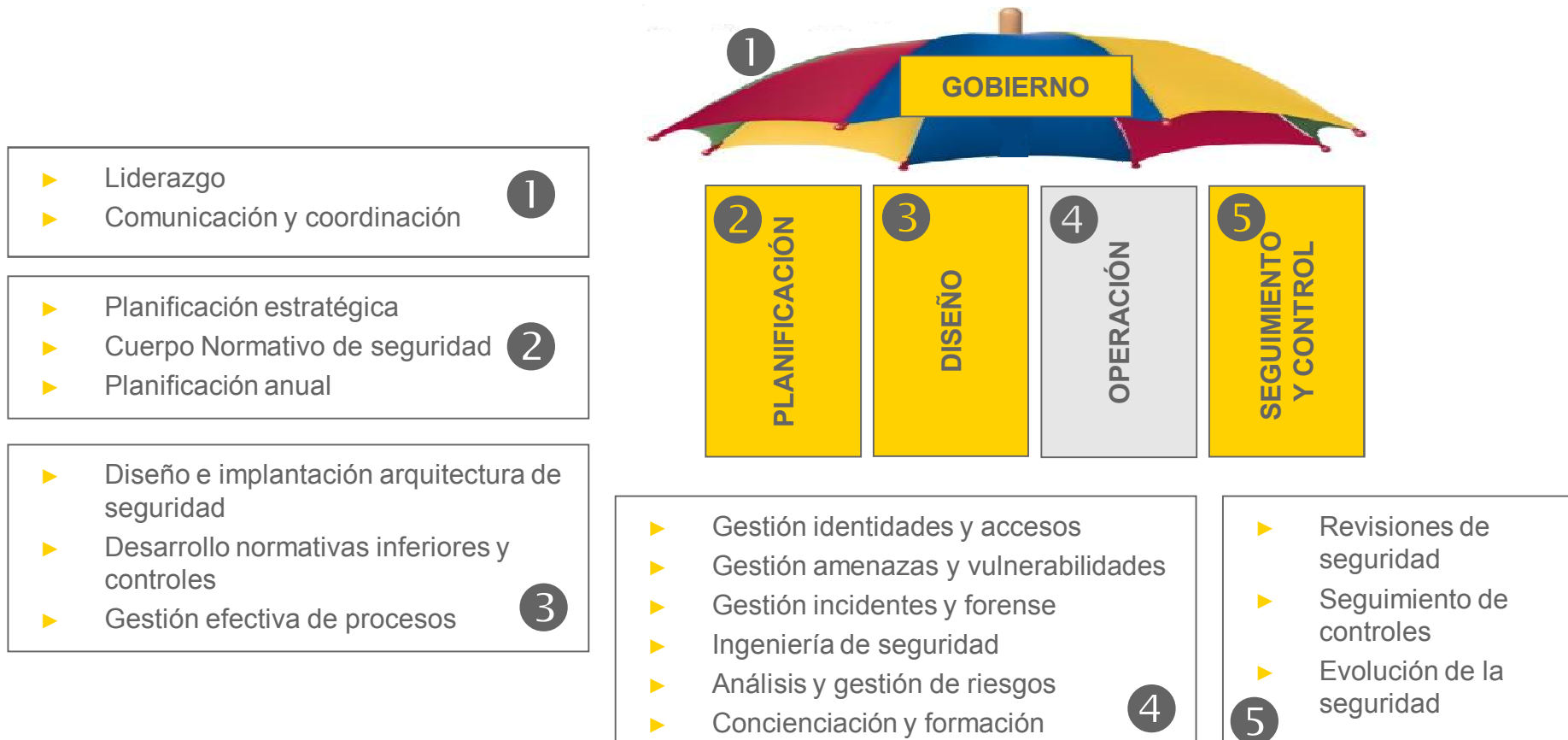
Algo de historia el momento actual



- ▶ **Las alturas (2007 -)**
 - ▶ Entorno
 - ▶ Distribuido. Internet. Intranet. Extranet
 - ▶ Globalización. Crecimientos por adquisición
 - ▶ Elevada dependencia del negocio en los sistemas
 - ▶ Presión regulatoria: cross y sectorial
 - ▶ Eficacia y eficiencia
 - ▶ Ubicación
 - ▶ Seguridad Informática / de la Información
 - ▶ Reporte
 - ▶ Área de TI – Staff de Dirección TI
 - ▶ Seguridad corporativa
 - ▶ Riesgos Corporativos
 - ▶ Funciones
 - ▶ Política de seguridad
 - ▶ Análisis y gestión de riesgos
 - ▶ Gestión de identidades y amenazas
 - ▶ Cumplimiento normativo
 - ▶ Gestión de incidentes y forense
 - ▶ Perfil
 - ▶ Técnicos. Gestión. Comerciales (COMUNICACIÓN)

¿A qué se dedica Seguridad?

