

GOBIERNO CORPORATIVO TIC

Objetivos y Metodología para su implantación



GOBIERNO CORPORATIVO TIC

ÍNDICE

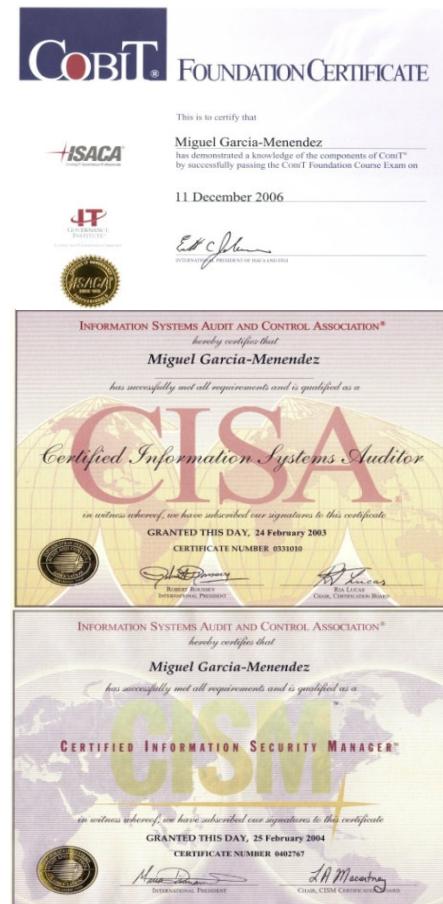
1. Introducción
2. Coso – Internal Control Integrated Framework
3. Balance Scorecard – Cumplimiento Legal
4. ISO 38500 - COBIT / VallIT
5. ISO 27000 – ISO 20000 (ITIL V3) - ISO 24762
6. Metodología.
6. Desarrollo del proyecto.
7. Fases de desarrollo del proyecto

ALGUNA INFORMACIÓN PERSONAL



José Manuel Ballester Fernández
mballester@temanova.com

- ▶ Doctor Ingeniero Industrial, MBA, CISA, CISM, CGEIT
 - » Consejero Delegado TEMANOVA
 - » Socio ALINTEC
 - » Director Estratégia Fundación DINTEL
 - » Director Postgrado Buen Gobierno Universidad Deusto
 - » Director Cátedra Buen Gobierno Universidad Deusto
- ▶ Miembro de ISACA, AUTELSI, AETIC, AEDI, AENOR
- ▶ Former President de ASIA / ISACA Madrid Chapter
- ▶ *CobiT® Foundation Certificate*
- ▶ *Certified Information Systems Auditor (CISA)*
- ▶ *Certified Information Security Manager (CISM)*
- ▶ *Certified Governance Enterprise IT (CGEIT)*
- ▶ *Accredited CobiT® Trainer*

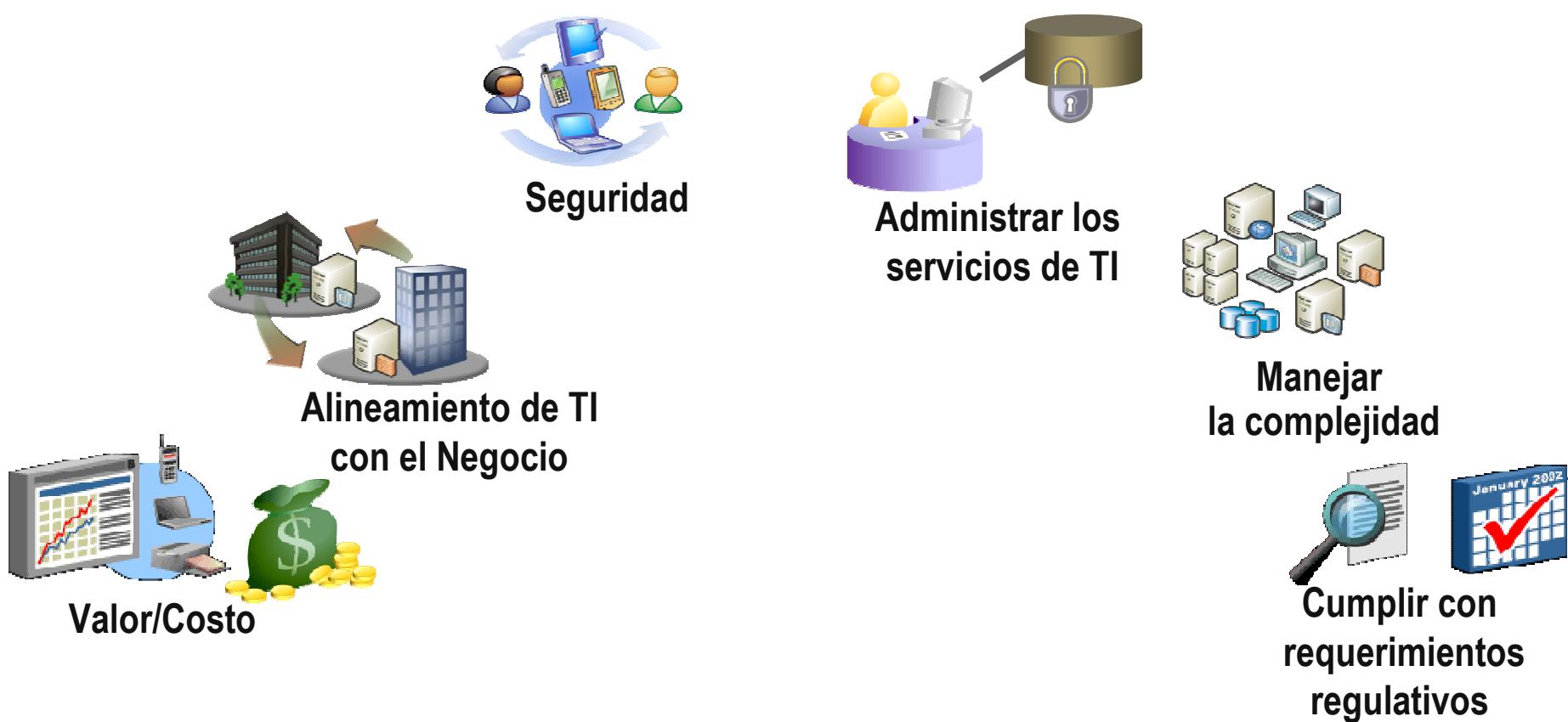


Complejidad social

Es importante tener en cuenta la creciente complejidad social que se presenta en las relaciones que las organizaciones desarrollan. El gobierno corporativo reconoce a los Stakeholders o terceros interesados la importancia que tienen y como afectan a la hora de implantar cualquier sistema.



Las organizaciones requieren una aproximación estructurada para abordar éstos y otros desafíos.





Gobierno Corporativo TIC es

- Un conjunto de responsabilidades y prácticas ejecutadas por la junta directiva y la administración ejecutiva con el fin de **proveer dirección estratégica**,
- garantizando que los **objetivos** sean alcanzados,
- estableciendo que los **riesgos** son administrados apropiadamente y
- verificando que los **recursos de la empresa** son usados responsablemente.

Niveles de gobernanza



Niveles de Gobernanza

Gobernanza corporativa (COSO)

La provisión de la estructura que permita determinar los objetivos de la Organización y supervisar el rendimiento, a fin de asegurar que los objetivos son cumplidos.

OCDE (2004)

Gobernanza de la TIC ISO 38500 – COBIT / Val IT

La especificación del marco de derechos a la toma de decisiones y la alta responsabilidad para favorecer un comportamiento deseable en el uso de las TIC.

MIT/Sloan School of Management (2004)

No obstante, la Gobernanza no tiene que ver con qué decisiones son tomadas - eso es Gestión -; sino que tiene que ver con quién toma las decisiones y con cómo se toman.

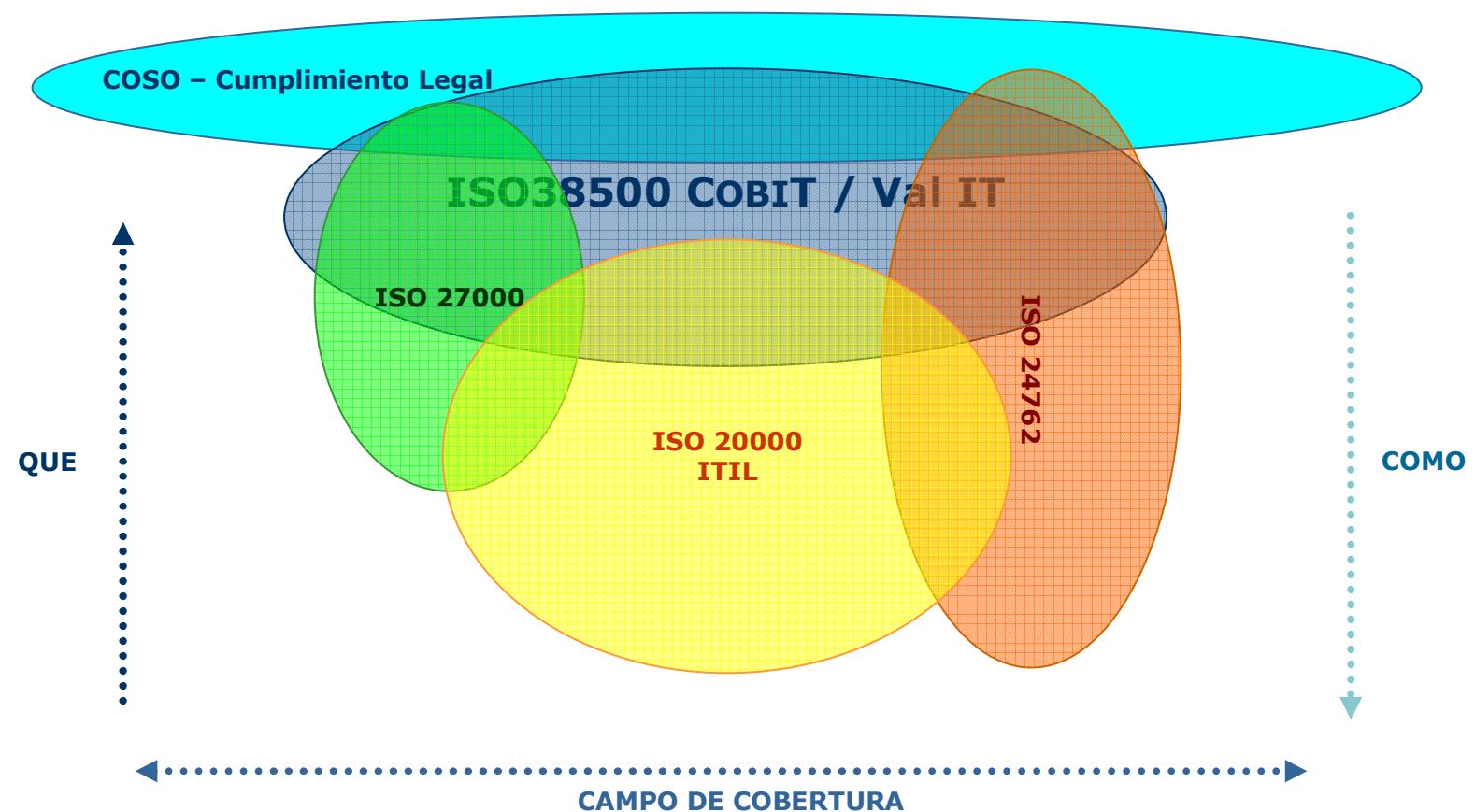
Gobernanza de la Seguridad de la Información y Tecnologías afines

El establecimiento y mantenimiento de un marco que provea garantía de que las estrategias de seguridad de la información están alineadas con los objetivos del negocio y son conformes a las leyes y regulaciones aplicables

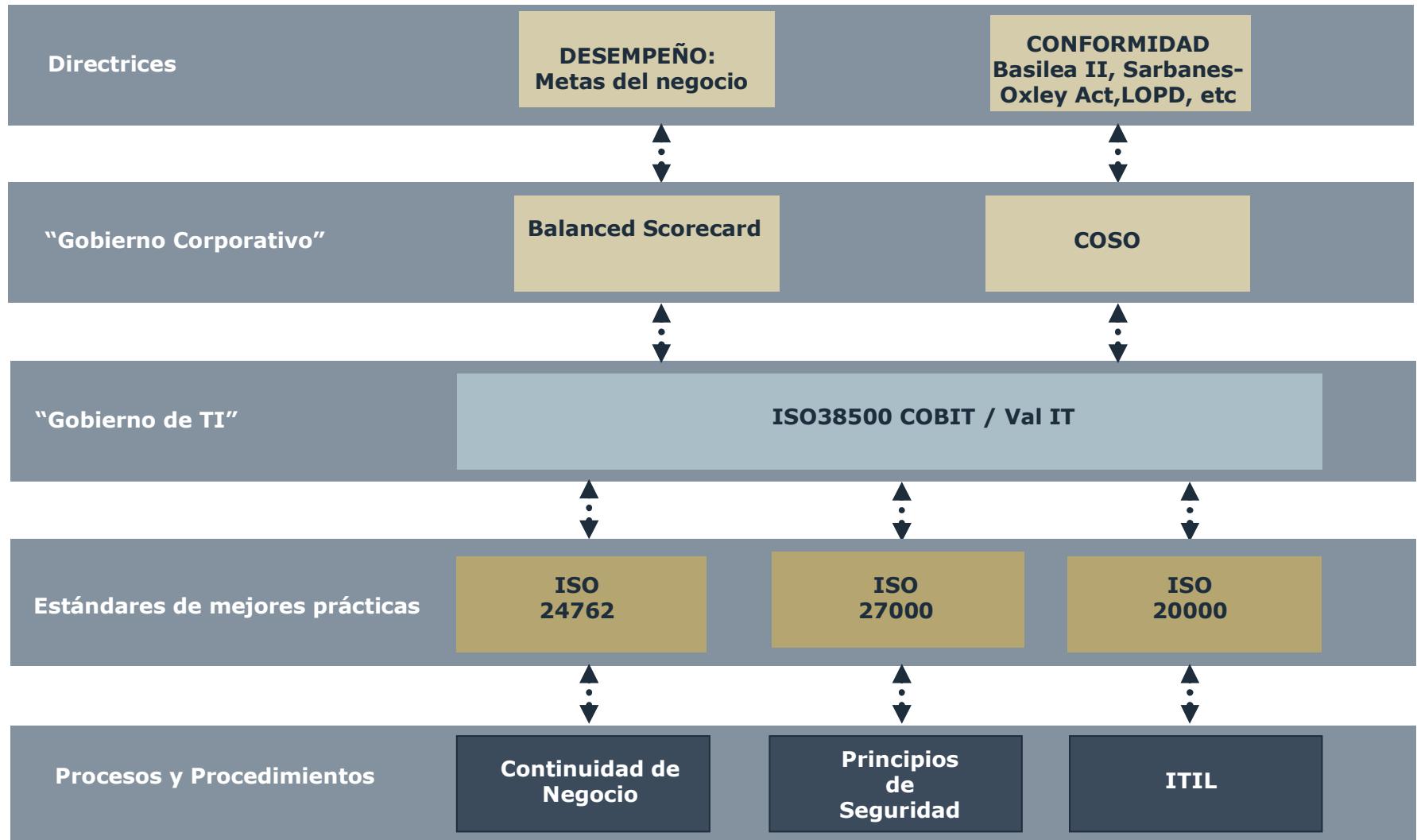
ISACA/CISM BoK (2002)

Marcos de Control

En la actualidad existe diferentes metodologías orientadas al control de las organizaciones, cada una de ellas abarca diferentes ámbitos, de forma que se complementan.



