Gobernabilidad de TI & Seguridad de la Información

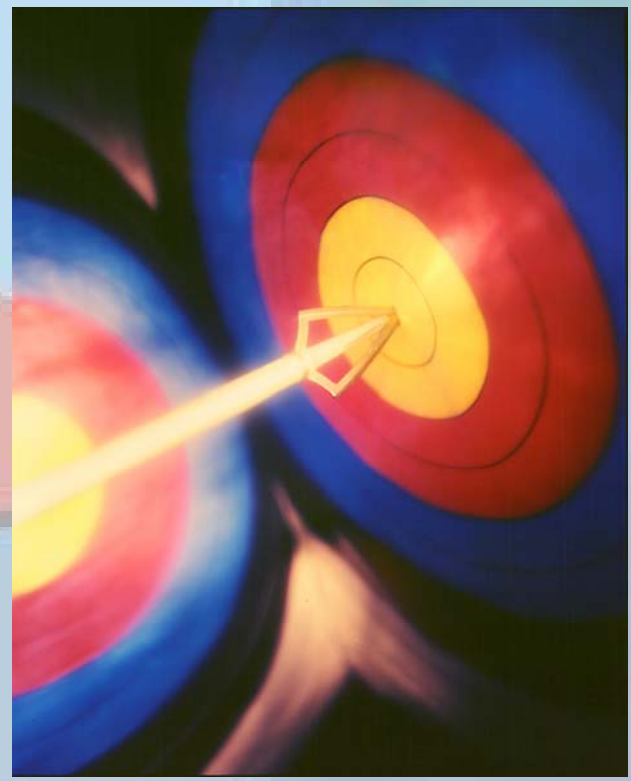
Guillermo Angarita Morris
CISA, CISSP

XXVI Salón de INFORMÁTICA

La gobernabilidad de TI: Una responsabilidad y reto para los directivos de TI

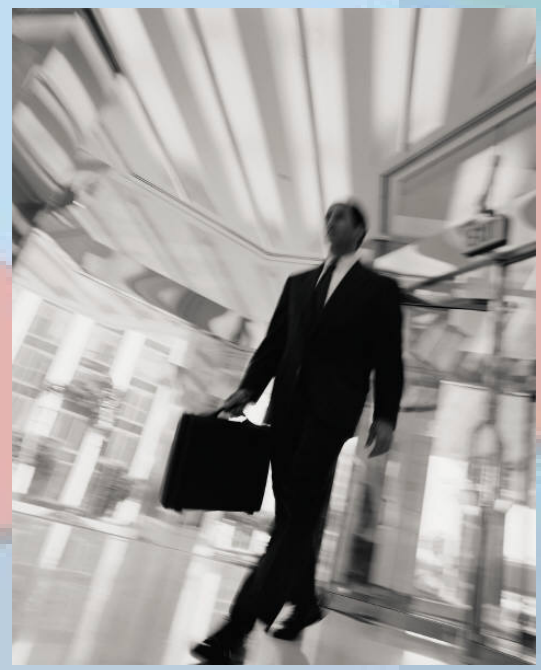
Objetivo

Identificar la importancia de la Seguridad de la Información como un elemento que forma parte del Gobierno Corporativo.



Agenda

- Introducción
- Importancia de la Seguridad de la Información
- Seguridad de la Información y TI
- La Gobernabilidad de SI.
- Conclusiones



Introducción

La difusión de la tecnología y la proliferación de la información transforma el papel de la información, para convertirse en un recurso de igual importancia que los recursos: tierra, mano de obra y capital.