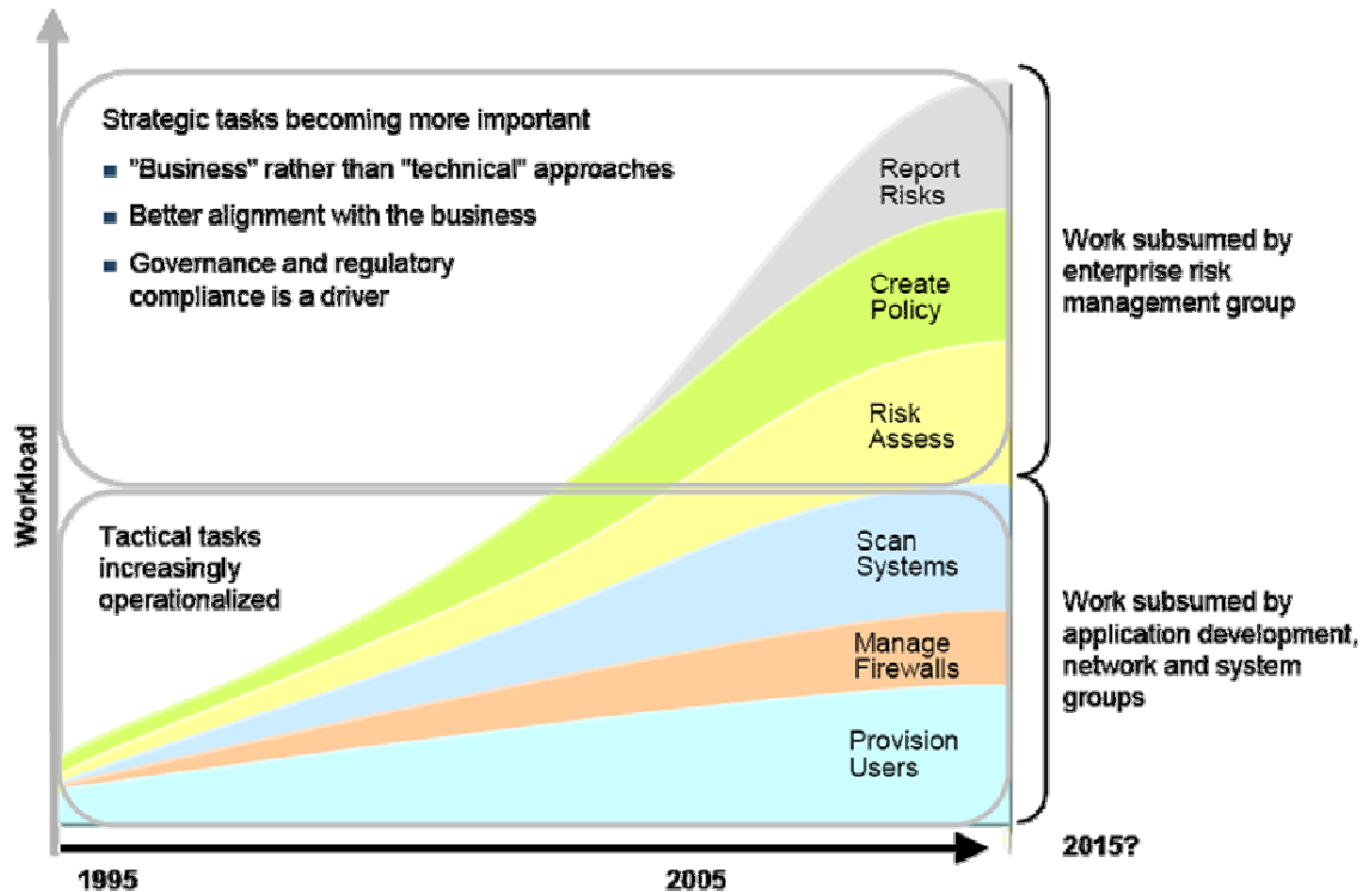
La seguridad es un **SERVICIO** soportado por un conjunto de macro-procesos



¿A qué se dedica Seguridad?