Niveles de gobernanza



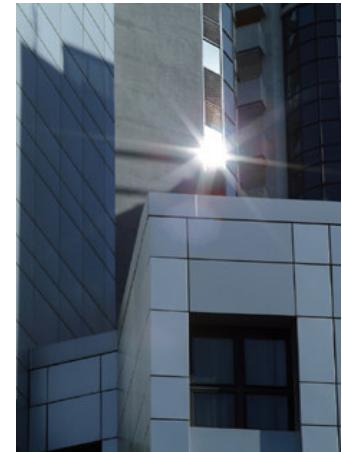
En 1992, COSO publicó el Sistema Integrado de Control Interno, un informe que establece una **definición común de control interno** y proporciona un **estándar** mediante el cual las organizaciones pueden **evaluar y mejorar sus sistemas de control**.



Control Interno

OBJETIVOS DE COSO

- Mejorar la calidad de la información financiera concentrándose en el manejo corporativo, las normas éticas y el control interno.
- Unificar criterios ante la existencia de una importante variedad de interpretaciones y conceptos sobre el control interno.

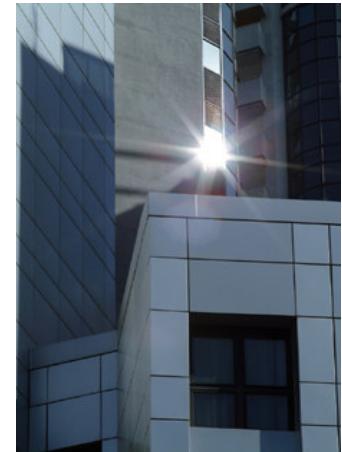


El Gobierno Corporativo incluye las siguientes capacidades:

- Alinear el riesgo aceptado y la estrategia
- Mejorar las decisiones de respuesta a los riesgos.
- Reducir las sorpresas y pérdidas operativas
- Identificar y gestionar la diversidad de riesgos para toda la entidad
- Aprovechar las oportunidades
- Mejorar la dotación de capital

Con estas capacidades se ayuda a la dirección a alcanzar los objetivos de rendimiento y rentabilidad de la entidad y prevenir la pérdida de recursos.

Con el Gobierno Corporativo permite asegurar una información eficaz y el cumplimiento de leyes y normas, además de ayudar a evitar daños a la reputación de la entidad y sus consecuencias derivadas.

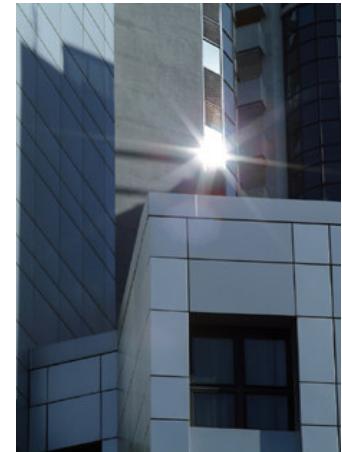


Definición de la Gobierno Corporativo

El Gobierno Corporativo es un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos.

El marco de Gobierno Corporativo está orientado a alcanzar los objetivos de la entidad, que se pueden clasificar en cuatro categorías:

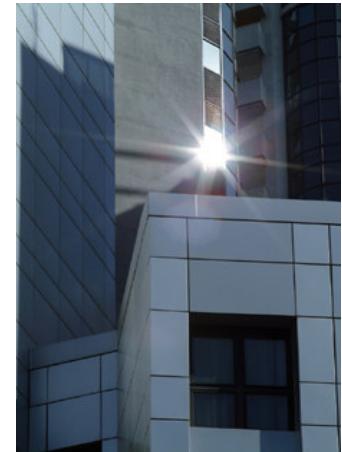
- **Estrategia:** objetivos a alto nivel, alineados con la misión de la entidad y dándole apoyo
- **Operaciones:** objetivos vinculados al uso eficaz y eficiente de los recursos
- **Información:** objetivos de fiabilidad de la información suministrada.
- **Cumplimiento:** objetivos relativos al cumplimiento de leyes y normas aplicables.



Componentes del Gobierno Corporativo

EL Gobierno Corporativo consta de ocho componentes relacionados entre sí, que se derivan de la manera en que la dirección conduce la empresa y cómo están integrados en el proceso de gestión.

- **Ambiente interno:** establece la base de cómo el personal de la entidad percibe y trata los riesgos.
- **Establecimiento de objetivos:** los objetivos deben de existir antes de que la dirección pueda identificar potenciales eventos que puedan afectar a su consecución.
- **Identificación de eventos:** tanto internos como externos que afectan a los objetivos de la entidad.
- **Evaluación de riesgos:** se analizan considerando su probabilidad e impacto como base para determinar como deben de ser gestionados.
- **Respuesta al riesgo:** las posibles respuestas – evitar, aceptar, reducir o compartir – los riesgos.
- **Actividades de control:** las políticas y procedimientos se establecen e implantan para ayudar a asegurar que las respuestas a los riesgos son eficaces.
- **Información y comunicación:** la información relevante se identifica, capta y comunica para que el personal pueda afrontar sus responsabilidades.
- **Supervisión:** la supervisión se lleva a cabo mediante actividades de la dirección o evaluaciones independientes.



Componentes de la gestión de Buen Gobierno Corporativo



Funciones y responsabilidades

La **Alta Gerencia** es la responsable última del sistema de control. La integridad y la ética deben ser elementos que aporten ejemplo a los demás empleados. Debe dirigir a los gerentes que a su vez son los responsables en sus respectivas áreas.

El **Consejo de Administración** fija las pautas y la visión global del negocio. El Consejo debe tener un papel activo en el conocimiento de las acciones que se ejecutan. Debe asegurarse de contar con vías de comunicación efectivas con la Alta Dirección y las áreas financieras, legales y de auditoría interna.

La **Auditoría Interna** debe desempeñar un papel de supervisión sobre la eficiencia y permanencia de los sistemas de control. Para ello debe contar con una ubicación jerárquica adecuada.

Los **empleados** en general tienen la responsabilidad de participar en el esfuerzo de aplicar el control interno, cuyos detalles deben ser incorporados a la descripción de los puestos de trabajo. Ellos deben comunicar al nivel superior las desviaciones que detecten a los códigos de conducta, a las políticas establecidas o la legalidad de las acciones realizadas.



Evaluación de riesgos

- Determinación de los Objetivos.
- Objetivos globales (tales como la Misión).
- Objetivos específicos de las diversas actividades (por ej. Producción), estos sub-objetivos medibles a través de metas deben ser coherentes.

Los objetivos deben ser:

- Definidos de modo de identificar los criterios para medir el rendimiento y establecer factores críticos de éxito (que pueden ser a nivel de actividad o unidad operacional).
- Coherentes y compatibles.
- Como ejemplo se puede considerar: efectuar pagos sólo para compras autorizadas, que los sistemas informáticos se encuentren disponibles según los requerimientos del negocio, etc.



Información y comunicación

- Debe asegurase que se obtenga información de calidad y no meros datos.
- La información debe ser protegida ya que se trata de un activo valioso.
- Las vías de comunicación interna deben asegurar que el personal conozca los elementos suficientes para cumplir con su tarea.

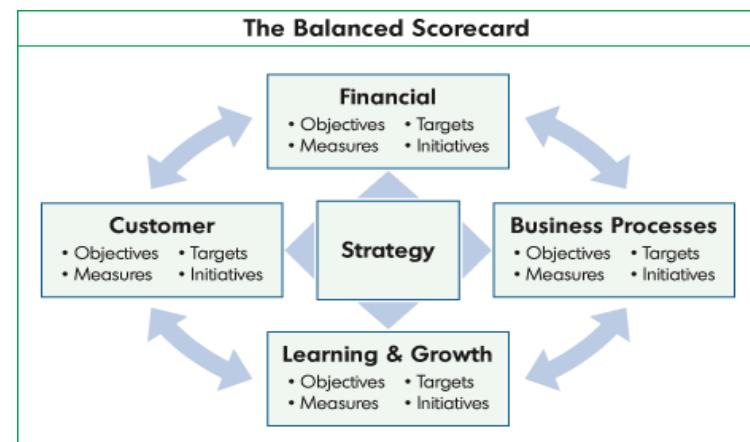
Supervisión

- Las actividades de supervisión continua y evaluaciones puntuales.
- Las deficiencias detectadas deben ser oportunamente comunicadas.

- Legislación extranjera de implantación en "branch offices".
- Decisiones del Consejo Europeo (emergentes).
 - Pretender preparar un marco para el desarrollo nacional.
- Agencias Gubernamentales:
 - AGPD.
 - Ministerio de Industria.
 - Ministerio del Interior.
- Foros sectoriales:
 - Asociaciones Profesionales.
 - Basilea II



- BalancedScoreCard:
 - Lenguaje común entre entornos diferentes.
 - Establecimiento de un mapa estratégico con "dónde queremos estar".
 - Estudio del impacto de determinadas acciones:
 - Seleccionar acciones.
 - Estudiar el impacto en el BSC.
 - Elaborar una regla.



• ISO/IEC 38500. *Corporate Governance of IT*

 International Organization for Standardization International Standards for Business, Government and Society Search »

Home Products Standards development News and media About ISO For ISO Members FAQs Fr ISO Store

Products > ISO Standards > By TC > JTC 1 Information technology > SC 7

ISO Store ISO Standards By ICS »By TC How to use the ISO Catalogue Management standards The ISO portfolio FAQs Country codes (ISO 3166/MA) Publications and e-products Copyright

ISO/IEC 38500

Corporate governance of information technology

General information

Number of Pages:

Edition: 1 (Monolingual)	ICS:
Status:  Under development	Stage: <u>60.00</u> (2008-05-08)
TC/SC: <u>JTC 1/SC 7</u>	

These standards could also interest you

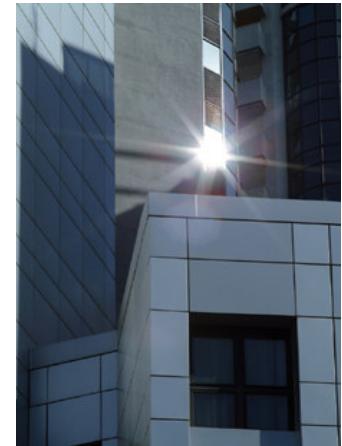
- ISO/IEC 29881:2008 Information technology -- Software and systems engineering -- FISMA 1.1 functional size measurement method
- ISO/IEC 15288:2008 Systems and software engineering -- System life cycle processes
- ISO/IEC 12207:2008 Systems and software engineering -- Software life cycle processes

OBJETIVOS DE LA NORMA

Objetivo de la norma: El uso de las tecnologías de la información de manera efectiva, optima y eficiente en las organizaciones, con la finalidad de:

- Generar confianza en los stakeholders (empleados, clientes, proveedores, socios, accionistas, etc.) en el Gobierno Corporativo de TIC de la Organización.
- Informar y guiar a la alta dirección en el gobierno TIC en su organización.
- Proveer de bases para la evaluación objetiva del Gobierno Corporativo TIC





BENEFICIOS DE LA IMPLANTACIÓN DEL ESTÁNDAR:

- Adecuada aplicación y operación de activos de TIC.
- Asignación de responsabilidades.
- Continuidad del negocio
- Sostenibilidad.
- **Alineación de TIC con los objetivos del negocio.**
- Asignación eficiente de recursos.
- Innovación en los servicios, los mercados y las empresas.
- Mejora de imagen y reputación en el mercado frente a los reguladores, agentes sociales y con los stakeholders.
- **Optimización en los costes de una organización**
- **Inversión efectiva en TIC.**
- **Cumplimiento legal.**

Con estas capacidades se ayuda a la dirección a alcanzar los objetivos de rendimiento y rentabilidad de la entidad y prevenir la pérdida de recursos.

Con el Gobierno Corporativo permite asegurar una información eficaz y el cumplimiento de leyes y normas, además de ayudar a evitar daños a la reputación de la entidad y sus consecuencias derivadas.



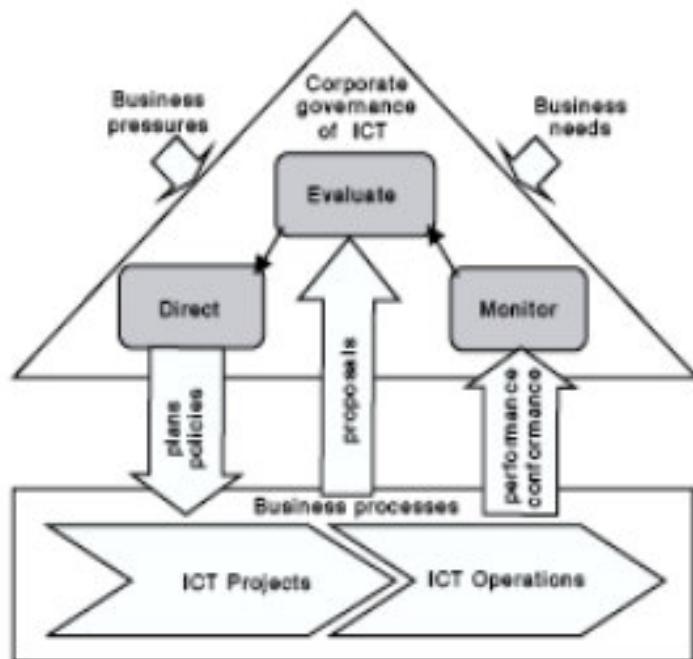
INTERNATIONAL
STANDARD

ISO/IEC
38500

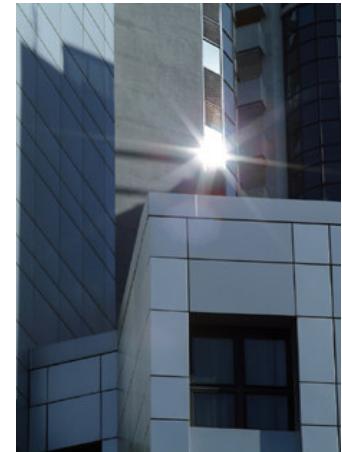
First edition
2009-09-21

Corporate governance of information
technology

Gouvernance des technologies de l'information par l'entreprise



Model for Corporate Governance of IT



MODELO

La Norma establece los principios para el buen gobierno corporativo de TIC:

- Responsabilidad
- Estrategia
- Inversión
- Rendición de Resultados
- Cumplimiento
- Recursos Humanos

En cada uno de los principios de la Norma es necesario realizar estas tres tareas principales:

- EVALUAR el uso actual y futuro de las TIC.
- DIRIGIR la preparación y ejecución de planes y políticas para garantizar que el uso de TIC cumple los objetivos empresariales.
- MONITORIZAR la conformidad con las políticas, y los resultados de los planes.