Peter Drucker 1996

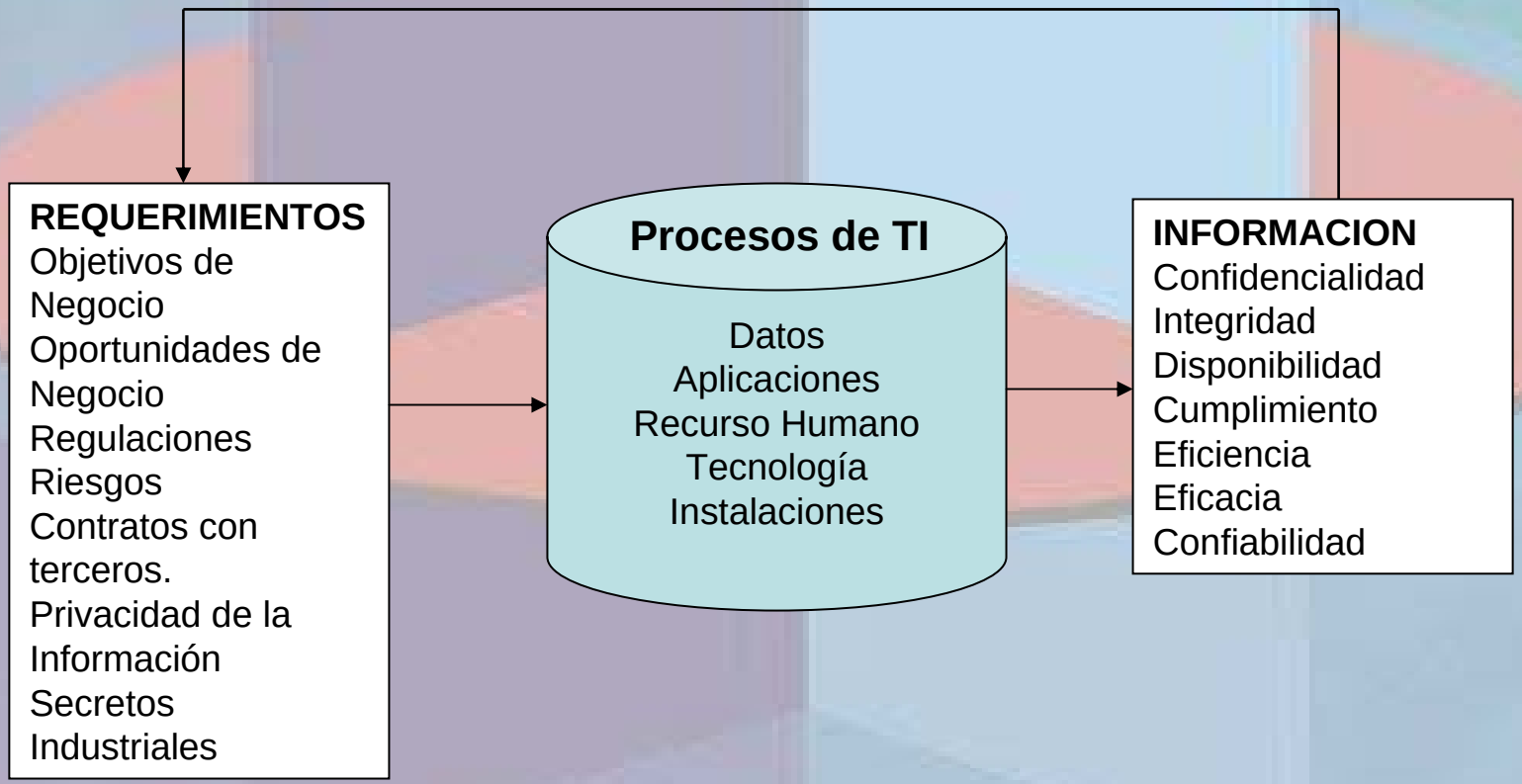
Introducción

Gartner recientemente estimo que en menos de una década, las organizaciones tendrán treinta veces mas contacto con la información de lo que tienen hoy en día.

Introducción

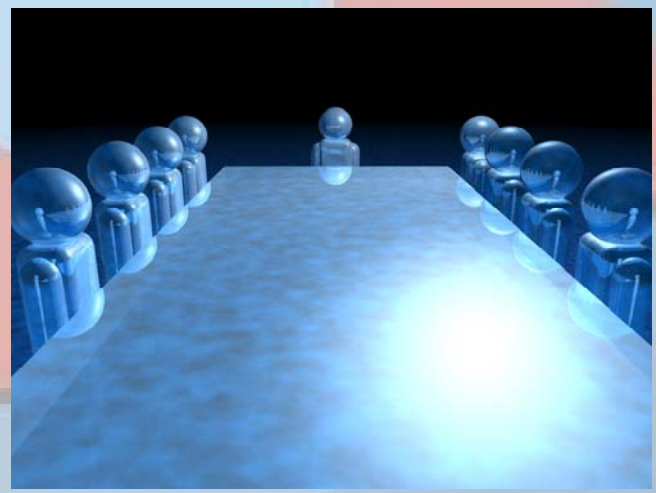
La INFORMACION es el NEGOCIO

Información como producto



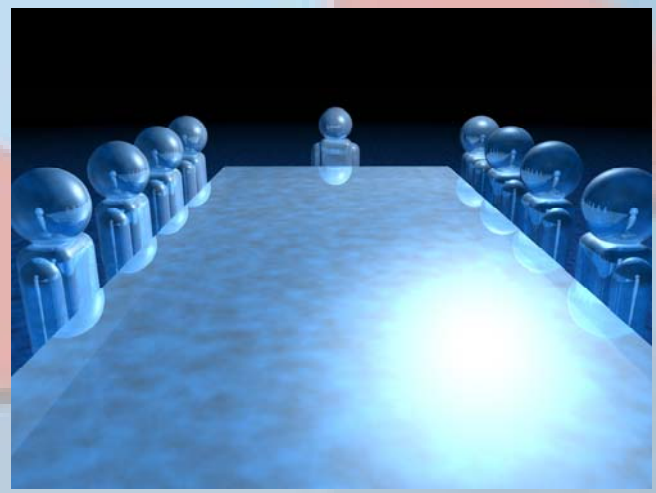
Antecedentes

- Cada vez mas regulaciones relacionadas con Seguridad de la Información
- La responsabilidad es del departamento de TI.
- Recurso humano.
- Foco únicamente en la información financiera.



Antecedentes

- Aumento de la dependencia de los sistemas y las comunicaciones que procesan la información.
- Dependencia de entidades que van mas allá del control de la organización.
- Aumento de la demanda para compartir información con socios, proveedores y clientes.
- Impacto en la reputación y el valor de la organización como resultado de fallas en la seguridad de la información.
- Los directivos no lo consideran un asunto estratégico.



Seguridad de la Información parte de la Governabilidad de IT

- Soporte a las políticas de seguridad.
- Soporte a las responsabilidades asignadas y los puntos de medición.
- Soporte a la clasificación de la información y la arquitectura.

Seguridad de la Información parte de la Governabilidad de IT

- Sirve como parte integral del sistema interno de control.
- Ayuda asegurar el cumplimiento legal y regulatorio.
- Privacidad de la información.

Gobierno Seguridad de la Información.

- Es un subconjunto del gobierno corporativo que provee dirección estratégica, asegura que los objetivos sean obtenidos, administra el riesgo apropiadamente, utiliza los recursos de la organización de manera responsable y monitorea el éxito o falla del programa corporativo de seguridad de la información.

Gobierno Seguridad de la Información

- Es la responsabilidad de la mesa directiva y los ejecutivos de alto nivel.
- Debe formar parte del Gobierno corporativo.
- Debe estar alineado con la estructura de Gobierno corporativo.
- Debe relacionarse con Gobernabilidad de TI.

Gobierno Seguridad de la Información

- Alineación de seguridad de la información con la estrategia del negocio para obtener los objetivos de negocio.
- Administración de riesgo para medir, mitigar y reducir el impacto a un nivel aceptable.
- Administración de los recursos para utilizar la infraestructura de manera eficiente y efectiva.
- Medición del desempeño

Gobierno Seguridad de la Información

- Definir una estructura para la administración de la seguridad de la información.
- Revisión y aprobación de las políticas de seguridad de la información.
- Asignar seguridad de la información a un comité.