Figure 1. Movement of Information Security Teams

Fuente: Gartner, Feb 2007



448892



Seguridad en Riesgo Tecnológico

Reto a corto: Riesgo Tecnológico



Mapa de Riesgos IT

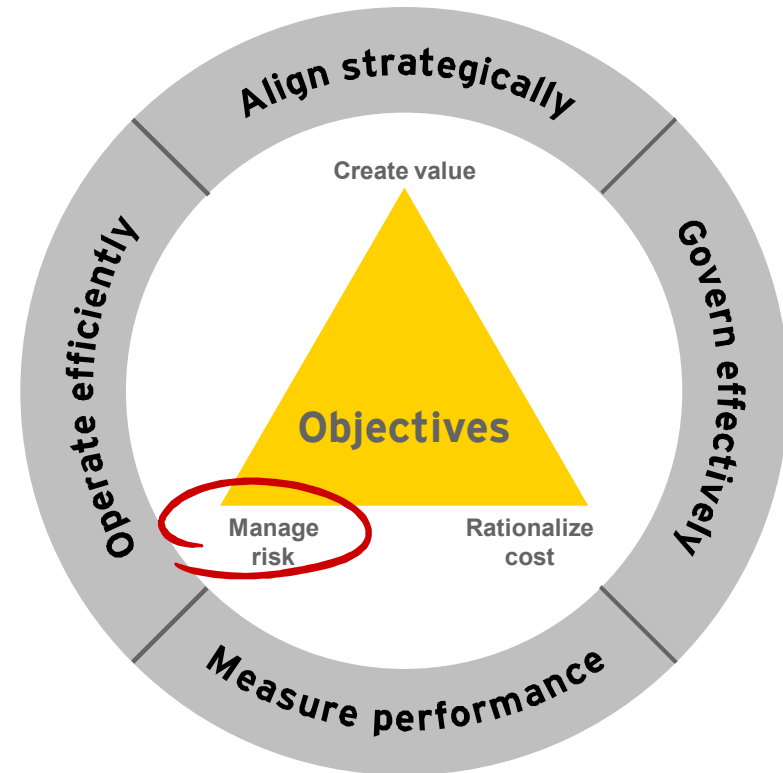




Seguridad en Gobierno de IT

Reto a medio: Gobierno de IT

- ▶ **Como afectan las IT a su negocio?**
 - ▶ *Valor* – como crean valor las IT para la empresa?
 - ▶ *Coste* – como ayudan las IT a racionalizar los costes totales del negocio?
 - ▶ *Riesgo* – como ayudan las IT a gestionar la posición de riesgo del negocio?
- ▶ Sabemos que para que las IT creen un impacto positivo en el negocio, existen 4 necesidades referentes a IT:
 - ▶ Alineación estratégica
 - ▶ Gobernar con efectividad
 - ▶ Operar eficientemente
 - ▶ Medir el rendimiento



¿Cómo podemos medir el valor para la empresa?

Gobierno de IT: Framework de procesos

Managing IT like a business

- ITG** IT Leadership and Governance
- BPM** Business Process Management
- BP** Business Planning
- SP** Strategic Planning
- DSM** Demand and Supply Management
- CFP** Capacity Forecasting and Planning
- RM** Risk Management
- AA** Accounting and Allocation
- ODP** Organisation Design and Planning
- SRC** Sourcing
- REM** Resource Management
- IM** Innovation Management
- PQM** Performance and Quality Management
- SAI** Service Analytics and Intelligence

Managing the IT budget

- FF** Funding and Financing
- BGM** Budget Management
- PPP** Portfolio Planning and Prioritisation
- BOP** Budget Oversight and Performance Analysis

Managing the IT capability

- EAM** Enterprise Architecture Management
- TIM** Technical Infrastructure Management
- PAM** People Asset Management
- ICM** Intellectual Capital Management
- RAM** Relationship Asset Management
- RDE** Research, Development and Engineering
- SD** Solutions Delivery
- SRP** Service Provisioning
- UMT** User Management and Training
- UED** User Experience Design
- PPM** Program and Project Management
- SUM** Supplier Management
- VCM** Value Chain Management
- CAM** Capability Assessment and Management

Managing IT for business value

- TCO** Total Cost of Ownership
- BAR** Benefits Assessment and Realisation
- PM** Portfolio Management
- IAP** Investment Analysis and Performance



Conclusiones

Algunas reflexiones.....

- ▶ La función de **Riesgo Tecnológico**
 - ▶ Existe únicamente en algunos sectores
 - ▶ Es inmadura y con un ámbito de actuación muy acotado
 - ▶ Convergencia normativa mediante controles técnicos
 - ▶ Seguridad de la información
 - ▶ Continuidad de servicio IT
 - ▶ Procesos de Service delivery de forma parcial
 - ▶ Principales barreras
 - ▶ Gestión de riesgos corporativos trabajando mediante silos
 - ▶ No existen taxonomías de riesgos globales para tener un lenguaje común
 - ▶ Modelos de seguimiento y reporting descentralizado
 - ▶ Visión parcial y sesgada de riesgos
 - ▶ Modelo organizativo y dependencias funcionales inadecuadas
 - ▶ Skills de gestión (comunicación) y no técnicas

Algunas reflexiones (2)

- ▶ El **Gobierno de IT**
 - ▶ ¿Cómo afrontar este reto sin consolidar antes la función de riesgo tecnológico?
 - ▶ Principales barreras
 - ▶ Madurar la función de Riesgo tecnológico
 - ▶ Conocimiento profundo del negocio para valorar el alineamiento con el negocio



GRACIAS