- ISO/IEC 38500. *Corporate Governance of IT*

 International Organization for Standardization
International Standards for Business, Government and Society

Search >

Independencia de las herramientas

Home Products > ISO Standards > By TC > IEC 1 Information technology > ISO 38500

Definición clara del concepto y sus límites

Identificación de los destinatarios del mensaje

Sencillez del propio mensaje a través de la proclamación de unos principios

These standards could also interest you

- ISO/IEC 29981:2008 Information technology -- Software and systems engineering -- FISMA 1.1 functional size measurement method
- IEC 15288:2008 Systems and software engineering -- System life cycle processes
- ISO/IEC 12207:2008 Systems and software engineering -- Configuration management

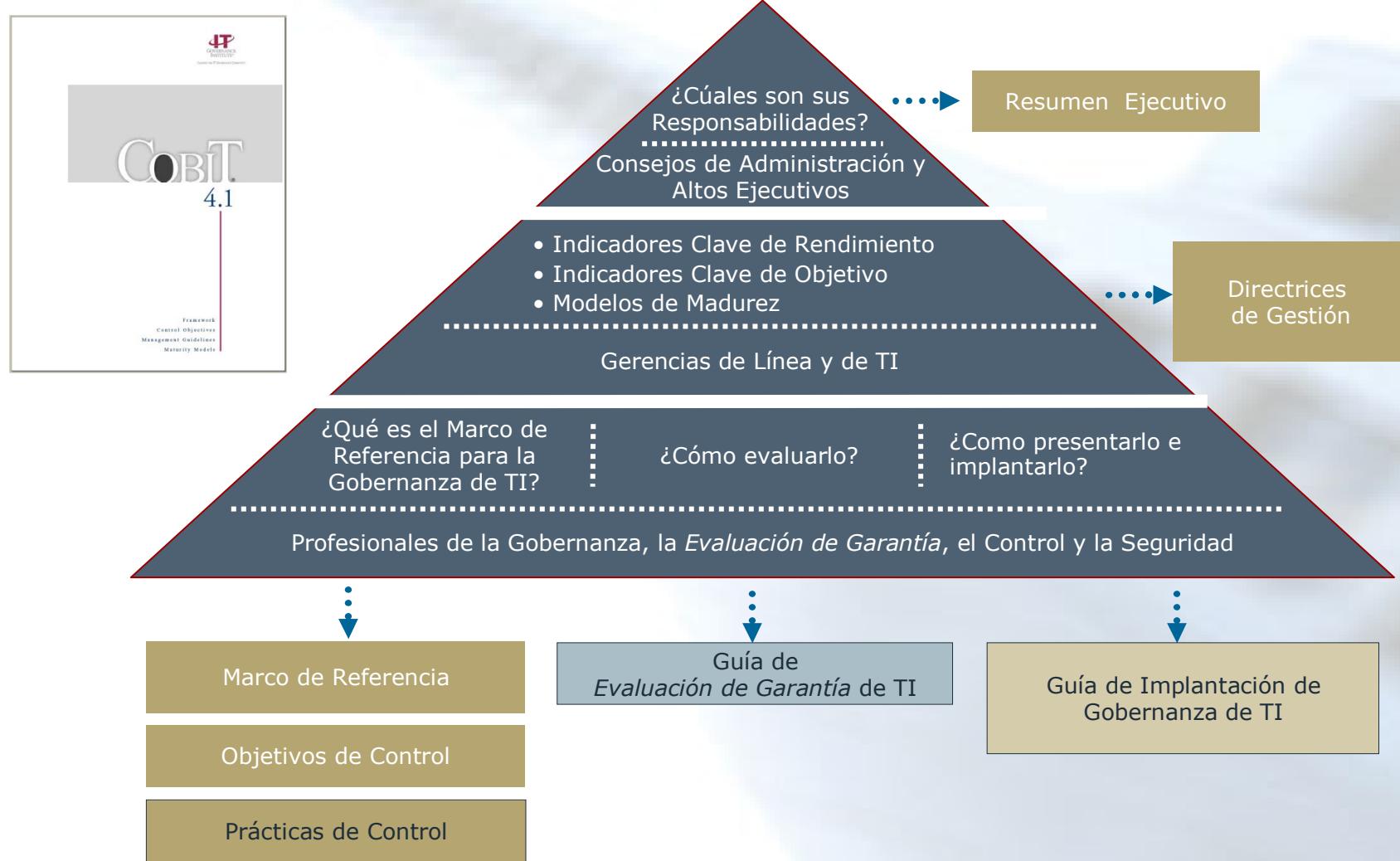
© 2008 ISO Privacy Policy Name and logo Sitemap Contact ISO Guided tour of ISO-Online Print Increase text size

- ISO/IEC 38500. Principios
 - ◊ Claro establecimiento de responsabilidades sobre las TIC
 - ◊ Planificación de las TIC para un mejor soporte de la organización
 - ◊ Adquisición de TIC de forma válida
 - ◊ Garantía de unas TIC que funcionan bien y cuando son requeridas
 - ◊ Garantía de unas TIC que cumplen (y ayudan a cumplir) con la normativa formalmente establecida
 - ◊ Garantía de unas TIC cuyo uso respeta los factores humanos

- ISO/IEC 38500. Cuestiones comprensibles

- ◊ ¿Los individuos de su organización entienden y aceptan su responsabilidad sobre las TIC?
- ◊ ¿Sus planes tecnológicos soportan los planes corporativos de su organización y cubren las necesidades presentes y futuras de la misma?
- ◊ ¿Las adquisiciones de TIC se realizan por razones aprobadas y de la forma aprobada?
- ◊ ¿Su marco TIC garantiza adecuadamente la continuidad y sostenibilidad de su organización?
- ◊ ¿Su marco TIC es conforme a regulaciones externas y/o internas?
- ◊ ¿Su entorno TIC cumple con las necesidades de la “gente involucrada en el proceso”?

Control Objectives for Information and Related Technology



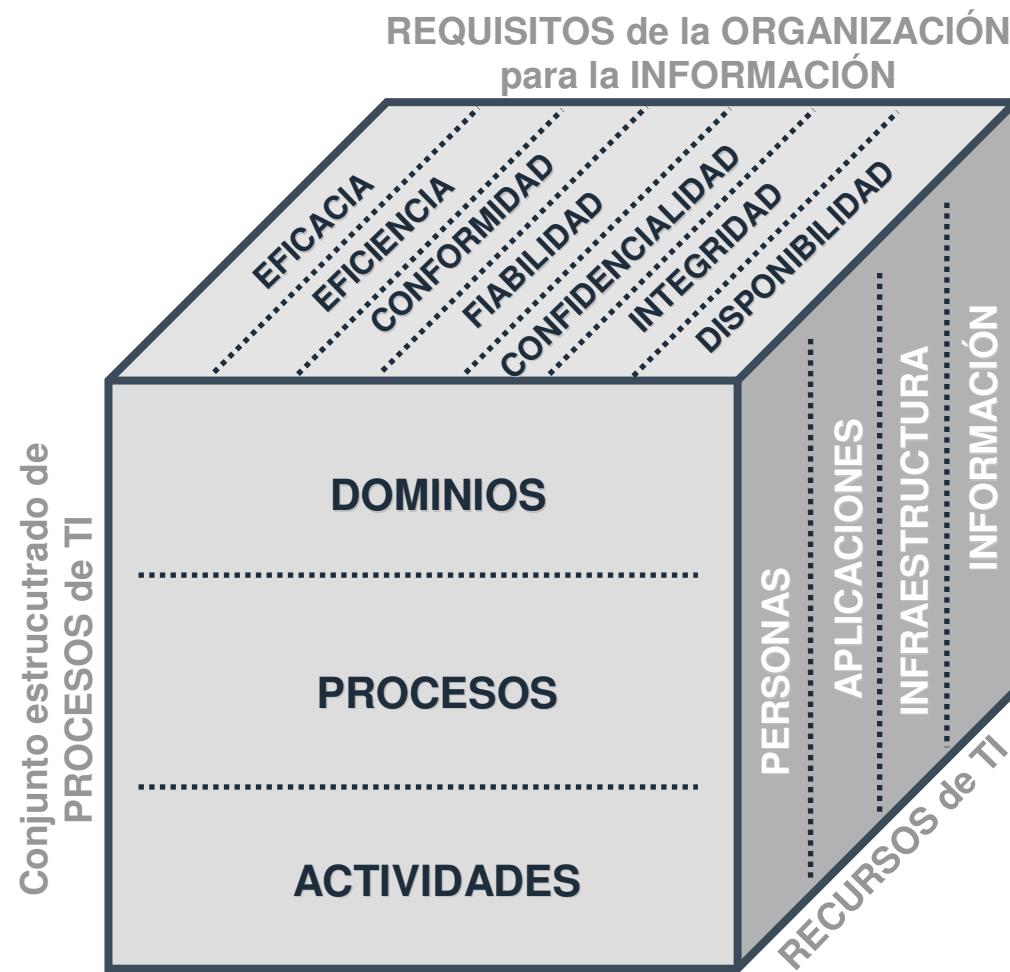
MARCO DE REFERENCIA

La principal cualidad de CobiT es su orientación hacia los OBJETIVOS de la ACTIVIDAD de la Organización y cómo TIC apoya su logro





MARCO DE REFERENCIA EL CUBO DE COBIT



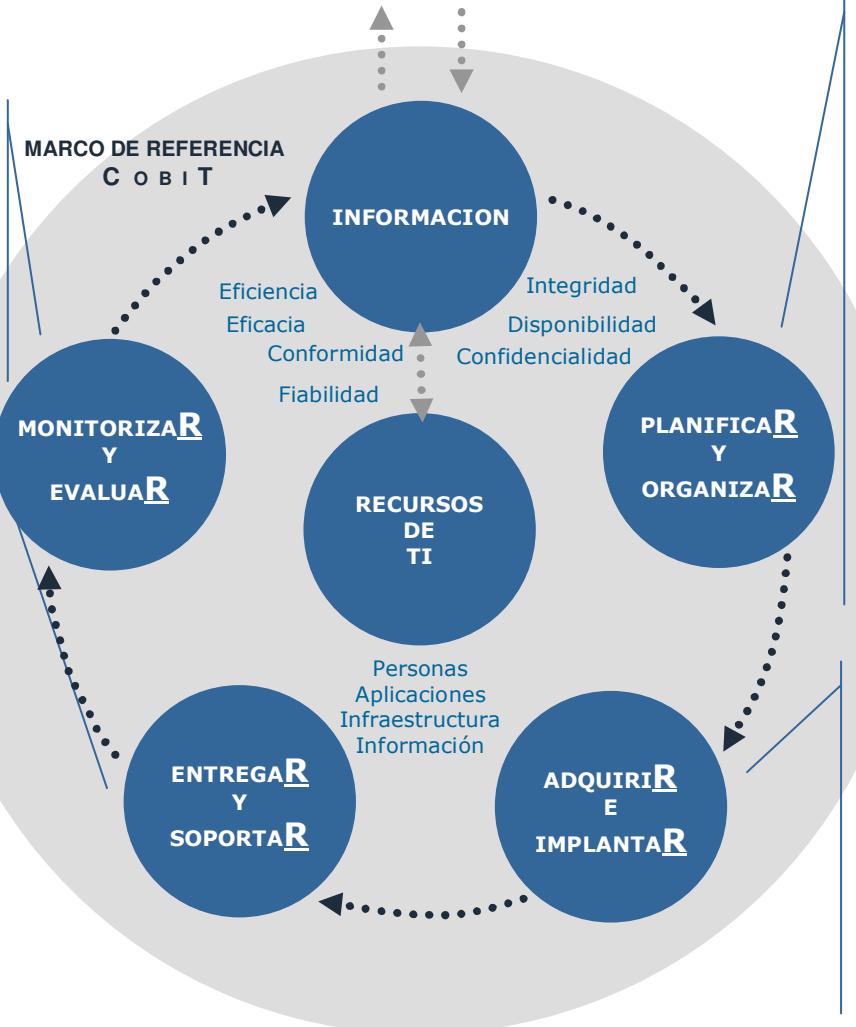


OBJETIVOS DE CONTROL

El conjunto estructurado de 34 PROCESOS [objetivos de control de alto nivel] se agrupa de forma natural en 4 DOMINIOS.

- ▶ [PO] **PLANIFICAR y ORGANIZAR** 10 Procesos de TI
- ▶_[AI] **ADQUIRIR e IMPLANTAR** 07 Procesos de TI
- ▶_[DS] **ENTREGAR y SOPORTAR** (dar soporte) 13 Procesos de TI
- ▶_[ME] **MONITORIZAR y EVALUAR** 04 Procesos de TI

OBJETIVOS DE LA ENTIDAD OBJETIVOS DE GOBIERNO CORPORATIVO



Todos los procesos han de evaluarse periódicamente para verificar su calidad y suficiencia en cuanto a los requisitos de control.

Advierte a la Dirección sobre la necesidad de garantizar procesos de control independientes (auditorías).

Trata la entrega o la prestación de los servicios requeridos - desde las operaciones tradicionales, hasta la formación; pasando por la seguridad en los sistemas y las continuidad de las operaciones -.

Deberán establecerse los procesos necesarios para la provisión de los servicios.

OBJETIVOS DE CONTROL

Cubre las estrategias y las tácticas para identificar la forma en la que la TI puede contribuir de la mejor manera al logro de los objetivos de la Organización.

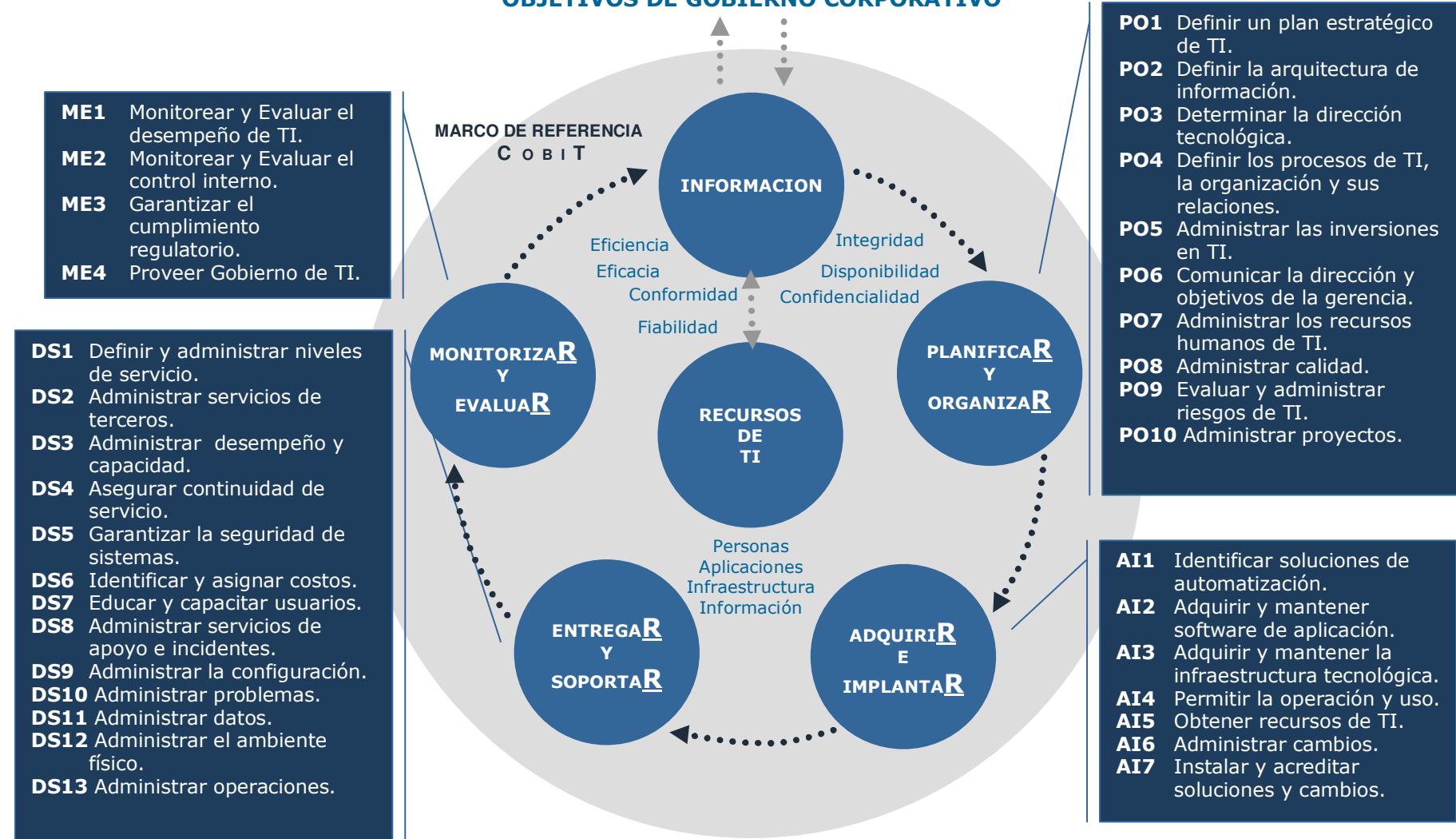
La consecución de la visión estratégica debe planearse, comunicarse y gestionarse desde diferentes perspectivas.