Importancia Gobierno Seguridad de la Información

- Las organizaciones pueden sobrevivir si pierden un activo como el edificio, equipo, personas pero no la información.
- Riesgo de perdida de CIA de activos críticos de información.
- Asignar seguridad de la información a un comité.

Enfoques.

“TOP-DOWN”:

Alta Dirección consciente y conocedora del problema.

Impone mecanismos para extender su Gobierno Corporativo a cubrir la Seguridad de la Información.

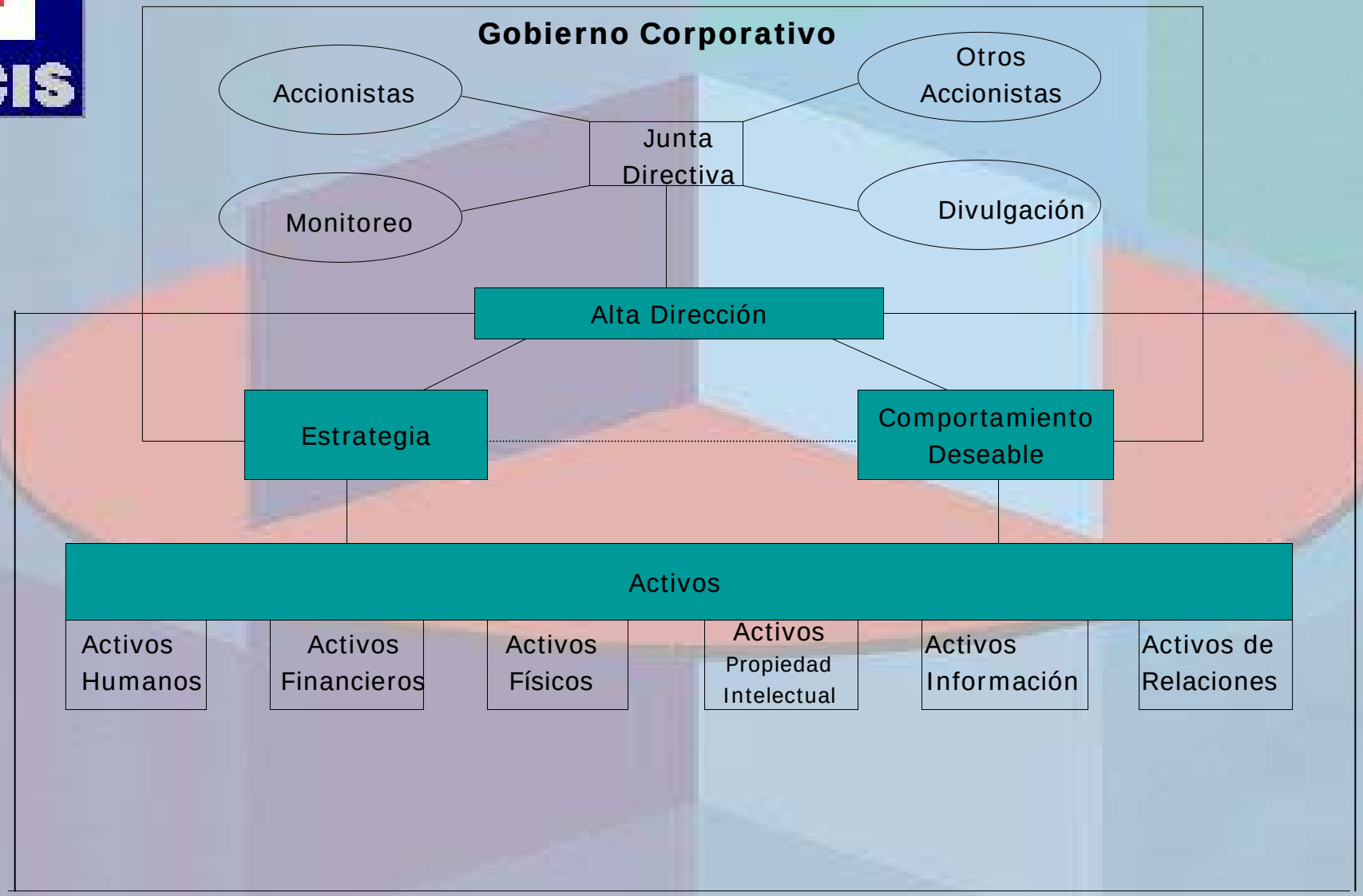
“BOTTOM-UP”:

Gerencia (o VP) de IT conciente de la necesidad.

Capacidad de alinear función y organización a los objetivos y estrategias del negocio.

Establece medios de comunicación sobre sus resultados y el cumplimiento de sus objetivos.

Gobierno Corporativo y de Activos Críticos



Framework

- Metodología para la administración del riesgo
- Estrategia de seguridad de la información relacionada con los objetivos de negocio y TI.
- Una efectiva estructura organizacional de seguridad.
- Una estrategia que hable acerca del valor de la información protegida y entregada.
- Políticas de seguridad que direccionen cada aspecto de la estrategia control y regulación.
- Estándares para cada una de las políticas que aseguren que los procedimientos y guías cumplen con la política.
- Proceso de monitoreo para asegurar cumplimiento y proveer retroalimentación sobre efectividad de los controles y mitigación del riesgo.
- Un proceso para asegurar evaluación continua y actualización de las políticas, estándares, procedimientos y riesgo.

