CII
Centro de Investigación en Informática

TECNOLÓGICO DE MONTERREY.

7 FORO INTERNACIONAL EN APLICACIONES DE TECNOLOGÍAS DE INFORMACIÓN

"NUEVOS ENFOQUES DE LA INFORMÁTICA"

Estrategias de Seguridad y Normatividad

José Ángel Peña Ibarra
japi@ccisa.com.mx

Contenido

1. Necesidades de seguridad en TI.
2. Estrategias de seguridad:
   Aplicación de estándares.
3. Administración de riesgos.

Contenido

1. Necesidades de seguridad en TI.
2. Estrategias de seguridad:
   Aplicación de estándares.
3. Administración de riesgos.

Importancia creciente de TI

- Las aplicaciones de la tecnología de información no son un "nice to have".
- La mayoría de los procesos críticos de una organización, dependen de aplicaciones de TI y en algunos casos éstas forman una segunda o primera línea de producción.
- La información que se maneja en una empresa es uno de los principales activos de la misma.
- Cualquier afectación de las aplicaciones de TI o de la información que estas manejan, puede impactar seriamente **la operación de una organización.**

Incremento del riesgo por el medio ambiente tecnológico y de negocios

- Las aplicaciones de la tecnología de información han evolucionado de ambientes protegidos a ambientes promiscuos.
- Las aplicaciones de negocio utilizando internet son cada vez más frecuentes.
- Él uso de las tecnologías de comunicación inalámbricas se incrementará grandemente, creando peligrosas puertas de acceso a una organización.
- Las cadenas de valor hacen más frecuente el intercambio de información entre las organizaciones.

Incremento del riesgo por vulnerabilidades internas

- La mayoría de las organizaciones no cuenta con una adecuada cultura de seguridad.

Por ejemplo:

- **72% de todos los negocios tienen alguna de estas condiciones:**
  - No tienen Plan de Continuidad del Negocio.
  - Si lo tienen, nunca lo han probado.
  - Su Plan falló cuándo lo probaron.
- **Solamente 18% de los datos de usuario final están protegidos. ***

*VERITAS Disaster Recovery Survey 2002.

Incremento del riesgo por vulnerabilidades internas

- Muchos administradores de TI han llegado a su nivel de incompetencia.
- Han dejado de ser buenos técnicos para ser malos gerentes.

Por ejemplo:

- **La gran mayoría de los responsables de TI no está capacitado en control interno:**
  - No conocen lo que es **CobiT**.
  - No definen controles en el desarrollo de las aplicaciones
  - No son buenos en control de proyectos.
  - Manejan la seguridad en forma reactiva.

Contenido

1. Necesidades de seguridad en TI.
2. Estrategias de seguridad: Aplicación de estándares.
3. Administración de riesgos.

Estándares en TI

- La aplicación de estándares es una buena estrategia en seguridad y control.
- ISO 17799
- CobiT
- ITIL

ISO 17799

- El conjunto de recomendaciones **ISO 17799**, fue desarrollado por la ISO, con el propósito de contar con un conjunto de mejores prácticas en el campo de seguridad de la información.

- El **ISO 17799** incluye 10 dominios.