Es necesario establecer una organización e infraestructura tecnológica apropiada.

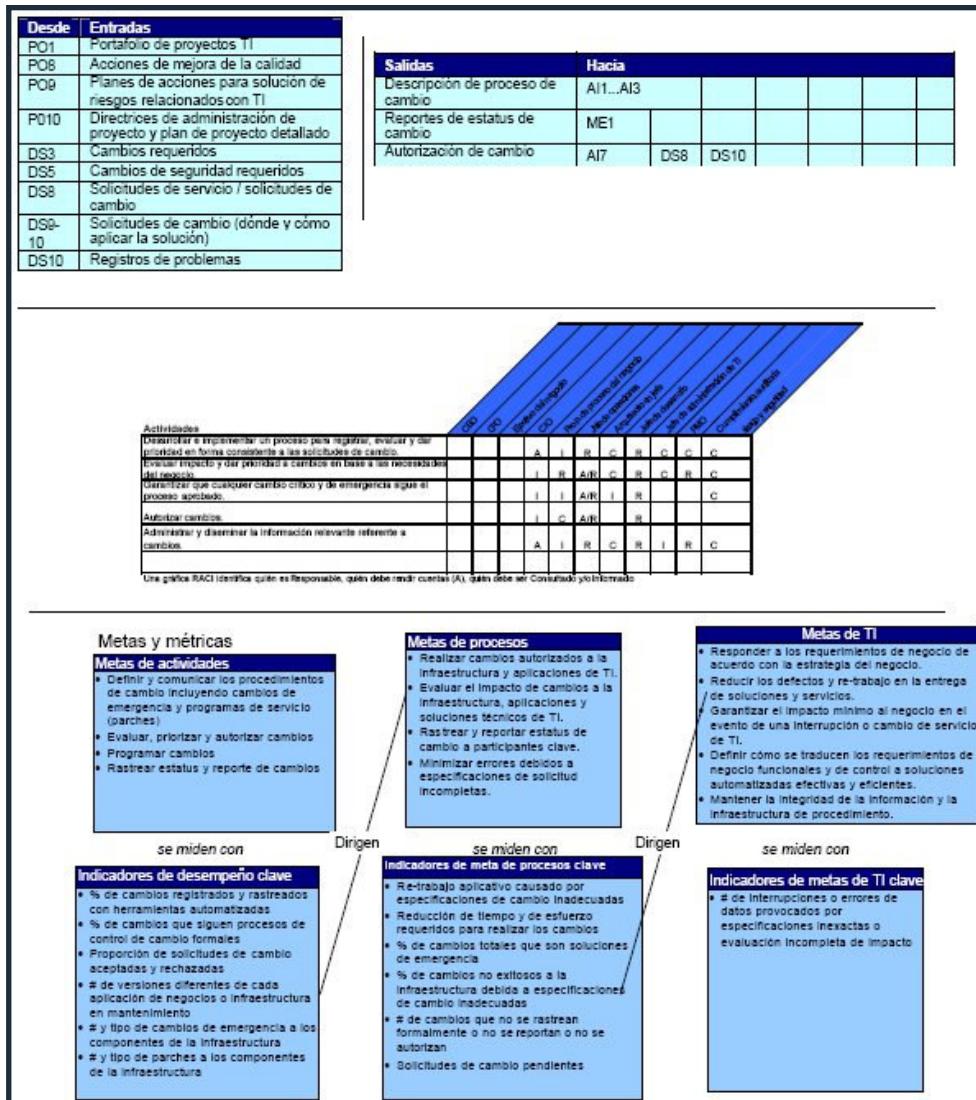
Para llevar a cabo la estrategia de TI, éstas deben identificarse, construirse o adquirirse, implantándose e integrándose en el proceso de la Organización.

Contempla, asimismo, los cambios y mantenimiento de sistemas existentes, para garantizar su continuidad.

OBJETIVOS DE LA ENTIDAD OBJETIVOS DE GOBIERNO CORPORATIVO



DIRECTRICES DE GESTIÓN



Entradas y Salidas del Proceso

Actividades y Matriz RACI

Objetivos (metas) de TI Objetivos (metas) de los procesos Objetivos (metas) de las actividades

KGI - Indicadores clave de objetivos KPI - Indicadores clave de rendimiento

DIRECTRICES DE GESTIÓN. MODELOS DE MADUREZ

Los **MODELOS DE MADUREZ**, ayudarán a la organización a dar respuesta a los siguientes interrogantes:

¿Dónde nos encontramos? (Estado actual de la organización)

¿Cuál es la referencia de la industria? (Estado actual de las normas internacionales)

¿Dónde está la competencia? (Estado actual del “mejor de la clase”)

¿Dónde queremos llegar? (Estrategia de mejora de la entidad)



ENTERPRISE VALUE: GOVERNANCE OF IT INVESTMENTS

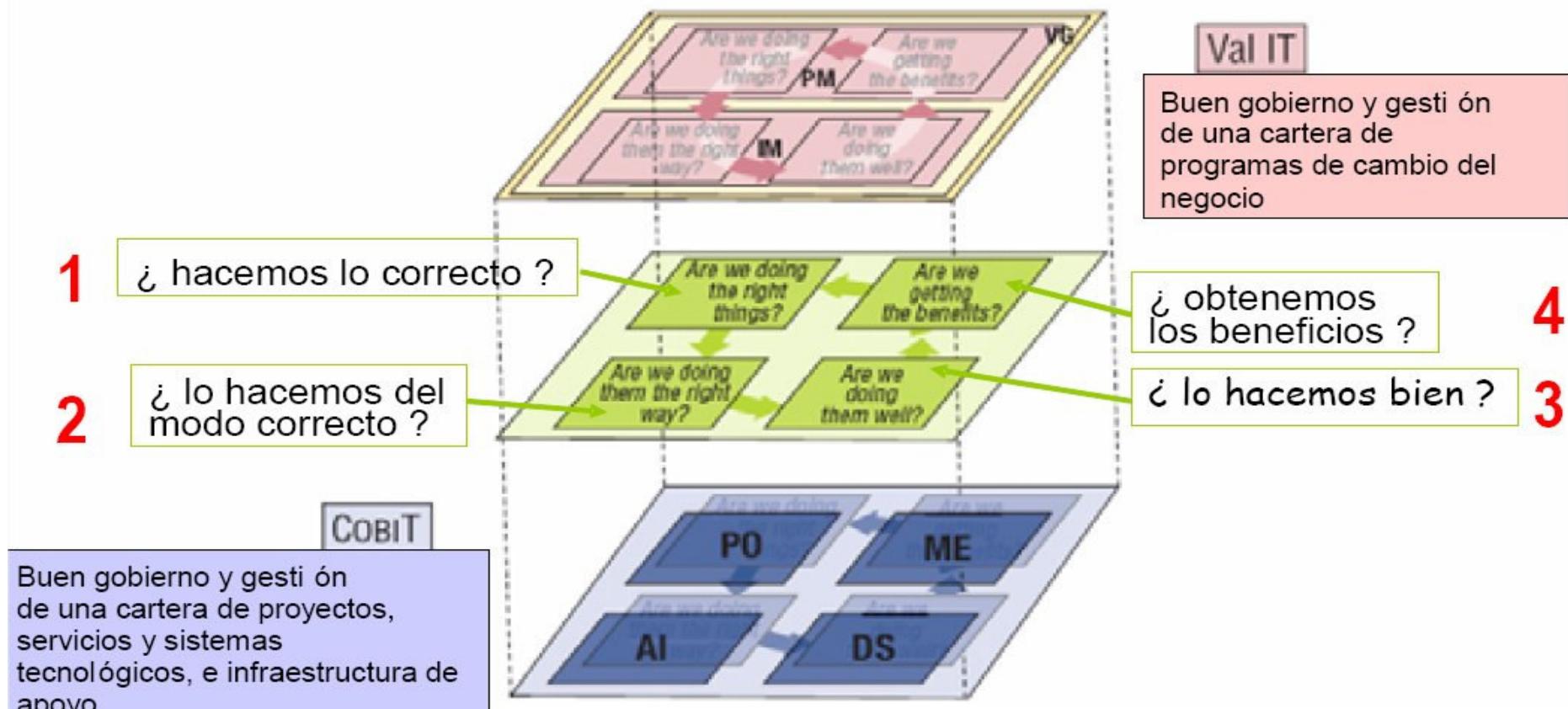
The Val IT Framework







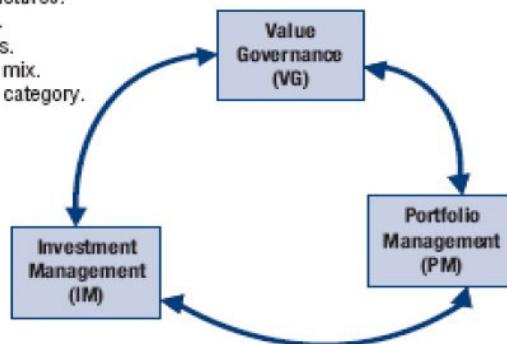
Val IT™ y CobiT®, complementarios; **dos planes distintos**



Val IT ofrece un marco complementario al de CobiT; pero con un enfoque estratégico y de gobernanza, al más alto nivel.

Procesos y prácticas clave de Gobernanza de Valor

- VG1 Ensure informed and committed leadership.
- VG2 Define and implement processes.
- VG3 Define roles and responsibilities.
- VG4 Ensure appropriate and accepted accountability.
- VG5 Define information requirements.
- VG6 Establish reporting requirements.
- VG7 Establish organisational structures.
- VG8 Establish strategic direction.
- VG9 Define investment categories.
- VG10 Determine a target portfolio mix.
- VG11 Define evaluation criteria by category.



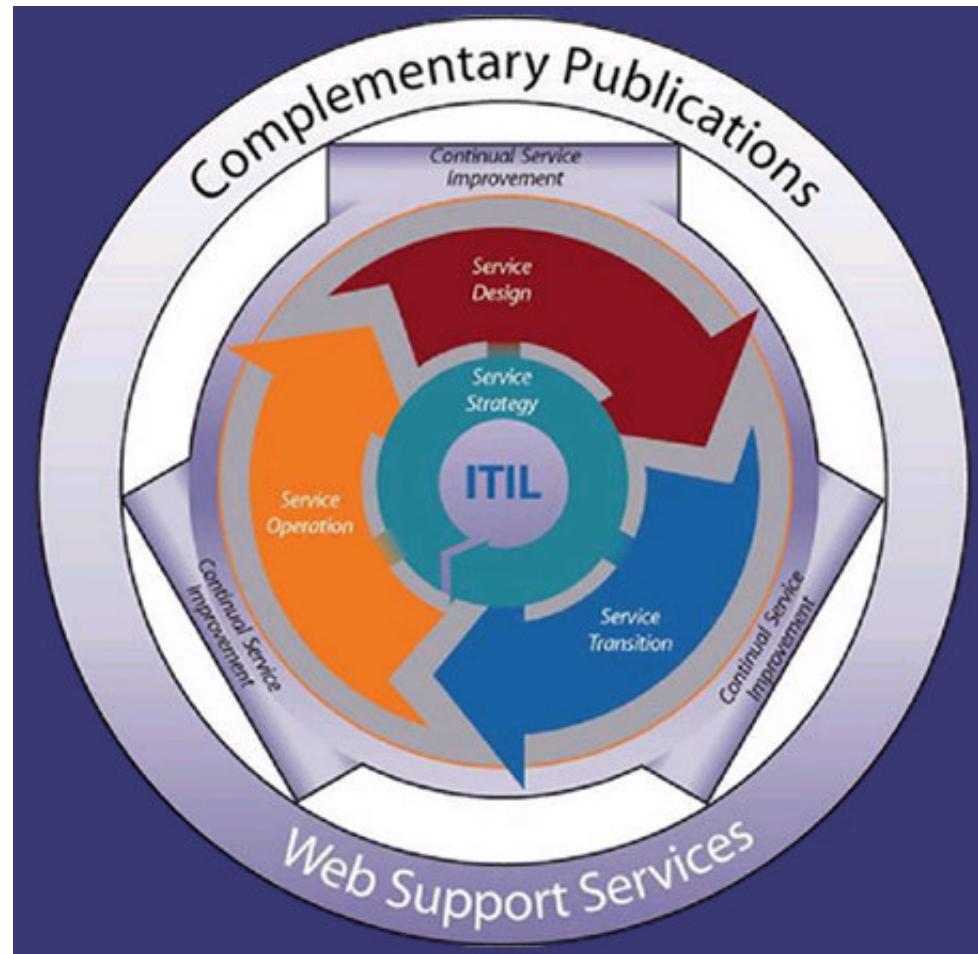
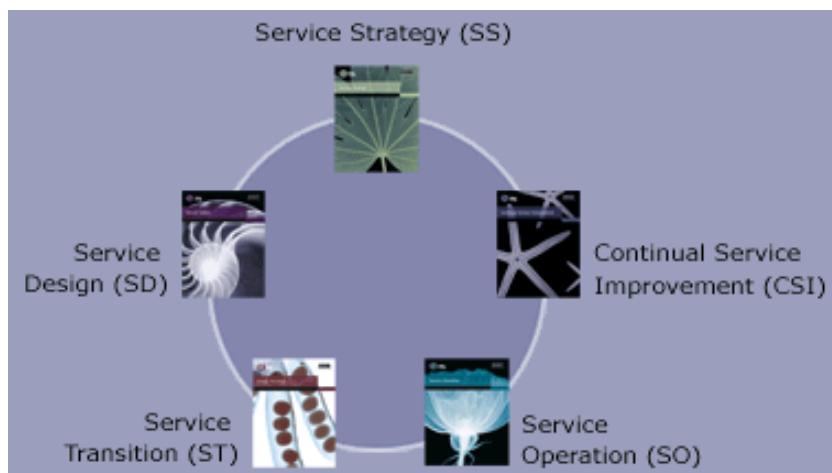
- IM1 Develop a high-level definition of investment opportunity.
- IM2 Develop an initial programme concept business case.
- IM3 Develop a clear understanding of candidate programmes.
- IM4 Perform alternatives analysis.
- IM5 Develop a programme plan.
- IM6 Develop a benefits realisation plan.
- IM7 Identify full life cycle costs and benefits.
- IM8 Develop a detailed programme business case.
- IM9 Assign clear accountability and ownership.
- IM10 Initiate, plan and launch the programme.
- IM11 Manage the programme.
- IM12 Manage/track benefits.
- IM13 Update the business case.
- IM14 Monitor and report on programme performance.
- IM15 Retire the programme.