Programa de Seguridad de la Información

- Desarrollo y mantenimiento de las políticas de seguridad
- Roles y responsabilidades,
- Desarrollo de estándares, procedimientos, indicadores, practicas y procedimientos
- Evaluación periódica de riesgos e impacto al negocio.
- Asignación de activos de información y su clasificación
- Controles adecuados, efectivos para las personas, procesos y tecnología
- Integración de seguridad en todos los organización
- Administración de incidentes

Programa de Seguridad de la Información

- Proceso de administración de identidad y control de acceso para usuarios y proveedores de información.
- Monitores de los indicadores de gestión
- Educación de todos lo usuarios y miembros de la junta directiva acerca de los requerimientos de seguridad de la información.
- Evaluación anuales de seguridad de la información y desempeño a la junta directiva.
- Plan de acción para superar las deficiencias encontradas
- Desarrollo y pruebas de planes de continuidad de negocio en caso de una interrupción o desastre.

Políticas y Procedimientos

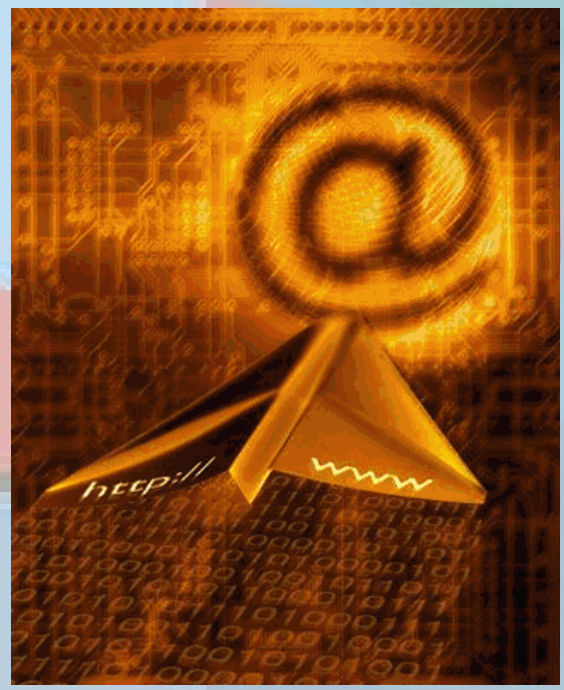
- Asignar responsabilidades
- Políticas y procedimientos para la prevención y detección .
- Procedimientos de monitoreo y reporte de incidentes.

Recurso Humano

- Tener las personas apropiadas en el lugar requerido
- Responsabilidades
  - Alta dirección
  - Usuarios toda la organización
  - Proveedores
  - Clientes.
  - Dueños de la información
  - Tecnología de la Información.
- Entrenamiento
- Cultura organizacional

Evaluación de Riesgo

La evaluación de riesgo habilita a las organizaciones a entender como determinados eventos pueden inhibir la consecución de los objetivos de negocio.



Identificar Procesos Críticos.

- Marco Estratégico
  - La organización y el ambiente en el que opera.
- Marco Organizacional
  - Conocer Objetivos y estrategias.
- Identificar Procesos críticos.
  - Definir los criterios bajo los cuales se pueda establecer la criticidad de un proceso con respecto a otro.

Impacto pérdida de Integridad.

- Pérdida financiera
- Fraude
- Decisiones de negocio equivocada
- Demandas
- Pérdida de clientes
- Pérdida de reputación.

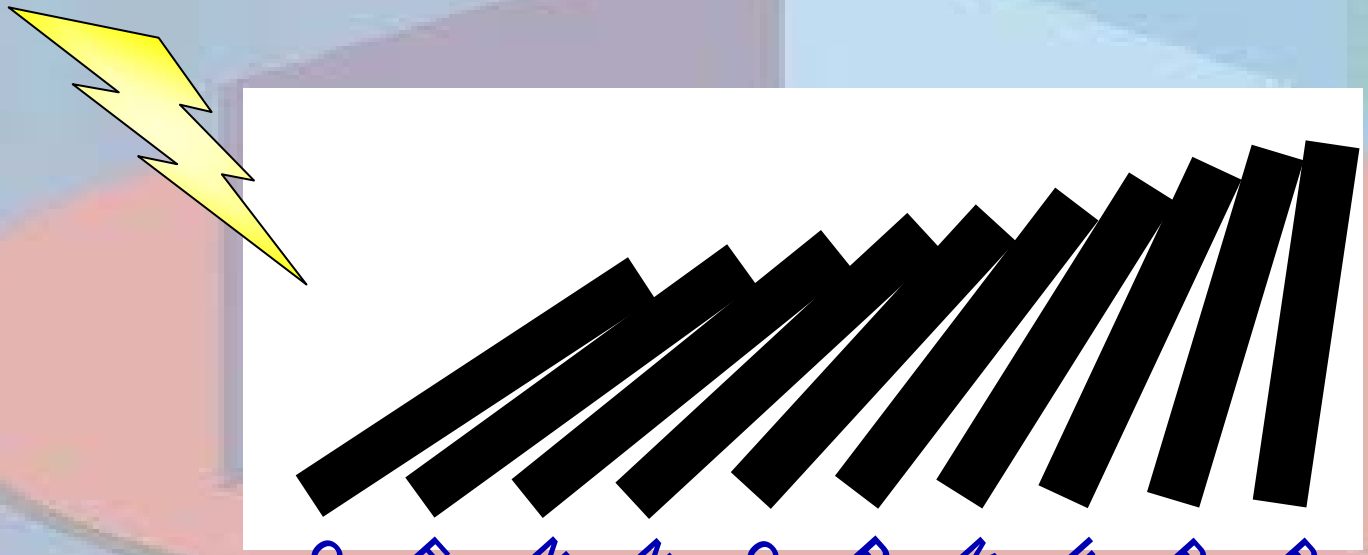
Impacto perdida de Confidencialidad.

- Perdida propiedad intelectual
- Privacidad de los clientes.
- Demandas
- Perdida de clientes
- Perdida de reputación.
- Fraudes.

Impacto Incumplimiento legal, contractual o regulatorio.