Marco Metodológico ISO 17799

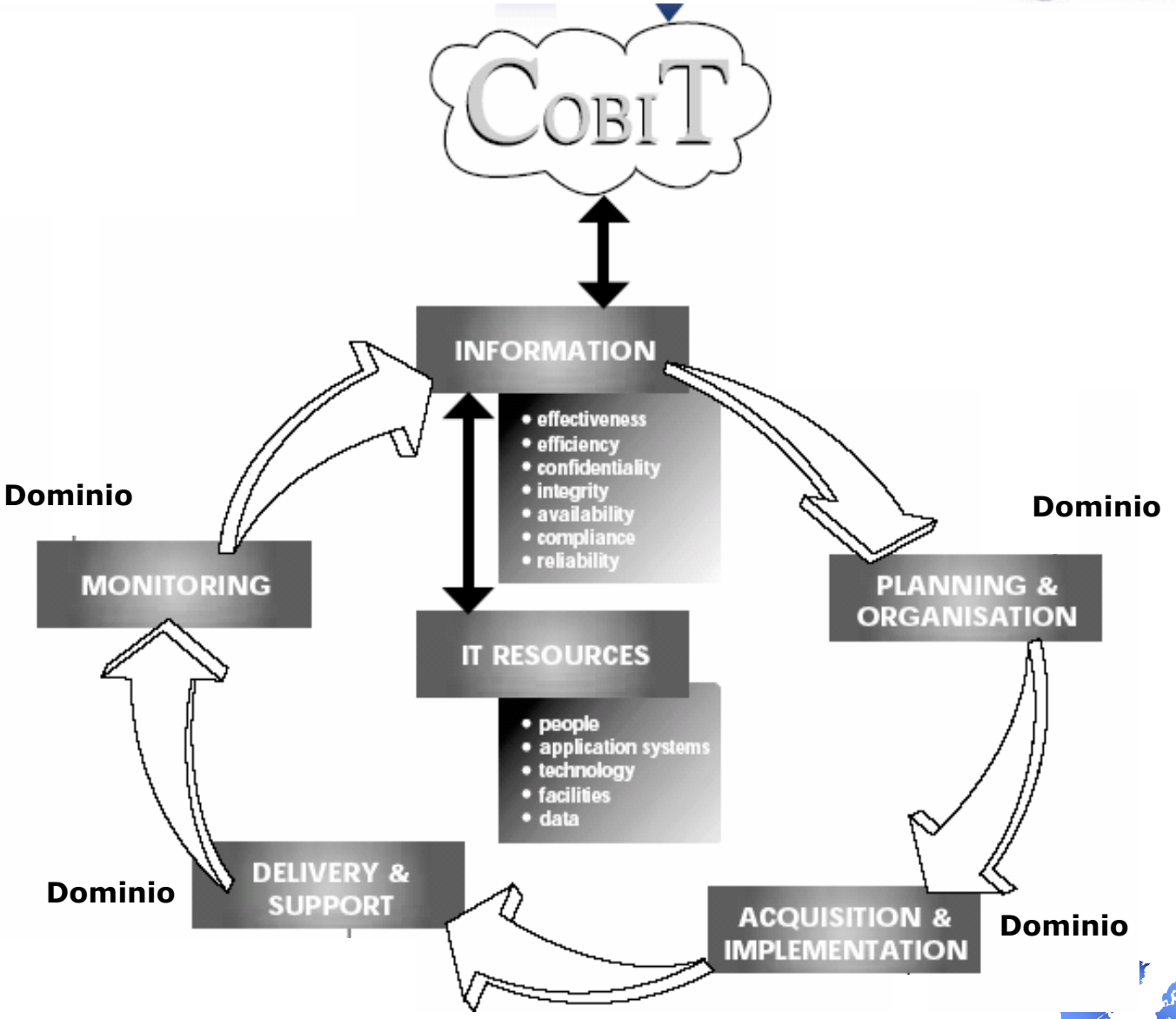
Dominios	Políticas de Seguridad
	Seguridad en la organización
	Control y clasificación de activos
	Seguridad en el personal de la organización
	Seguridad física y ambiental
	Administración de operaciones y comunicaciones
	Control de accesos
	Desarrollo y mantenimiento de sistemas
	Administración de la continuidad de las operaciones del negocio
	Acatamiento de leyes y normas