- PM1 Maintain a human resource inventory.
- PM2 Identify resource requirements.
- PM3 Perform a gap analysis.
- PM4 Develop a resourcing plan.
- PM5 Monitor resource requirements and utilisation.
- PM6 Establish an investment threshold.
- PM7 Evaluate the initial programme concept business case.
- PM8 Evaluate and assign a relative score to the programme business case.
- PM9 Create an overall portfolio view.
- PM10 Make and communicate the investment decision.
- PM11 Stage-gate (and fund) selected programmes.
- PM12 Optimise portfolio performance.
- PM13 Re-prioritise the portfolio.
- PM14 Monitor and report on portfolio performance.

Val ITTM

Val IT consta de tres (3) PROCESOS,
soportados en un total de cuarenta (40) PRÁCTICAS clave de gobernanza

Gestión y Calidad del Servicio TIC





International
Organization for
Standardization

ISO/IEC 17799:2005, *Code of Practice for Information Security Management*

Año: 2005 (primera edición, 2000)

Editor: International Organization for Standardization (ISO)

URL: <http://www.iso.ch>

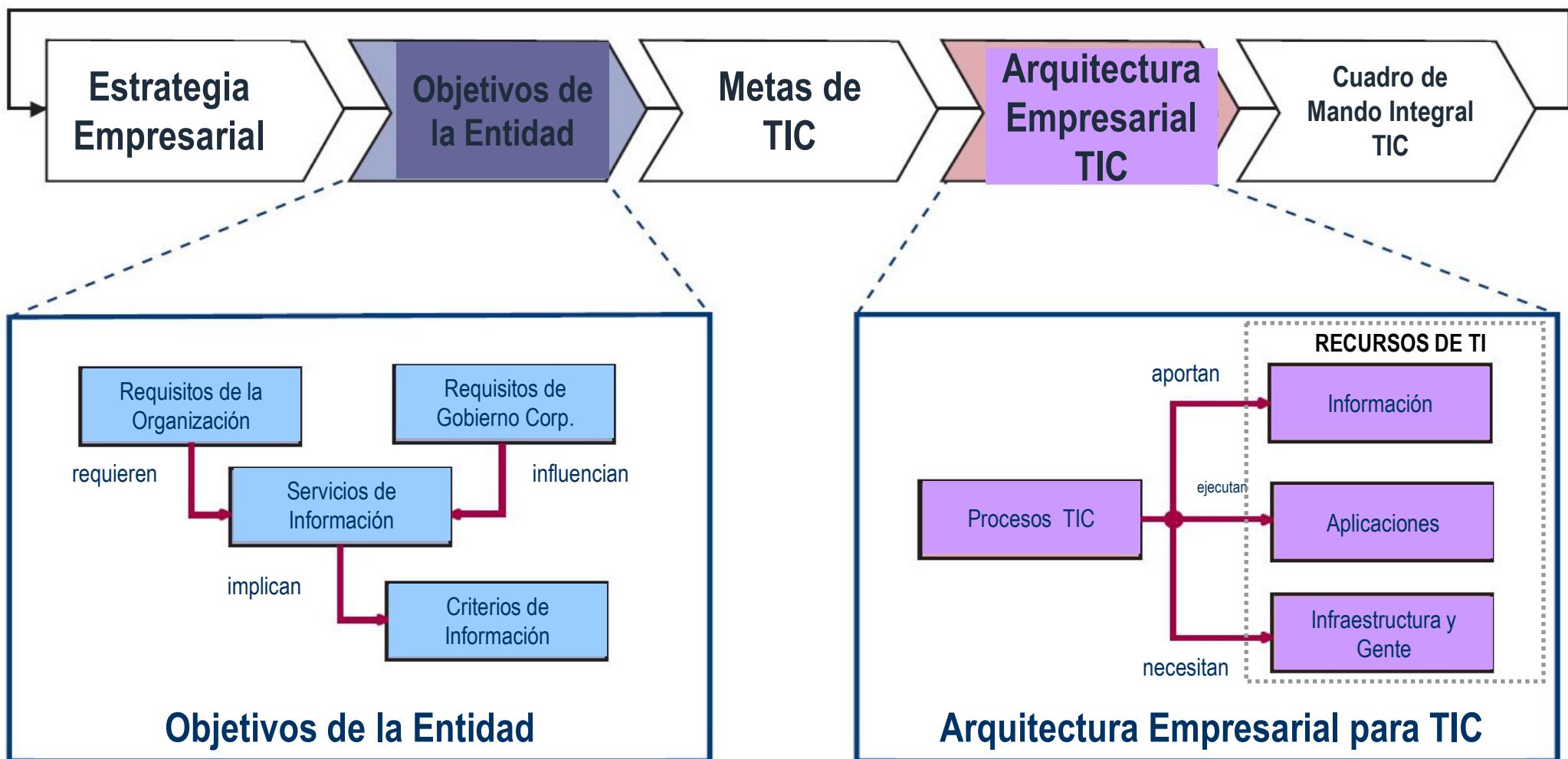
11 Áreas de Control

- Política de Seguridad
- Organización de la Seguridad de la Información
- Gestión de Activos
- Seguridad en los Recursos Humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de incidentes de seguridad
- Gestión de continuidad del negocio
- Conformidad

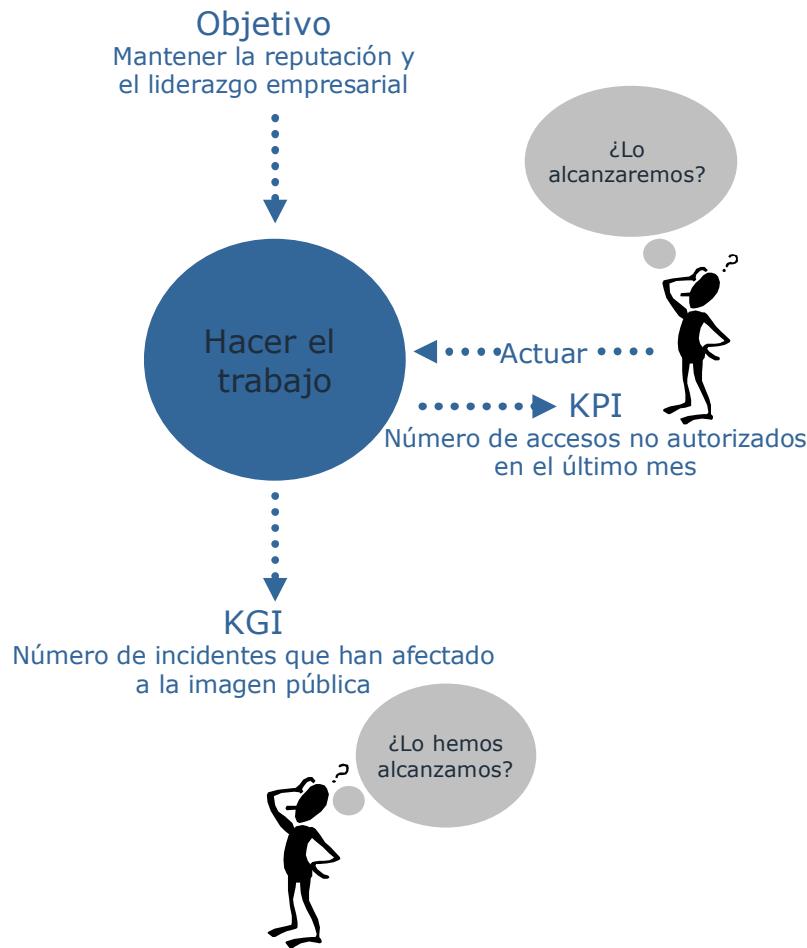
Continuidad de Negocio



Marco de Referencia. Definiendo las metas TIC y la arquitectura empresarial TIC



Objetivos e indicadores

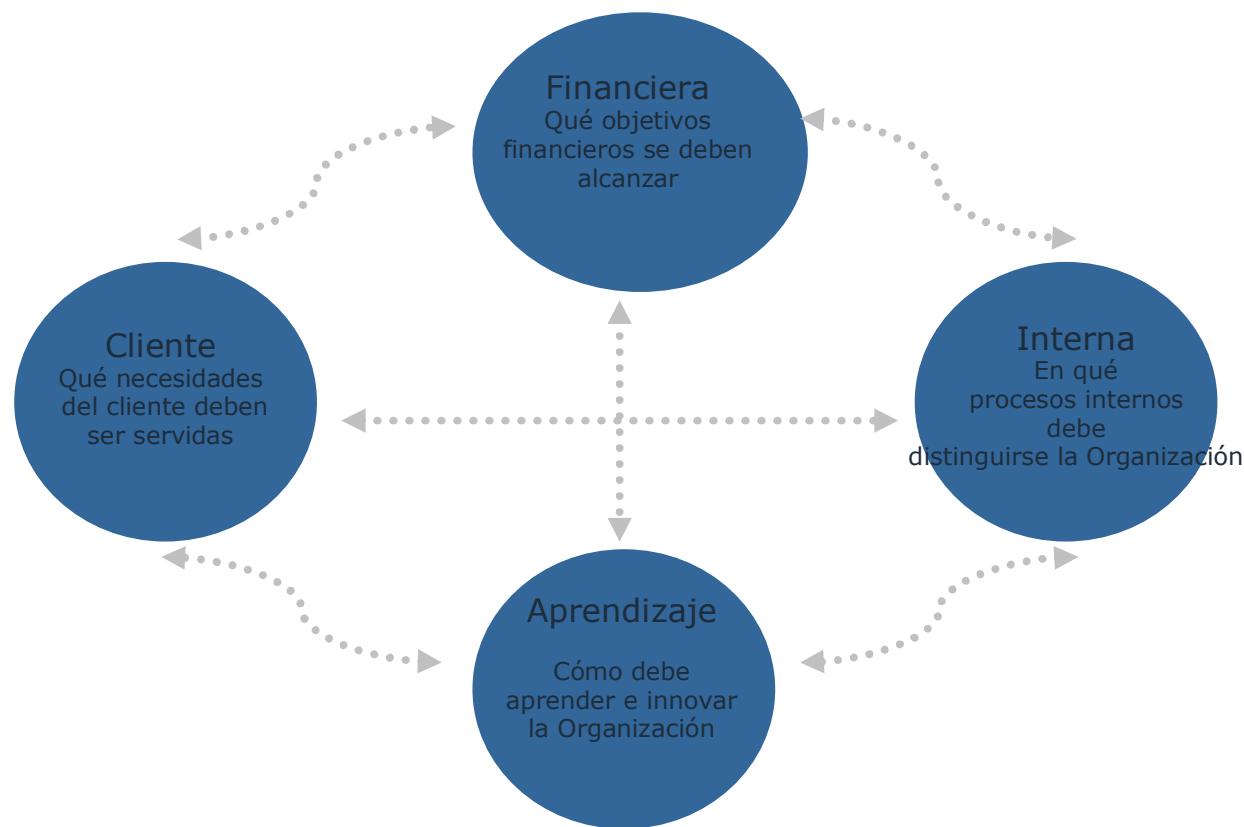


- **KPI (Key Performance Indicator / Indicador Clave de Rendimiento):**

Indican cómo se está desarrollando el proceso, cuál está siendo su comportamiento.
Predicen la probabilidad es éxito o fracaso en el futuro. Son indicadores “guía”.
Ayudarán a mejorar el proceso de Seguridad de la Información cuando sean medidos y se actúe sobre ellos.
- **KGI (Key Goal Indicator / Indicador Clave de Meta u Objetivo):**

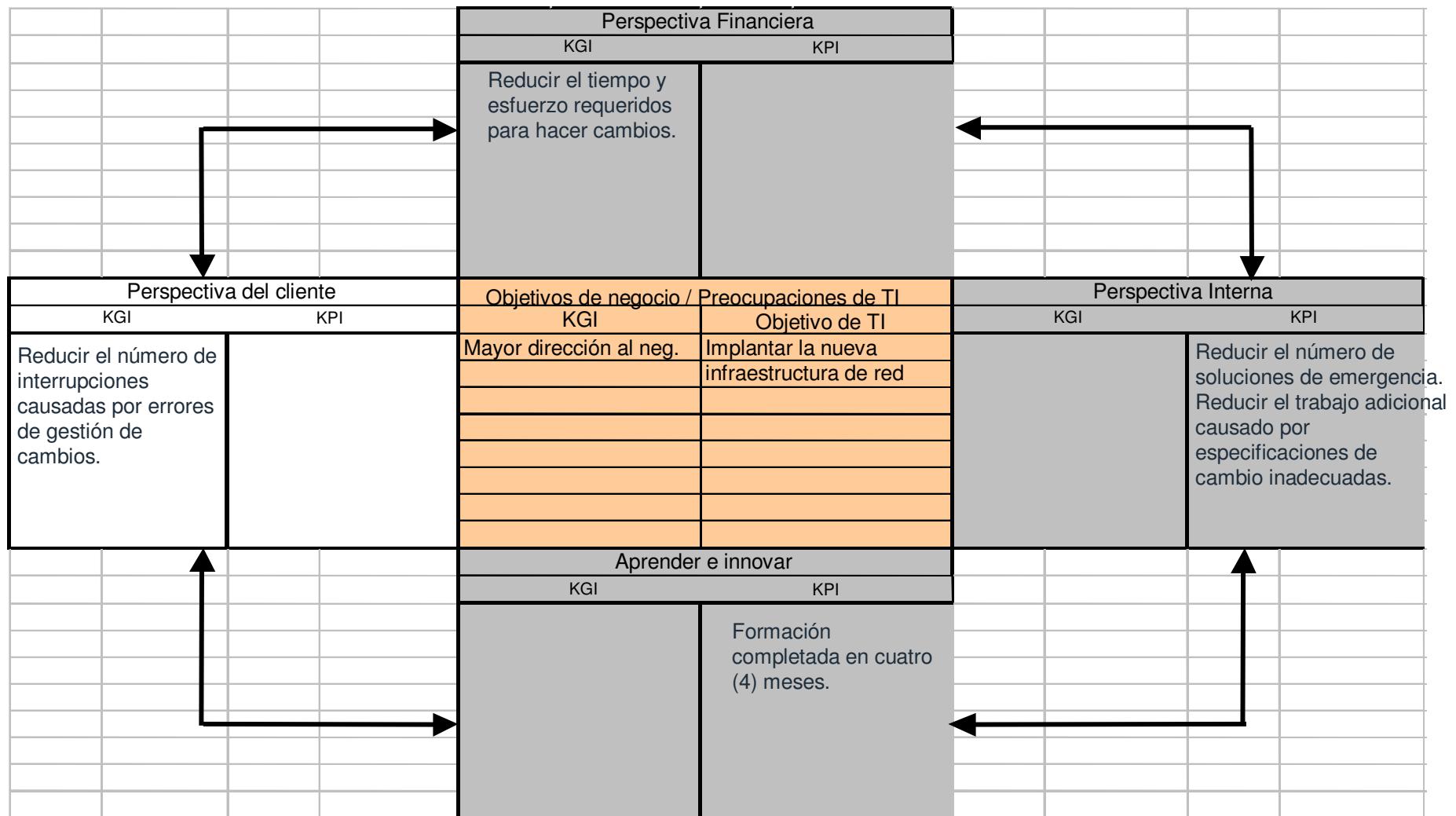
Indican, después del hecho, si un determinado objetivo se ha alcanzado.