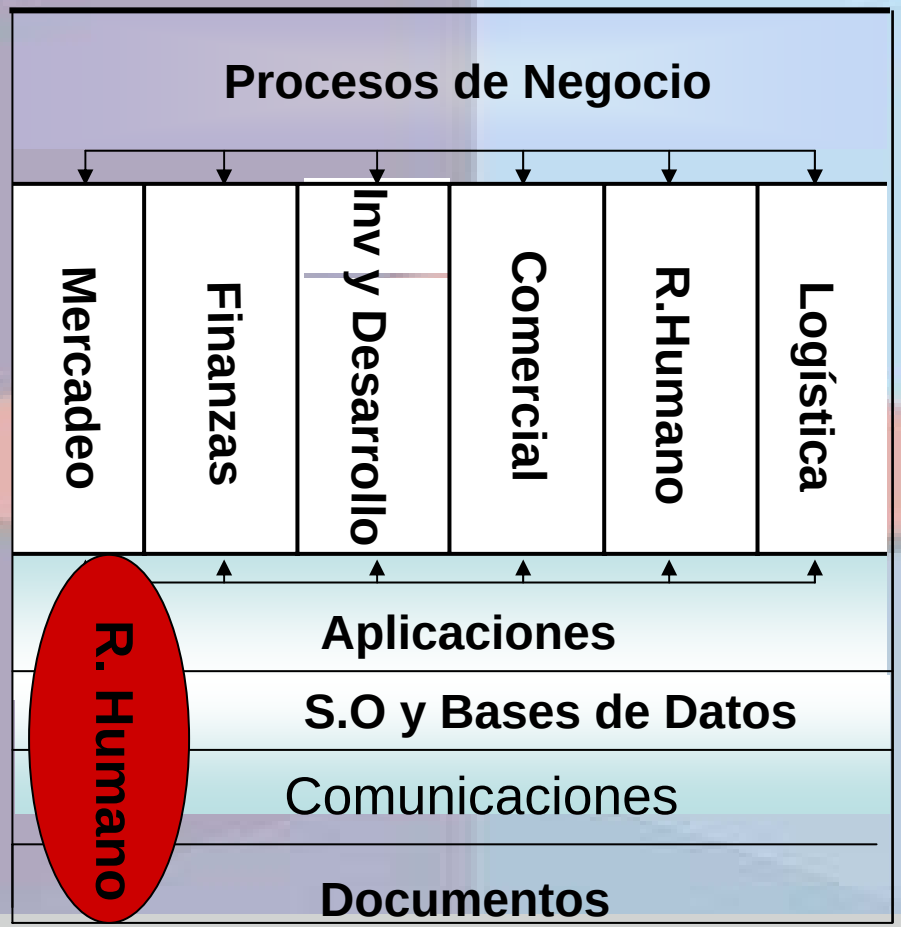
- Multas o Sanciones
- Perdida de clientes
- Perdida de valor de la compañía.
- Perdida de reputación.

Impacto perdida de Disponibilidad



Un Evento Ocurre Seguido por el efecto Domino

Identificar activos de Información.



Riesgos

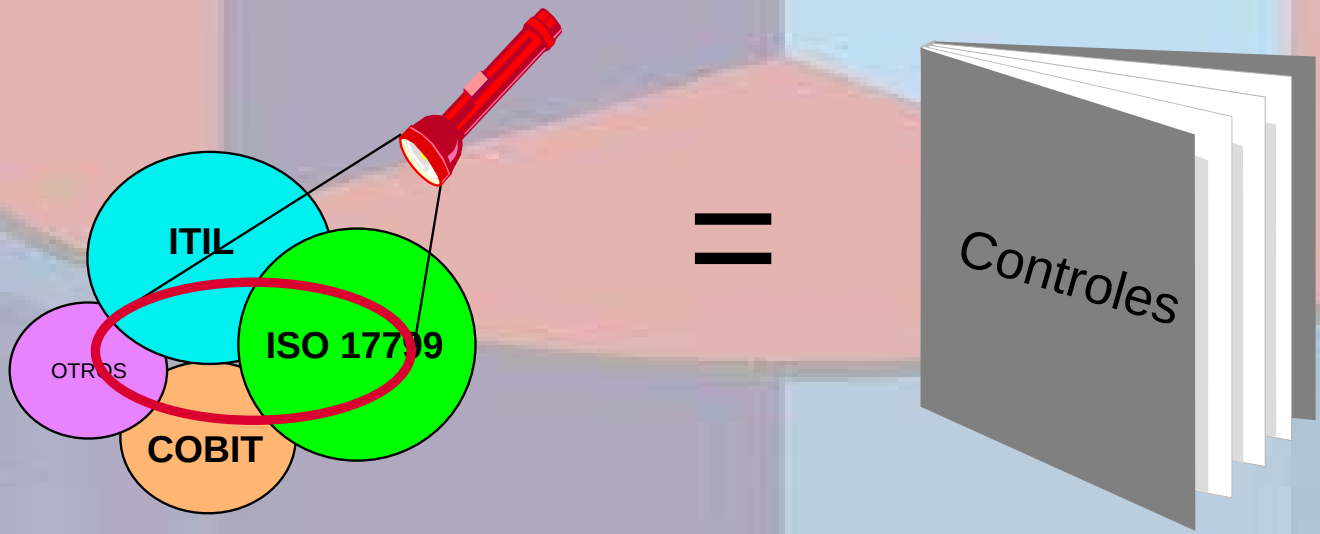
Mayores Riesgos:

- Pérdida de Confidencialidad.
- Pérdida de Disponibilidad.
- Incumplimiento Regulatorio
- Incumplimiento Contractual
- Perdida de Integridad.

Evaluar y definir prioridades.

- Identifique controles existentes.
- Identifique la efectividad de los controles.
- Riesgos de Mayor a Menor.
- Identificar los riesgos sobre los cuales se deben plantear opciones de tratamiento.