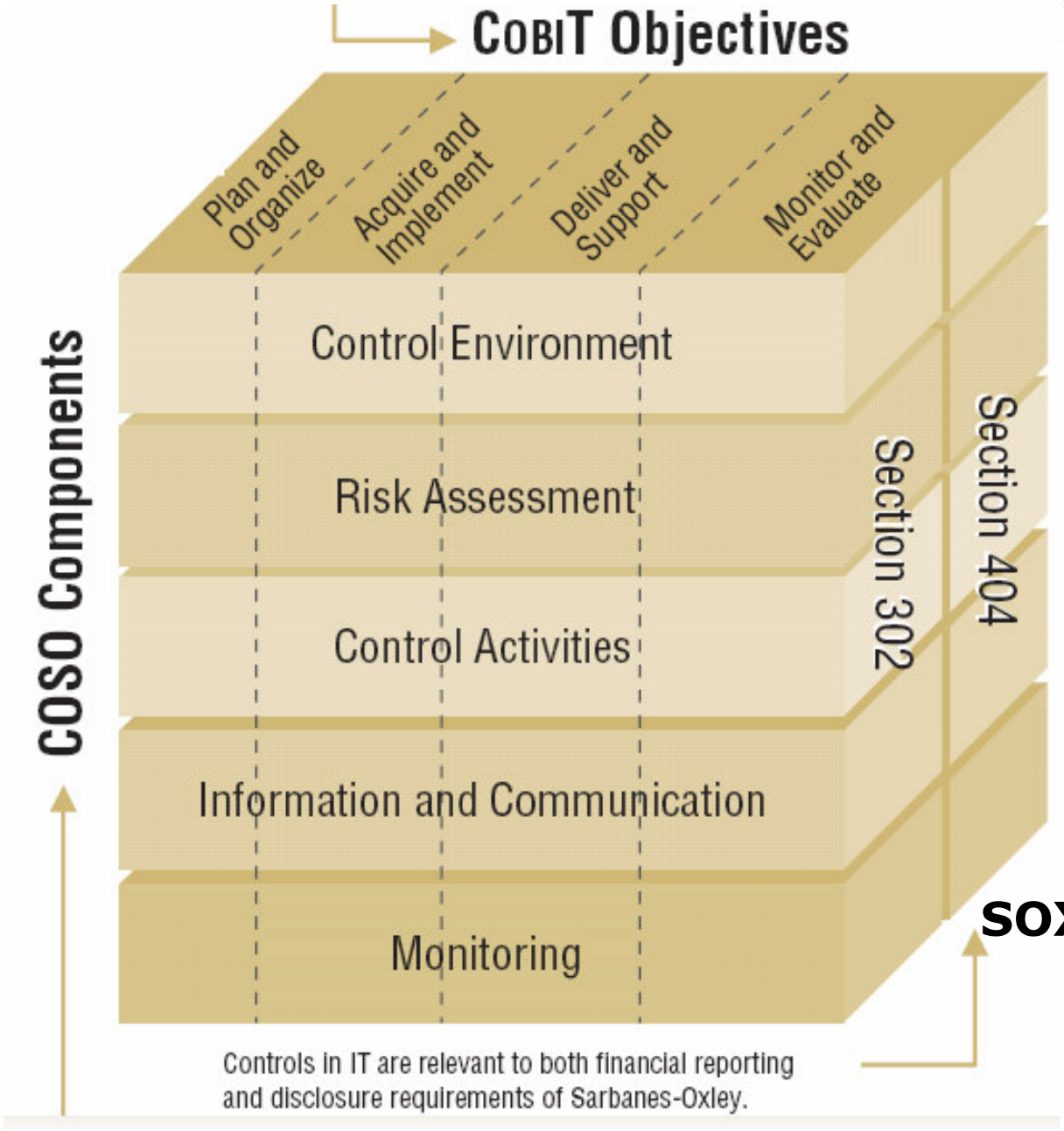
Modelo ISO 17799

CobiT

- Control Objectives for Information and related Technology, **CobiT**, fue desarrollado por la Information Systems Audit and Control Association, **ISACA**, con el propósito de contar con un conjunto de mejores prácticas en el campo de control interno en TI.

- El **CobiT** incluye 4 dominios


COBIT
INFORMATION
• effectiveness
• efficiency
• confidentiality
• integrity
• availability
• compliance
• reliability
Dominio
MONITORING
PLANNING & ORGANISATION
Dominio
IT RESOURCES
• people
• application systems
• technology
• facilities
• data
Dominio
DELIVERY & SUPPORT
ACQUISITION & IMPLEMENTATION
Dominio


COBIT Objectives
Plan and Organize
Acquire and Implement
Deliver and Support
Monitor and Evaluate
COSO Components
Control Environment
Risk Assessment
Control Activities
Information and Communication
Monitoring
Section 302
Section 404
SOX
Controls in IT are relevant to both financial reporting and disclosure requirements of Sarbanes-Oxley.