Cuadro de Mando Integral TIC



- El **Cuadro de Mando Integral (BSC, *Balanced ScoreCard*)** presenta el rendimiento desde cuatro perspectivas.
- Los **KGI** hacen referencia a las vertientes financiera y del cliente, dentro del BSC.
- Los **KPI** se enfocan hacia el proceso y la dimensión del aprendizaje.

Cuadro de Mando Integral. Un ejemplo



Las directrices de auditoría de COBIT Orientan en la preparación de programas de auditoría, a través de una estructura comúnmente aceptada del PROCESO de AUDITORÍA ...



... basada en:

[ADQUIRIR] conocimiento, a través de:

- entrevistando ...
- obteniendo ...

[EVALUAR] la conveniencia de los controles establecidos:

- considerando ...

[VALORAR] la suficiencia:

- probando que ...

[JUSTIFICAR] el riesgo de que los objetivos de control no se alcancen:

- ejecutando ...
- identificando ...

PROCESO DE AUDITORÍA

IS Standards, Guidelines and Procedures for Auditing and Control Professionals

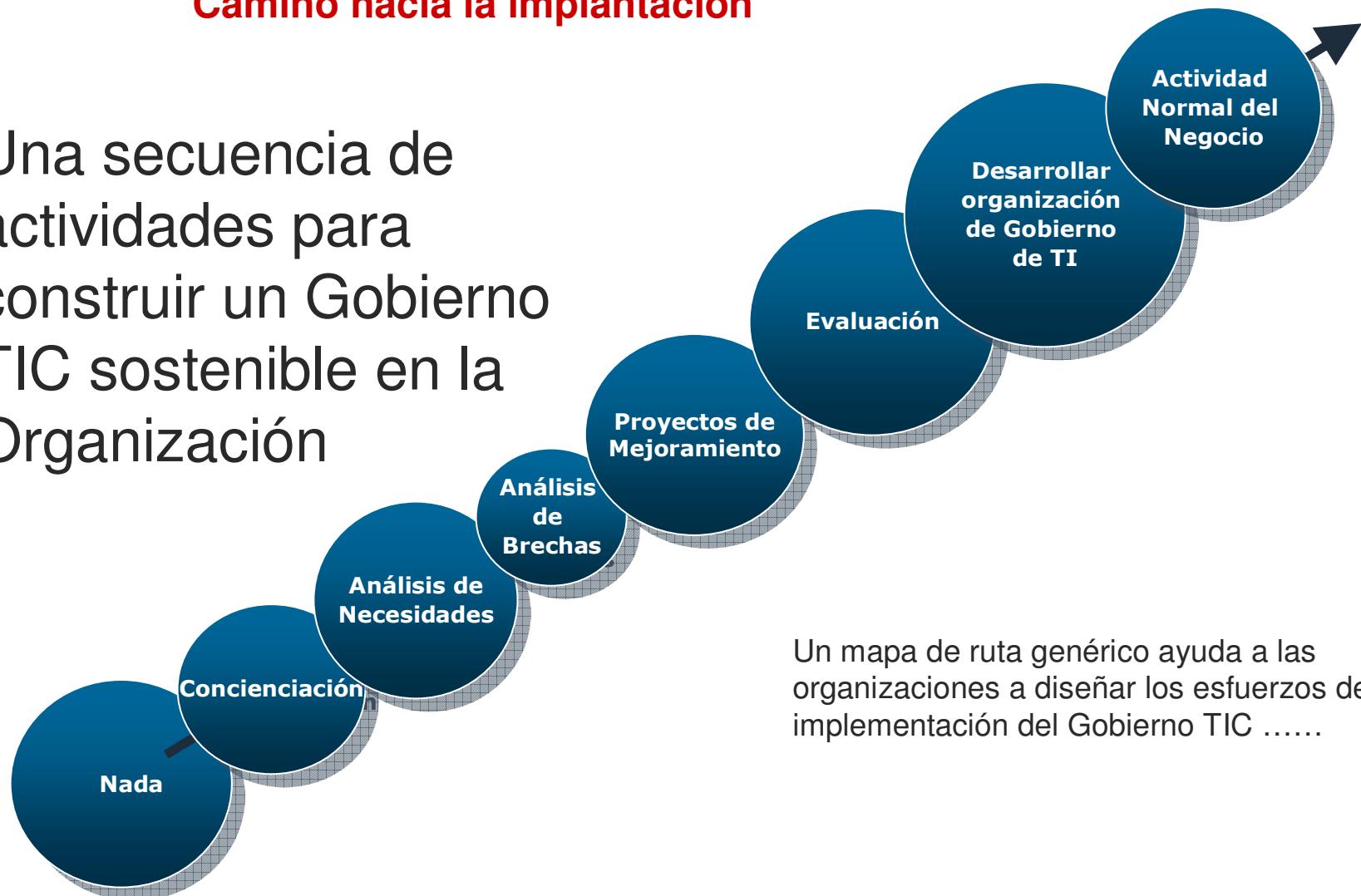
- Code of Professional Ethics
- IS Auditing Standards, Guidelines and Procedures
- IS Control Professionals Standards



Current as of 1 May 2003

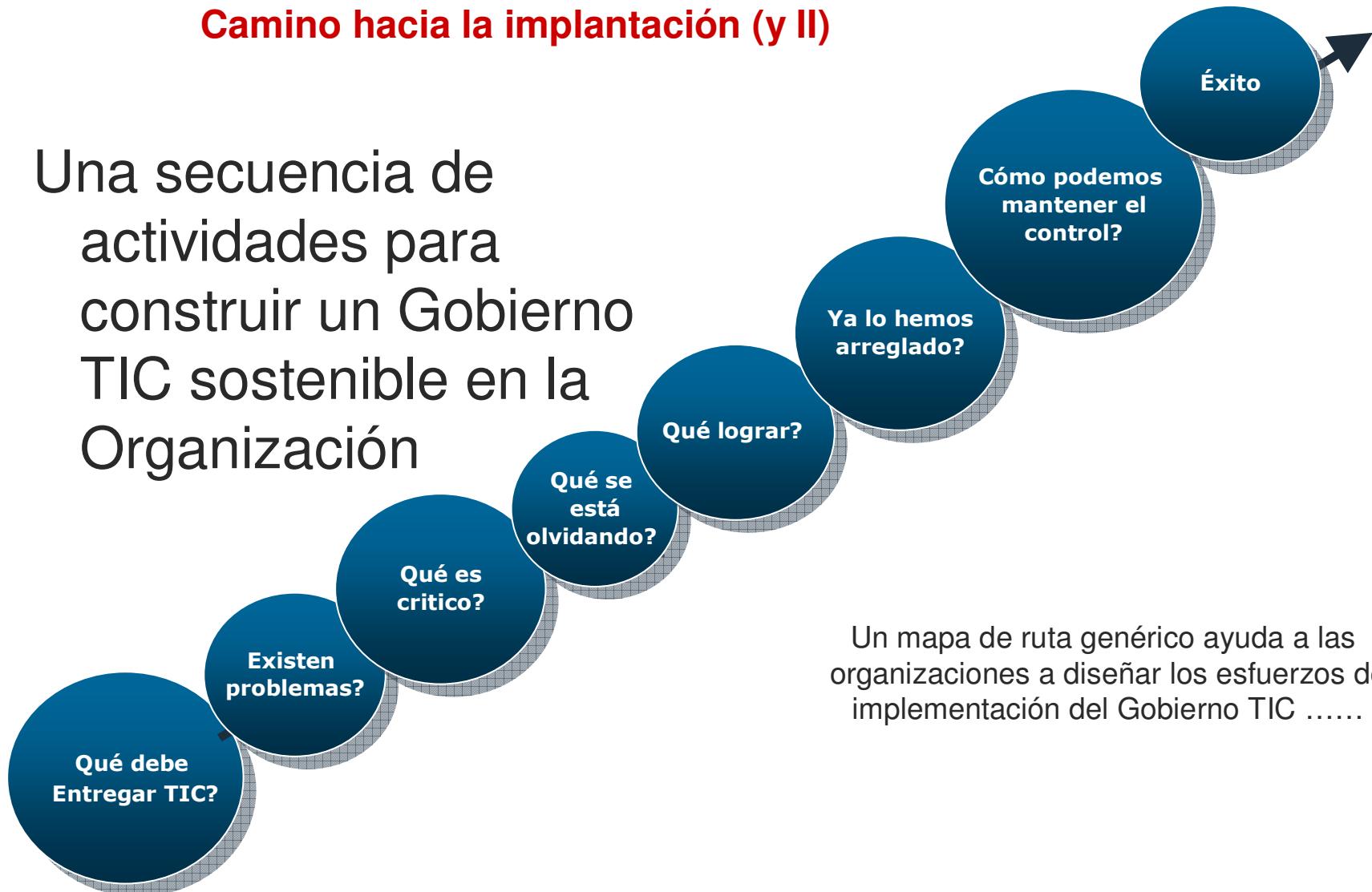
Camino hacia la implantación

Una secuencia de actividades para construir un Gobierno TIC sostenible en la Organización



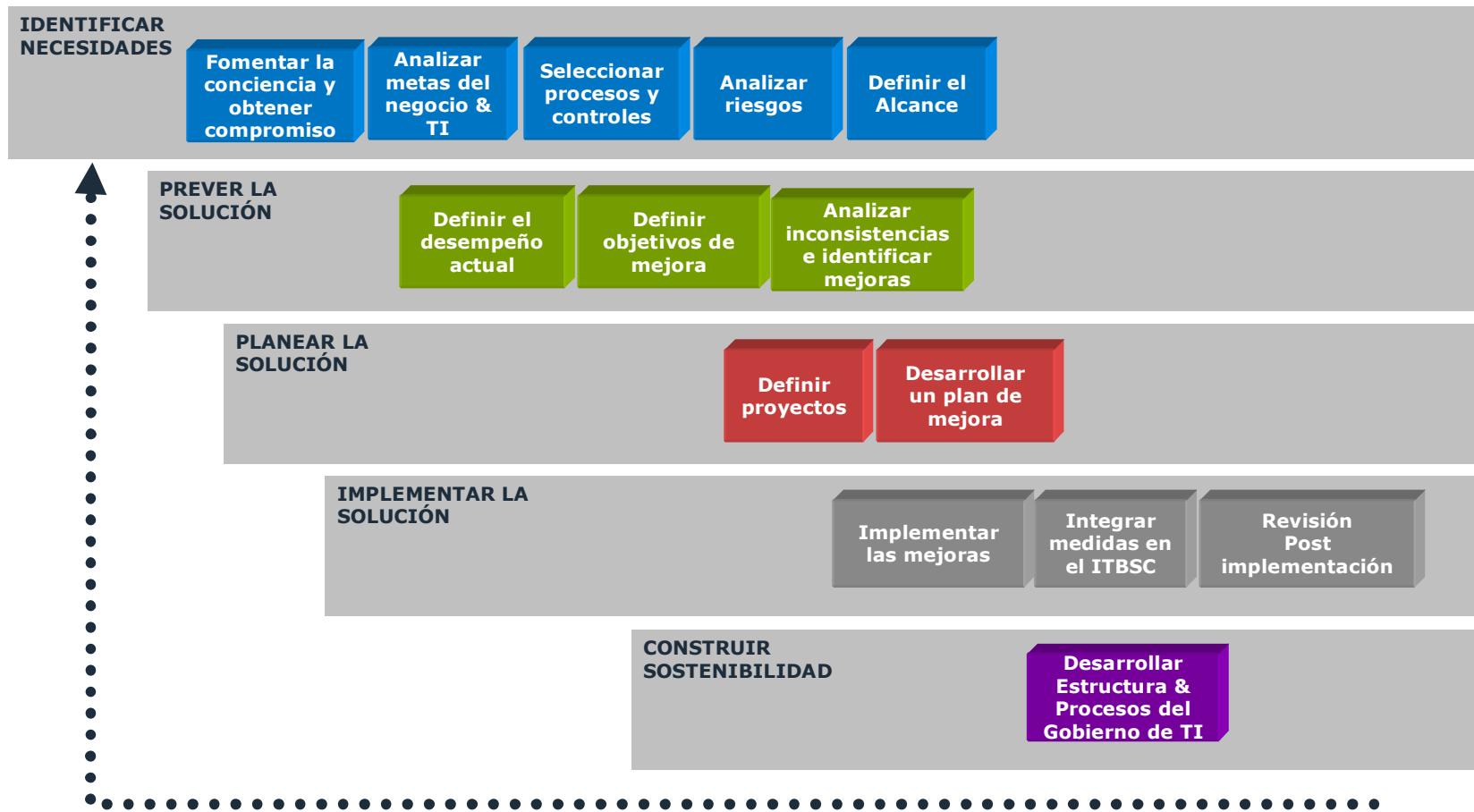
Camino hacia la implantación (y II)

Una secuencia de actividades para construir un Gobierno TIC sostenible en la Organización



Un mapa de ruta genérico ayuda a las organizaciones a diseñar los esfuerzos de implementación del Gobierno TIC

Hoja de Ruta de Implementación Gobernanza TIC



Procesos de Negocio – Asignación de Responsables

Meycor COBIT AG v.3.1.2 - [Mantenimiento de Procesos de Negocios]

Archivo Edición Planillas Proyectos Centros de Análisis Evaluaciones Supervisión Administración Informes Ventana ?

Reportes

Procesos de Negocios

- Applications Development
- Client Accounts
- Electronic Banking
- Foreign Payment
- Investments

Unidades

- Board of Directors
- Senior Management
- Business Operational
 - Client Accounts
 - Electronic Banking
- Financial Management
- Business Management
 - Business Strategic Group
 - Electronic Banking
 - IT Management
 - Electronic Banking
 - IT Teams
 - Electronic Banking

Proceso Applications Development

Descripción

Documentación

Comentarios

Agregar Modificar Borrar Actualizar Cancelar

Actualizar Desasignar Cerrar

Usuario: WDAVIS Proyecto: Project 1 Centro: CENTER

Inicio Meycor COBIT AG v.... ES 11:21

Relación Procesos de Negocio – Objetivos de Negocio – Objetivos de TI

Meycor COBIT AG v.3.1.2 - [Mantenimiento de Objetivos de Negocio]

Archivo Edición Planillas Proyectos Centros de Análisis Evaluaciones Supervisión Administración Informes Ventana ?

Reportes

Proceso-Unidad

- Client Accounts(Business Operational)
- Electronic Banking(Business Operational)
- Electronic Banking(Business Strategic Group)
- Electronic Banking(IT Management)
- Electronic Banking(IT Teams)

Objetivos de Negocio

- Electronic Banking(Business Strategic Group)
 - Develop a new solution through better use of resources
 - Develop and test module in 2 months
 - Manage project delivery risks
- Improve Trust Image
 - Improve communications of security
 - Reduce security incidents by 20%
- Reduce Costs
 - Manage availability risks
 - Reduce heads in operations by 10%

Objetivos de TI

Nombre	Descripción
Develop and test module in 2 months	Develop and test module in 2 months
Improve communications of security	Improve communications of security
Manage availability risks	Manage availability risks
Reduce heads in operations by 10%	Reduce heads in operations by 10%
Reduce security incidents by 20%	Reduce security incidents by 20%

Objetivo de Negocio

Nombre:

Descripción:

Agregar Modificar Actualizar Borrar Cancelar Desasignar Cerrar

Usuario: WDAVIS Proyecto: Project 1 Centro: CENTER

Inicio Meycor COBIT AG v.... Documento1 - Micros... ES 11:23

Relación Objetivos de TI – Recursos y Atributos de TI

Meycor COBIT AG v.3.1.2 - [Mantenimiento de Recursos de TI]

Archivo Edición Planillas Proyectos Centros de Análisis Evaluaciones Supervisión Administración Informes Ventana ?