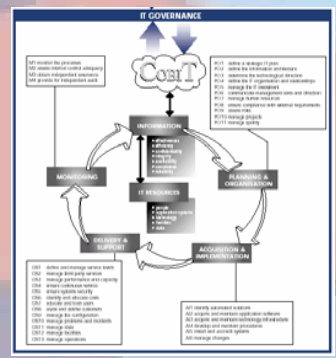
Tratamiento de los Riesgos



CobiT

Planear Organizar
PO

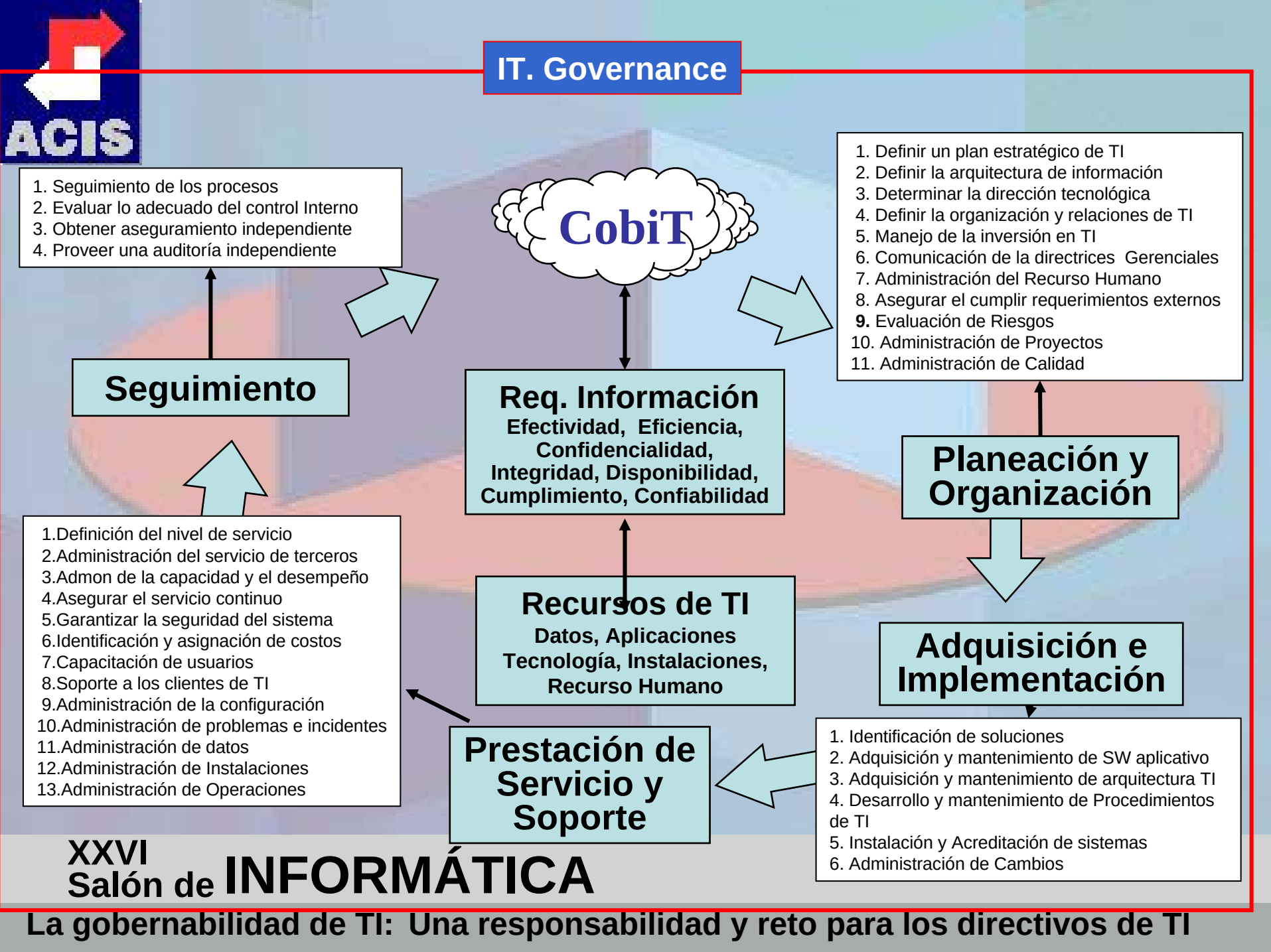
Adquirir e Implementar
AI



Monitorear
M

Entrega y Soporte
DS

IT. Governance



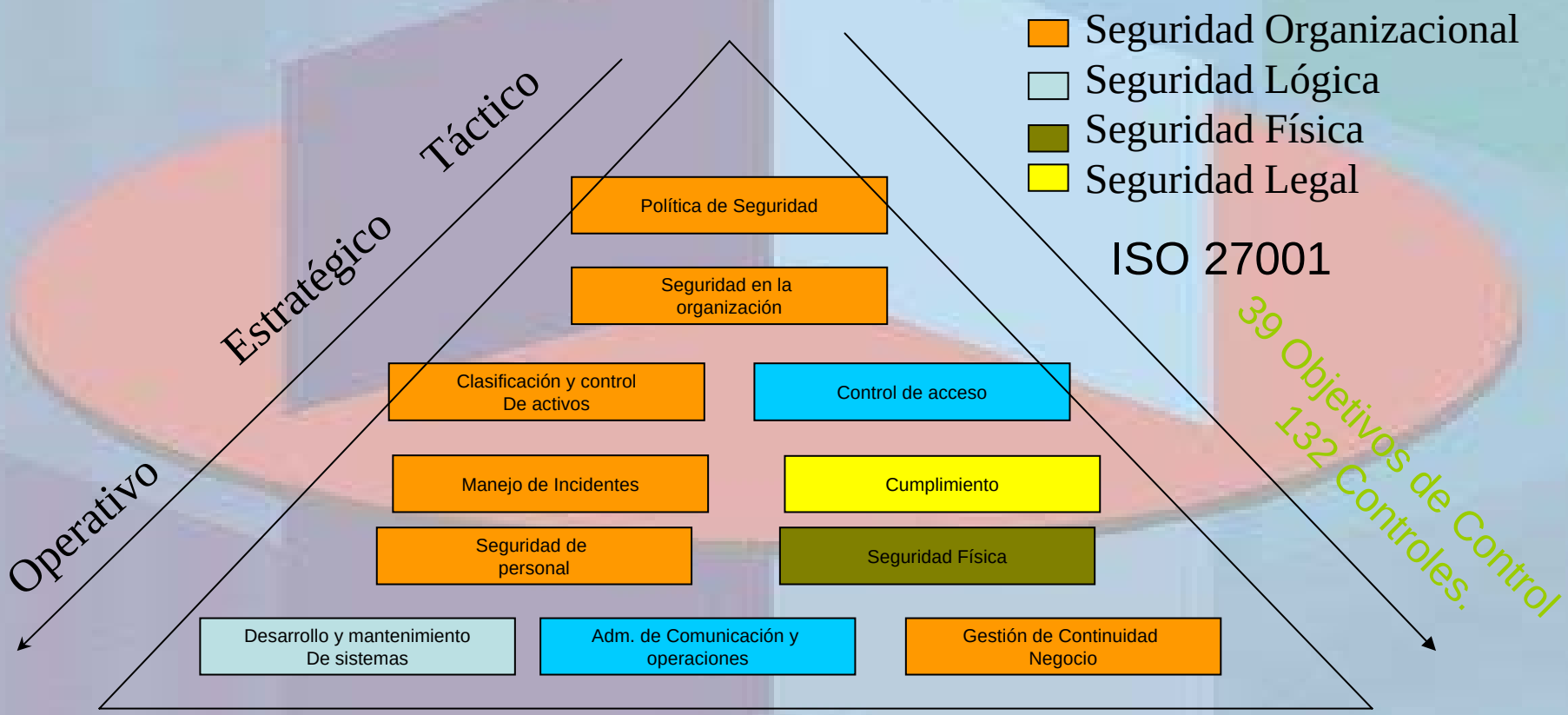
XXVI Salón de **INFORMÁTICA**

La gobernabilidad de TI: Una responsabilidad y reto para los directivos de TI

ISO 27001


Cumplimiento
Política de seguridad
Organización de la Seguridad
Administración de la continuidad
Clasificación y control de los activos
integridad
Confidencialidad
Información
Desarrollo y mantenimiento
Seguridad del personal
disponibilidad
Control de accesos
Seguridad física y medioambiental
Manejo de Incidentes
Gestión de comunicaciones y operaciones

Objetivos Básicos.

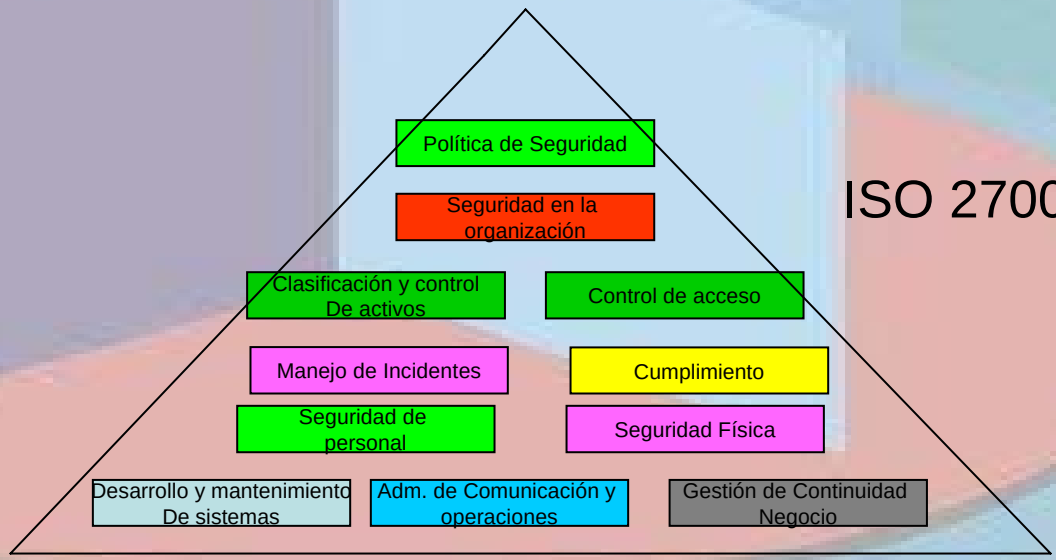


Planear y Organizar

- Definir Plan Estrategico
- Def. Arquitectura Información
- Def Diercción Tecno.
- Definir la Organización De IT y Sus relaciones
- Adm Inversion de TI
- Comunicar y De losobjetivos De la gerencia
- Manejar Recurso humano
- Asegurar cumplimiento
- **Evaluar riesgo**
- Adm proyectos
- Adm calidad

Adquirir e implementar

- Identificar Soluciones Automatizadas
- Adquiir y Mantener Software de aplicación
- **Instalar Y acreditar sistemas**
- **Adm. cambio**
- Adquiir y Mantener Infraestru. tecnológica
- Desarrollar Y mantener Proc. IT



ISO 27001

Monitorear

- Monitor The Process
- Assess Internal Control Adequacy
- Obtain Independent Assurance
- Provide Independent Audit

Entrega y Soporte

- **Definir y Adm niveles Servicio**
- **Adm Servicios Con terceros**
- **Adm. capacidad**
- **Asegurar Servicio continuo**
- **Asegurar Seguridad De los sistemas**
- **Identificar Y asociar costos**
- Administrar La operación
- Entrenar usuarios
- **Asistir Los Usuarios de IT**
- **Adm. Configuración**
- **Adm. Incidentes**
- Admi. datos
- Adm Instalaciones

La gobernabilidad de TI: Una responsabilidad y reto para los directivos de TI

Evaluación y Monitoreo

- Indicadores (Guías de administración de COBIT).
- Medir los resultados para conocer el desempeño actual y las mejoras.
- Procedimientos de acciones correctivas y preventivas.