Contenido

1. Necesidades de seguridad en TI.
2. Estrategias de seguridad: Aplicación de estándares.
3. Administración de riesgos.

Administración de riesgos.

IDENTIFICAR LOS RIESGOS

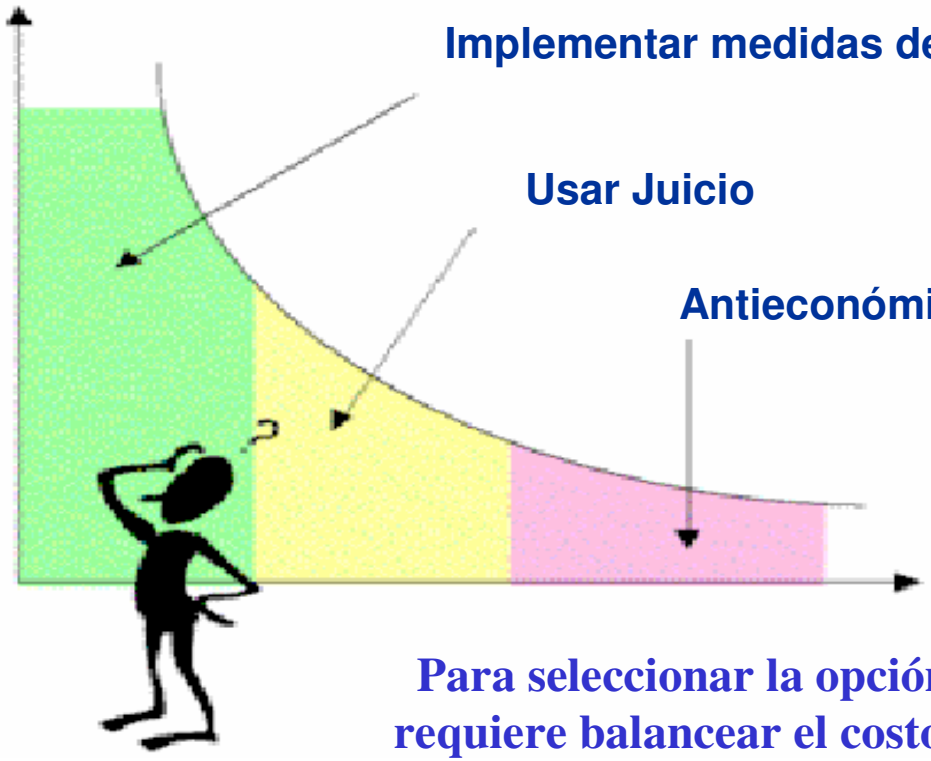
EVALUAR IMPACTOS

IMPLEMENTAR CONTROLES

Se considera el impacto y la probabilidad de ocurrencia

Tratamiento del Riesgo

Cómo Hacerlo?



Para seleccionar la opción más apropiada se requiere balancear el costo de implementación contra los beneficios derivados.

Fuente: Fernando Izquierdo, ISACA LatinCACS Sao Paulo

7 FORO INTERNACIONAL EN APLICACIONES DE TECNOLOGÍAS DE INFORMACIÓN

"NUEVOS ENFOQUES DE LA INFORMÁTICA"

TECNOLÓGICO DE MONTERREY.

¡ GRACIAS !

José Ángel Peña I.

japi@ccisa.com.mx

CCISA

Consultoría en Comunicaciones e Informática, S.A.de C.V.

Ave. Lázaro Cárdenas 1111
Plaza Brisas, 2o. Piso D- 35
Col. Valle Brisas C. P. 64780
Monterrey, Nuevo León, Méx.
Tel. 8357-1000, 8357-1400

www.ccisa.com.mx