Reportes

Recursos de TI

- Aplicaciones
 - CRM
 - WebOp
- Infraestructura
 - Servidores
 - 5 Unix Servers
 - IBM (Mainframe)
 - Software de Base
 - Windows 2000
 - Telecomunicaciones
 - IT-Net
- Personas
 - IT Development Team
 - IT Manager

Objetivo de TI

- Develop and test module in 2 months
- Improve communications of security
- Manage availability risks
- Manage project delivery risks
- Reduce heads in operations by 10%
 - Personas
 - IT Development Team
 - IT Manager
- Reduce security incidents by 20%

Acciones

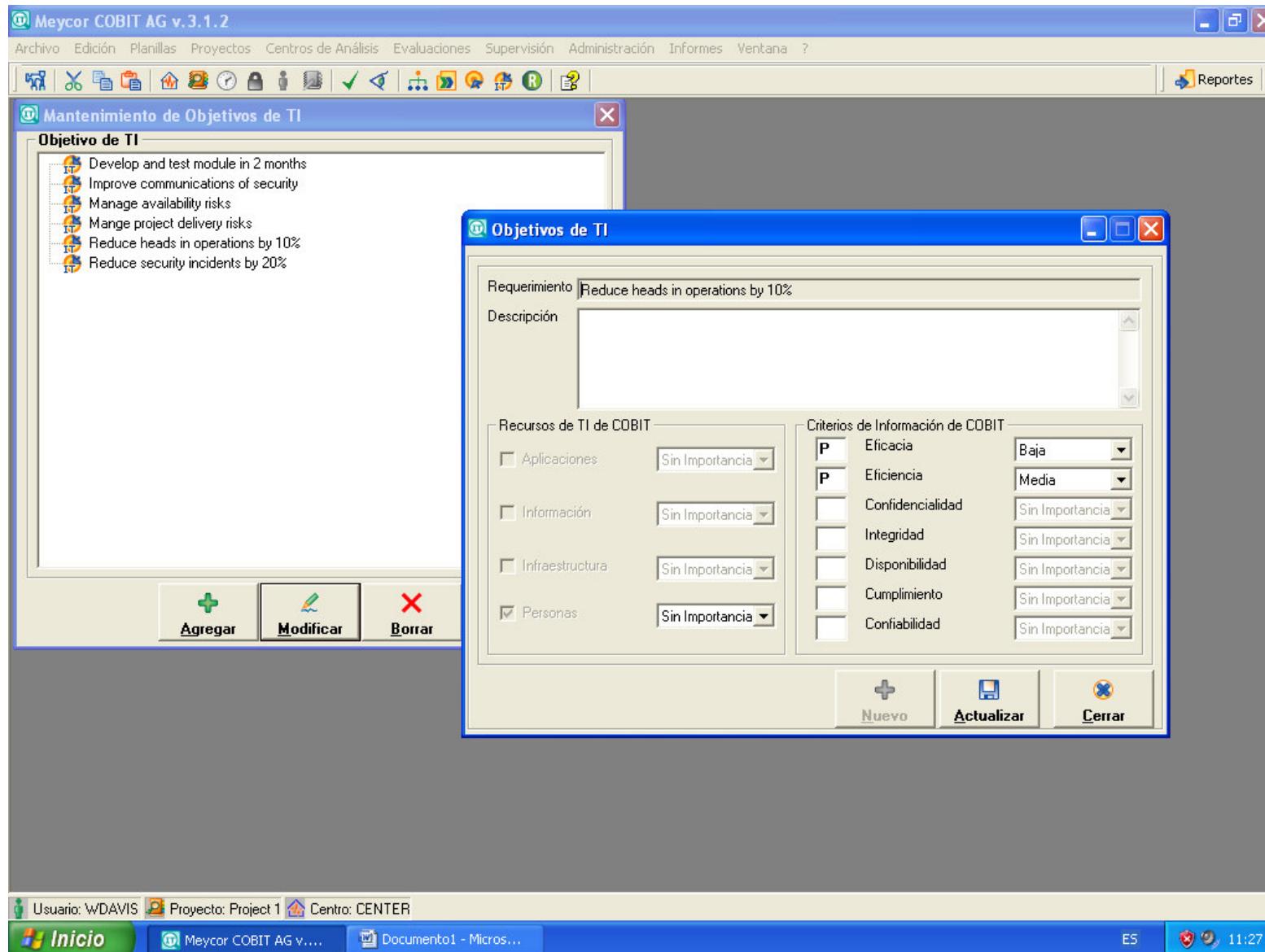
Agregar Modificar Borrar Actualizar Desasignar Cerrar

Usuario: WDAVIS Proyecto: Project 1 Centro: CENTER

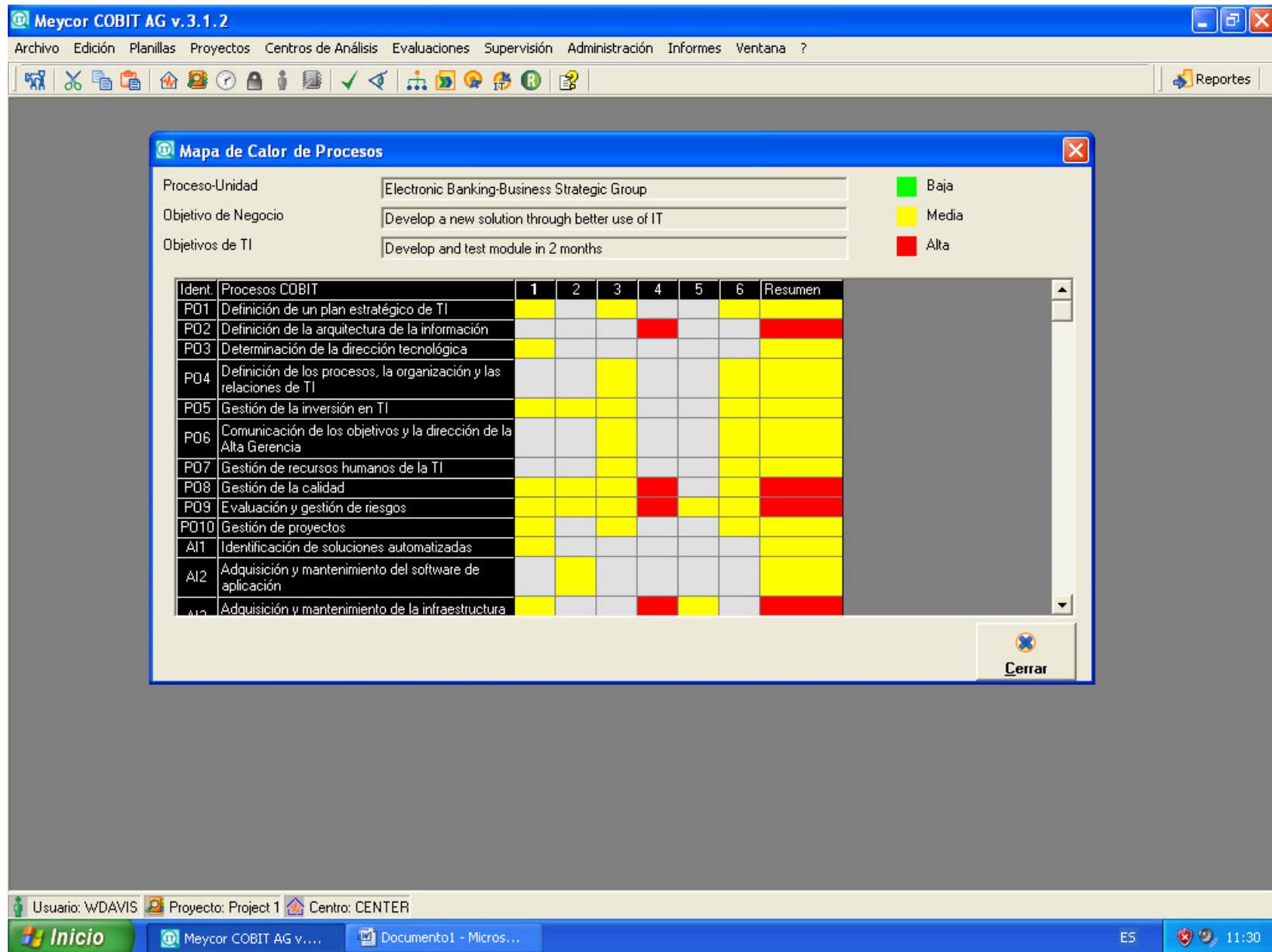
Inicio Meycor COBIT AG v.... Documento1 - Micros... ES 11:26

The screenshot shows a software application window titled 'Meycor COBIT AG v.3.1.2 - [Mantenimiento de Recursos de TI]'. The menu bar includes 'Archivo', 'Edición', 'Planillas', 'Proyectos', 'Centros de Análisis', 'Evaluaciones', 'Supervisión', 'Administración', 'Informes', 'Ventana', and '?'. Below the menu is a toolbar with various icons. The main area is divided into two sections: 'Recursos de TI' (left) and 'Objetivo de TI' (right). The 'Recursos de TI' section contains a tree view with categories like 'Aplicaciones', 'Infraestructura', and 'Personas'. The 'Objetivo de TI' section lists several objectives with associated icons. At the bottom are buttons for 'Añadir', 'Modificar', 'Borrar', 'Actualizar', 'Desasignar', and 'Cerrar'. The status bar at the bottom shows 'Usuario: WDAVIS', 'Proyecto: Project 1', 'Centro: CENTER', and system information like 'ES' and '11:26'.

Evaluación de Objetivos de TI por Criterios de Información y Recursos de TI



Mapa de Calor (Heat Map) de Procesos de TI -> Procesos de COBIT seleccionados



Análisis de Riesgos de procesos TI

Meycor COBIT RM v.2.0.1 - Usuario: ADMIN - Base: DATA - [Evaluación de Riesgos]

Archivo Edición Codificación Entidades Grupos y Revisores Evaluaciones Períodos Ventana ?

Reportes

Revisor ADMIN

PROCESOS y SUB-PROCESOS

- PO1-Definición de un plan estratégico de TI (Gerencia)
- AI6-Gestión de cambios (Gerencia de TI)
- AI7-Instalación y acreditación de soluciones (Grupo)
- DS8-Gestión de incidentes y de la mesa de soporte

OBJETIVOS y FACTORES DE RIESGO

- AI6-Gestión de cambios (Gerencia de TI)
 - 1 - Estándares y procedimientos de cambios
 - 1 - Antecedentes de diferentes versiones instaladas
 - 2 - Elevado número de versiones y métodos
 - 3 - Antecedentes de desviaciones de la configuración
 - 4 - Antecedentes de arreglos de emergencia
 - 5 - Antecedentes de prolongados retrasos en las implementaciones
 - 6 - Baja tasa de solicitudes de implementación

Planificación y Organización

- PO1-Definición de un plan estratégico de TI
 - 1 - KGI
 - 2 - KPI
 - 3 - PO1.1 Administración del valor de TI
 - 5 - PO1.2 Alineación de TI con el negocio
 - 6 - PO1.3 Evaluación del desempeño actual
 - 7 - PO1.4 Plan estratégico de TI
 - 8 - PO1.5 Planes tácticos de TI
 - 9 - PO1.6 Administración del portafolio de TI
- PO2-Definición de la arquitectura de la información
 - 1 - KGI
 - 2 - KPI
 - 3 - PO2.1 Modelo de arquitectura de información empresarial
 - 4 - PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos
 - 5 - PO2.3 Esquema de clasificación de datos
 - 6 - PO2.4 Administración de la integridad
- PO3-Determinación de la dirección tecnológica
 - 1 - KGI
 - 2 - KPI
 - 3 - PO3.1 Planificación de la dirección tecnológica
 - 4 - PO3.2 Plan de infraestructura tecnológica
 - 5 - PO3.3 Monitoreo de tendencias y regulaciones futuras
 - 6 - PO3.3 Monitoreo de tendencias y regulaciones futuras
 - 7 - PO3.4 Estándares tecnológicos
 - 8 - PO3.5 Consejo de arquitectura
- PO4-Definición de los procesos, la organización y las relaciones de TI
 - 1 - KGI
 - 2 - KPI
 - 3 - PO4.1 Marco de trabajo del proceso
 - 4 - PO4.2 Comité estratégico

Objetivo de Proceso Factor de Riesgo Borrar

Objetivos Actualizar Retornar

Inicio Documento1 - Micros... Meycor COBIT RM v.... ES 11:34

Mapa de Riesgos de Procesos de TI

Meycor COBIT RM v.2.0.1 - Usuario: ADMIN - Base: DATA

Archivo Edición Codificación Entidades Grupos y Revisores Evaluaciones Períodos Ventana ?

Evaluación de Riesgos

Revisor ADMIN

PROCESOS y SUB-PROCESOS

PO1-Definición de un plan estratégico de TI (G)
AI6-Gestión de cambios (Gerencia de TI)
AI7-Instalación y acreditación de soluciones (G)
DS8-Gestión

Mapa de Riesgos

OBJETIVOS y

AI6-Gestión
1 - Está
1 - A
2 - B
3 - A
4 - A
5 - A
6 - B

Objetivo de Proceso

Referencias

Unidad [Todas]
Proceso [Todos]

Nro	Factor de Riesgo	Probabilidad
1	La encuesta a la gerencia no puede detectar el riesgo	Baja
2	Bajo porcentaje de unidades de negocio que tienen un plan estratégico	Baja
3	Bajo porcentaje del presupuesto de TI destinado a la implementación de cambios	Baja
4	Cantidad inaceptable o poco razonable de cambios	Baja
5	Bajo porcentaje de planes estratégicos de TI que cumplen con los objetivos establecidos	Baja
6	Bajo porcentaje de unidades de negocio que tienen una estrategia de TI clara	Baja
7	Escasa satisfacción de los participantes en las reuniones de planeamiento	Baja
8	Antecedentes de prolongados retrasos en la implementación de cambios	Baja
9	Falta de un índice de participantes involucrados en la evaluación	Baja
10	Falta de un índice de calidad del plan, o que no cumple con las expectativas	Baja
11	Falta de vigencia de la evaluación de las estrategias de TI	Baja
12	Avanzada edad del plan estratégico de TI	Baja
13	Antecedentes de diferentes versiones inconsistentes	Baja
14	Elevado número de versiones y métodos utilizados	Baja
15	Antecedentes de desviaciones de la estrategia	Baja
16	Antecedentes de arreglos de emergencia	Baja
17	Antecedentes de prolongados retrasos en la implementación de cambios	Baja
18	Raya tasa de solvencias de implementación	Baja

Imagen

Retornar

IMPACTO

Alta
Media
Baja

Bajo
Medio
Alto

Evaluación de procesos por Madurez (Gap Análisis)

Meycor COBIT MG v.3.1.1 - Guías de Gerenciamiento - Usuario: ADMIN Centro: Data Center - [Evaluación del Modelo de Maduración]

Archivo Edición Evaluaciones Proyectos Informes Períodos Administración Ventana ?