Análisis Costo/ Beneficio

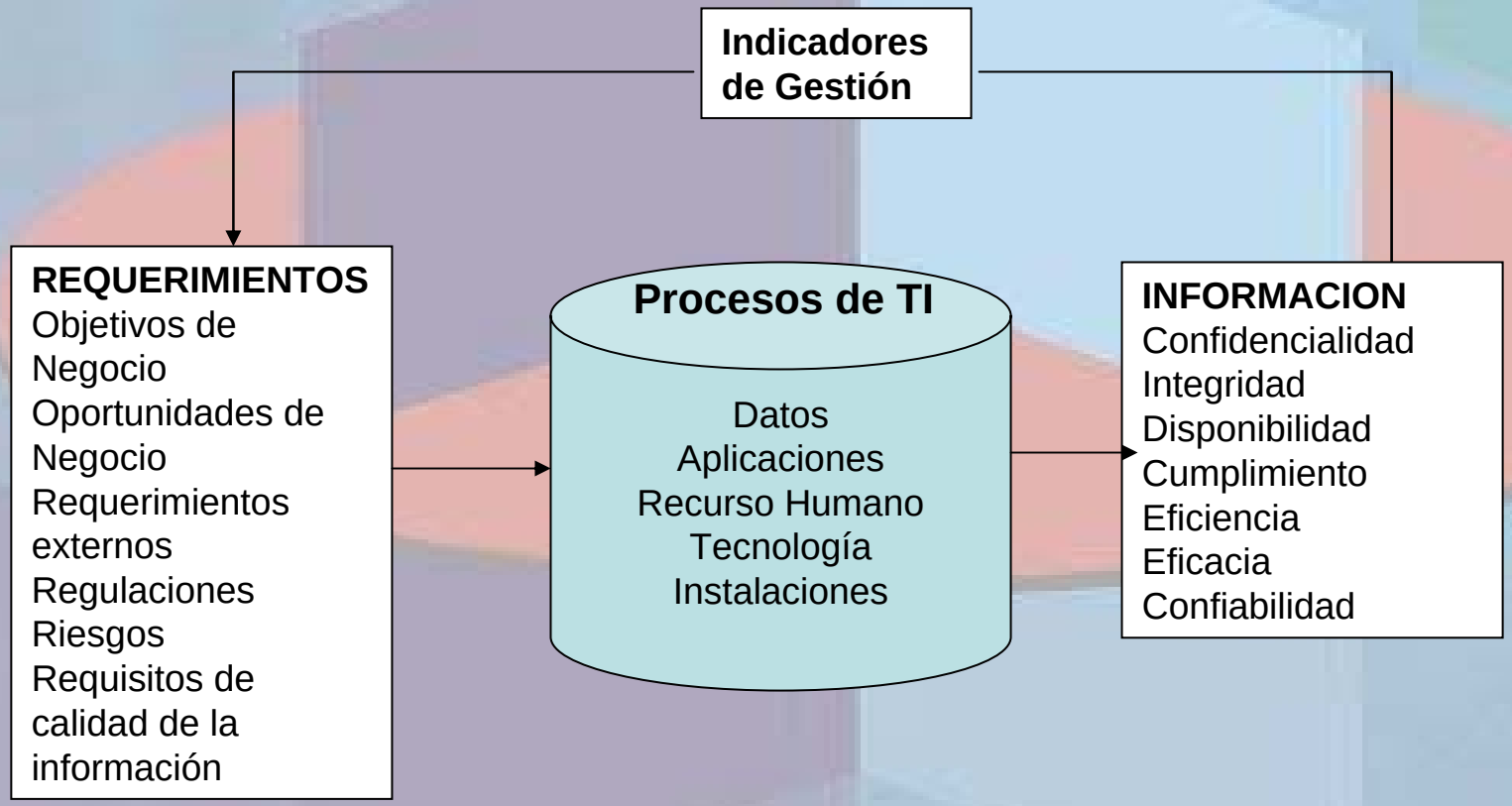
- **Estime el costo**: Tenga en cuenta los recursos de personas, hardware, software.
- **Estime la facilidad de implementación**: Considere la disponibilidad de recursos, el alcance y la duración del trabajo.
- **Estime los beneficios para el negocio:** Considere el impacto sobre uno o mas de las cinco prioridades de la organización.

Definición de Indicadores

- Indicadores

  - Implementación
  - Eficiencia
  - Eficacia

Información como producto



Beneficios

- Habilitador para cumplir los objetivos de negocio.
- Requisito para el cumplimiento de regulaciones Ej.: SOX, ISO 17799.
- Reducción en costos de procesamiento.
- Incremento de las ventas debido a calidad de los datos de los clientes.
- Incremento en la automatización de las decisiones y procesos.
- Aumento de la disponibilidad de Servicios y Aplicaciones
- Aumento del valor patrimonial o de la acción.

Conclusiones

- La información activo necesario para la operación de las organizaciones
- Es responsabilidad de las directivas minimizar los riesgos sobre los activos de información.
- Asunto Corporativo.
- Se debe tener un proceso unificado que mire los procesos del negocio de principio a fin.
- Recurso Humano

Referencias

- Information Security Governance, IT Governance Institute.
- ISO 27000, www.iso.org
- IT Governance Institute, COBIT® Security Baseline, USA, 2004, www.itgi.org

¿Preguntas?

Guillermo Angarita Morris
guillermo.angarita@iqcol.com
Miembro de ISACA, ISC2
Information Security Advisor
IQ Information Quality