Reportes

Proceso
DS8 | 25 - Gestión de incidentes y de la mesa de soporte

Evaluación
Nivel Sugerido: 0 - Inexistente
Evaluación Actual: 1 - Inicial / Ad Hoc
Objetivo: 2 - Repetitivo pero intuitivo
Brecha (0 a 5): 1

Comentario:

Generar Actualizar

Recomendaciones

Cod.	Descripción
1	Proceso para responder a las consultas de los
2	Necesidad de una función de mesa de soporte
3	Herramientas comunes
4	Disponibilidad de asistencia

+ Planificación y organización
+ Adquisición e implementación
Entrega y soporte
18 - Definición de los niveles de servicio
19 - Gestión de los servicios prestados por terceros
20 - Gestión de la capacidad y del desempeño del sistema
21 - Aseguramiento de la continuidad del servicio
22 - Aseguramiento de la seguridad de los sistemas
23 - Identificación y asignación de costos
24 - Educación y capacitación de los usuarios
25 - Gestión de incidentes y de la mesa de soporte
26 - Gestión de la configuración
27 - Gestión de problemas
28 - Gestión de datos
29 - Gestión del entorno físico
30 - Gestión de operaciones
Monitoreo y evaluación

Anterior Siguiente Retornar

Inicio MEYCOR.doc [Modo ...] Meycor COBIT MG v.... ES 16:10

Evaluación y Análisis de Recomendaciones

Meycor COBIT MG v.3.1.1 - Guías de Gerenciamiento - Usuario: ADMIN Centro: Data Center

Archivo Edición Evaluaciones Proyectos Informes Períodos Administración Ventana ?

Reportes

Proyectos Recomendaciones

Definir un plan estratégico de TI

Recomendaciones

Proceso	Indicador	Cod.	Recomendación	Impacto	Costo
1	Modelo	1	Discusión de la planificación estratégica de TI		
1	Modelo	2	Riesgos y beneficios de usuario de las decisiones estratégicas		
1	Modelo	3	Compartir la planificación estratégica		
1	Modelo	4	Discusión de la planificación estratégica		
1	Modelo	5	Política de planificación estratégica		
1	Modelo	6	Definición de la posición ante riesgos		
1	Modelo	7	Proceso de planificación estratégica		
2	Modelo	1	Comunicación de la necesidad de una arquitectura de la información		
2	Modelo	4	Desarrollo de componentes de la arquitectura de la información		
29	Modelo	4	Recuperación de recursos		
29	Modelo	7	Monitoreo de efectividad		

Lista de Recomendaciones del Proyecto

Definir un plan estratégico de TI

Sel.	Proceso	Indicador	Cod.	Recomendación	Impacto	Costo
<input checked="" type="checkbox"/>	1	Modelo	1	Discusión de la planificación estratégica de TI		
<input checked="" type="checkbox"/>	1	Modelo	2	Riesgos y beneficios de usuario de las decisiones estratégicas		
<input checked="" type="checkbox"/>	1	Modelo	3	Compartir la planificación estratégica de TI		
<input checked="" type="checkbox"/>	1	Modelo	4	Discusión de la planificación estratégica de TI		
<input checked="" type="checkbox"/>	1	Modelo	5	Política de planificación estratégica de TI		
<input checked="" type="checkbox"/>	1	Modelo	6	Definición de la posición ante riesgos		
<input checked="" type="checkbox"/>	1	Modelo	7	Proceso de planificación de TI sólido		
	1	Modelo	8	Adquisición de nuevos productos y tecnologías		
	1	Modelo	9	Discusión de la planificación estratégica de TI		
	1	Modelo	10	Riesgos y beneficios de usuario de las decisiones estratégicas		
	1	Modelo	11	Compartir la planificación estratégica de TI		
<input checked="" type="checkbox"/>	2	Modelo	1	Comunicación de la necesidad de una arquitectura de la información		
	2	Modelo	2	Necesidad de una arquitectura de la información		
	2	Modelo	3	Definiciones que consideran datos		
<input checked="" type="checkbox"/>	2	Modelo	4	Desarrollo de componentes de la arquitectura de la información		
	2	Modelo	5	Desarrollo de un proceso y procedimientos de arquitectura de la información		
	2	Modelo	6	Requerimientos tácticos		
	2	Modelo	7	Adquisición de habilidades a través de la práctica		
	5	Modelo	1	Justificación de inversiones de TI		

Retornar

Inicio MEYCOR.doc [Modo ...] Meycor COBIT MG v.... ES 16:11

Proyectos basadas en la Recomendaciones

Meycor COBIT MG v.3.1.1 - Guías de Gerenciamiento - Usuario: ADMIN Centro: Data Center

Archivo Edición Evaluaciones Proyectos Informes Períodos Administración Ventana ?

Reportes

Proyectos

Cod.	Descripción	Impacto	Costo	Fecha de creación	Fecha de iniciación	Fecha de finalización
1	Definir un plan estratégico de TI	9	4	10/01/2006		
2	Definir una metodología de análisis de riesgos de TI	8	4	10/01/2006		
3	Establecer una función de auditoría de TI	9	5	10/01/2006		
4	Formalizar y monitorear los servicios de terceras partes	7	5	10/01/2006		
5	Definir una metodología de planificación anual de TI	5	2	10/01/2006		

Código: 1 Nombre: Definir un plan estratégico de TI Categoría: Estratégico

Seguimiento:

Estado: Sin Iniciar Fecha de creación: 10/01/2006 Fecha de iniciación: Fecha de finalización:

Prioridad:

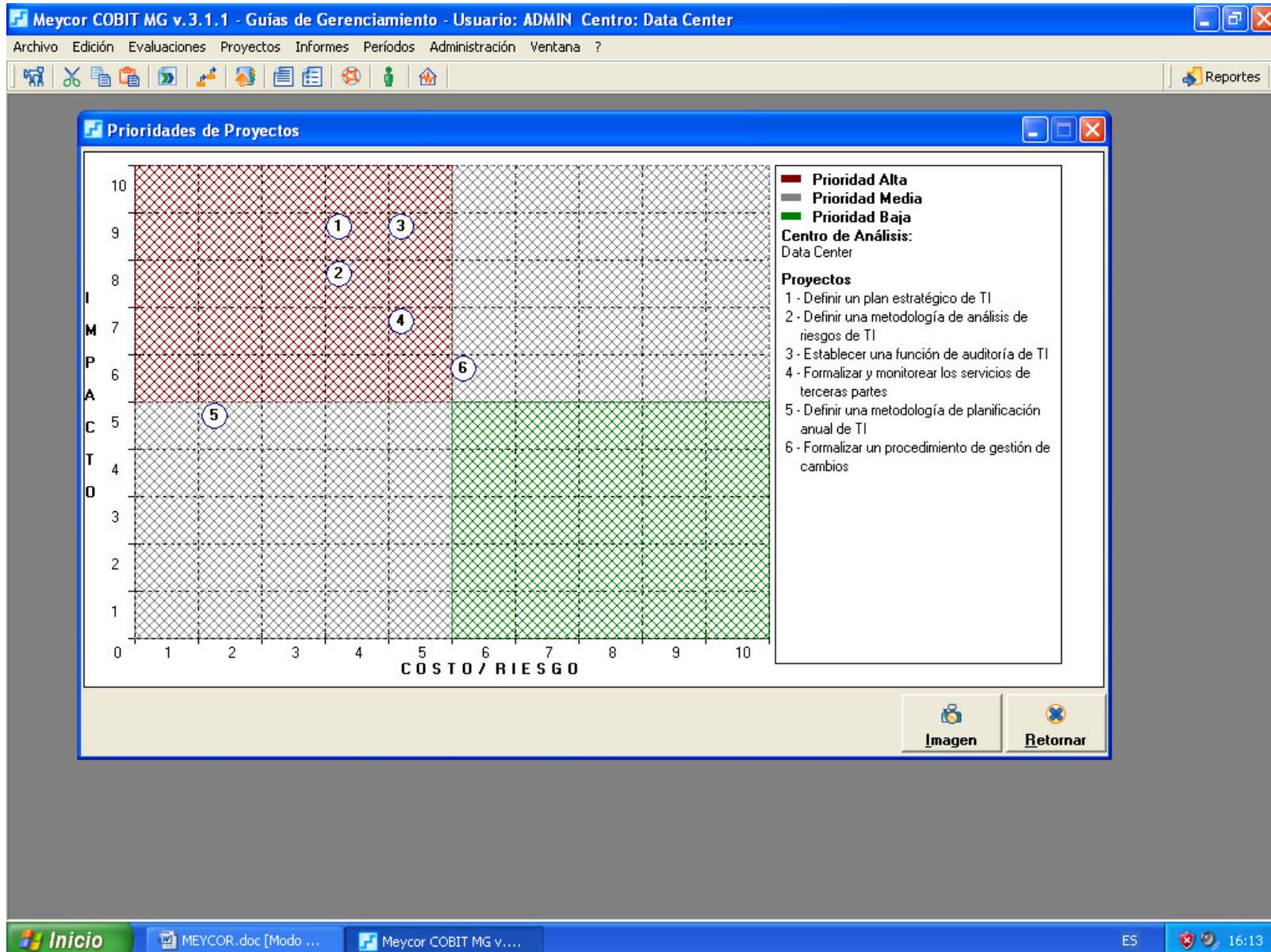
Impacto: 9 Costo/Riesgo: 4 Prioridad: Alta Importe: 0

Descripción | Recursos | Responsables | Comentarios |

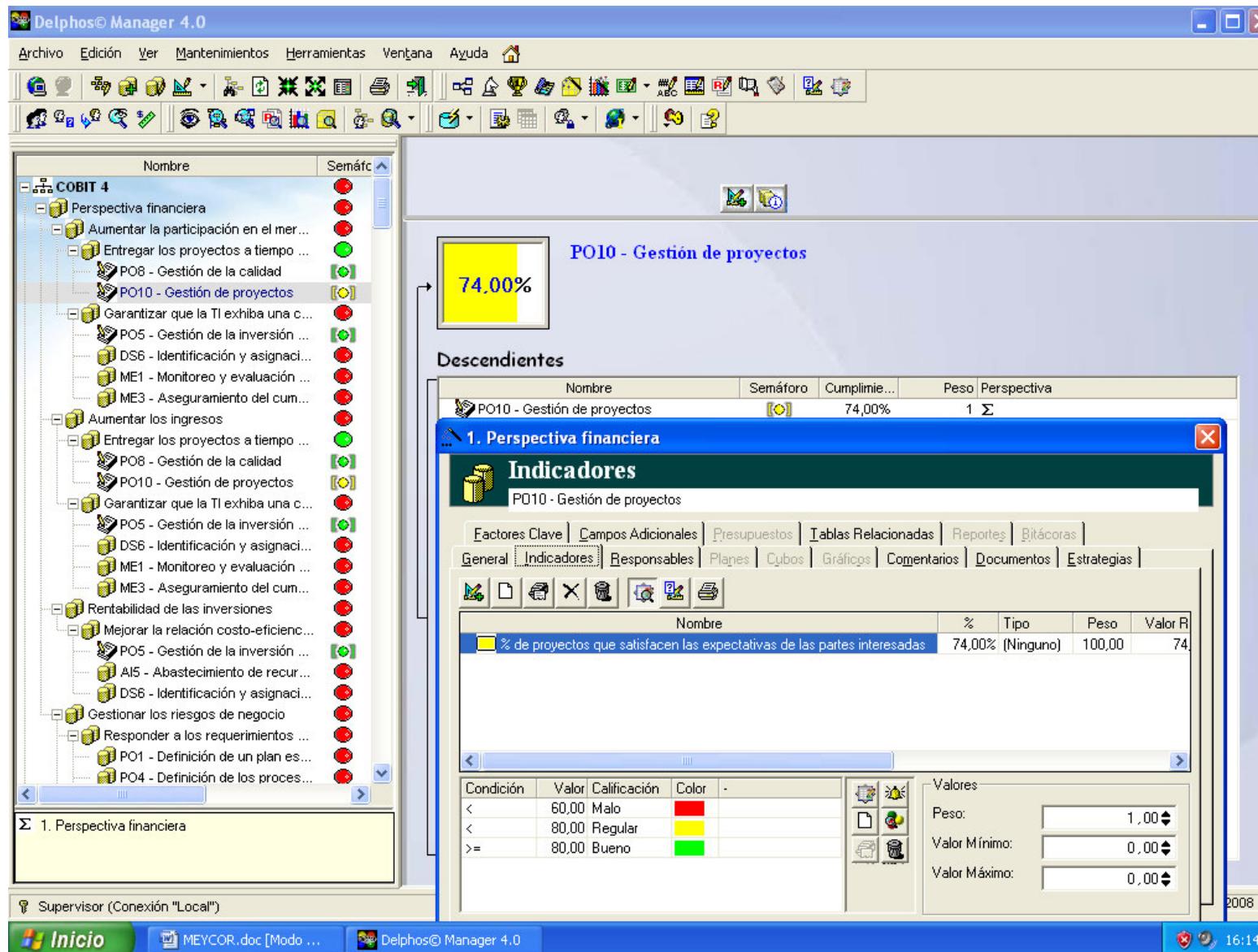
Agregar Actualizar Borrar Cancelar Graficar Retornar

Inicio MEYCOR.doc [Modo ...] Meycor COBIT MG v.... ES 16:12

Prioridades y selección de proyectos (Quick Win)



Balance Scorecard TI (Indicadores y Métricas)



FASES DE DESARROLLO

FASE 1. DEFINICIÓN Y PLANIFICACIÓN DEL PROYECTO.

FASE 2. CONOCIMIENTO DEL ENTORNO:

- Análisis de los objetivos del negocio.
- Análisis del control interno.
- Análisis de la estructura organizativa y de los procesos de negocio.
- Análisis de cumplimiento legal.
- Implantación de las Herramientas de Buen Gobierno
- Análisis de riesgos.
- Análisis de impacto en el negocio (BIA).
- Análisis de políticas y procedimientos.

FASE 3: DEFINICIÓN:

- Gestión del riesgo.
- Políticas y procedimientos.
- Gestión de continuidad del negocio.
- Plan de proyectos.
- Plan de formación.
- Plan de comunicación a los Órganos rectores de la compañía.



FASES DE DESARROLLO

FASE 4. IMPLANTACIÓN:

- Implantación del plan de tratamiento del riesgo y de las medidas elegidas.
- Formación y concienciación al personal.
- Cuadro de mando (BSC)
- Implantación de métricas y registros.
- Implantación de oficina de control interno.

FASE 5: REVISIÓN

- Auditoría del sistema.
- Apoyo a la certificación.





METODOLOGÍA EMPLEADA

proponemos una metodología para abarcar cada uno de los requisitos del proyecto

- **COSO Committee of Sponsoring Organizations.**
- **UNE – ISO/IEC 27001:2005:** certificación de los SGSI
- **ISO/IEC 27002 :** código de buenas prácticas de seguridad.
- **UNE –ISO/IEC 20000** Tecnología de la información. Gestión del servicio.
- **ITIL V3**
- **ISO38500 - COBIT / Val IT** publicado por IT GOVERNANCE INSTITUTE: Objetivos de control de información y tecnologías relacionadas.
- **ISO24762 - BUSSINES CONTINUITY MANAGEMENT GOOD PRACTICE GUIDELINES** (2006) publicado por THE BUSINESS CONTINUITY INSTITUTE: guía de buenas prácticas de planes de continuidad del negocio.
- **COSO-ERM , MAGERIT, NIST, UNE 71504** : metodologías de análisis de riesgos.