

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.

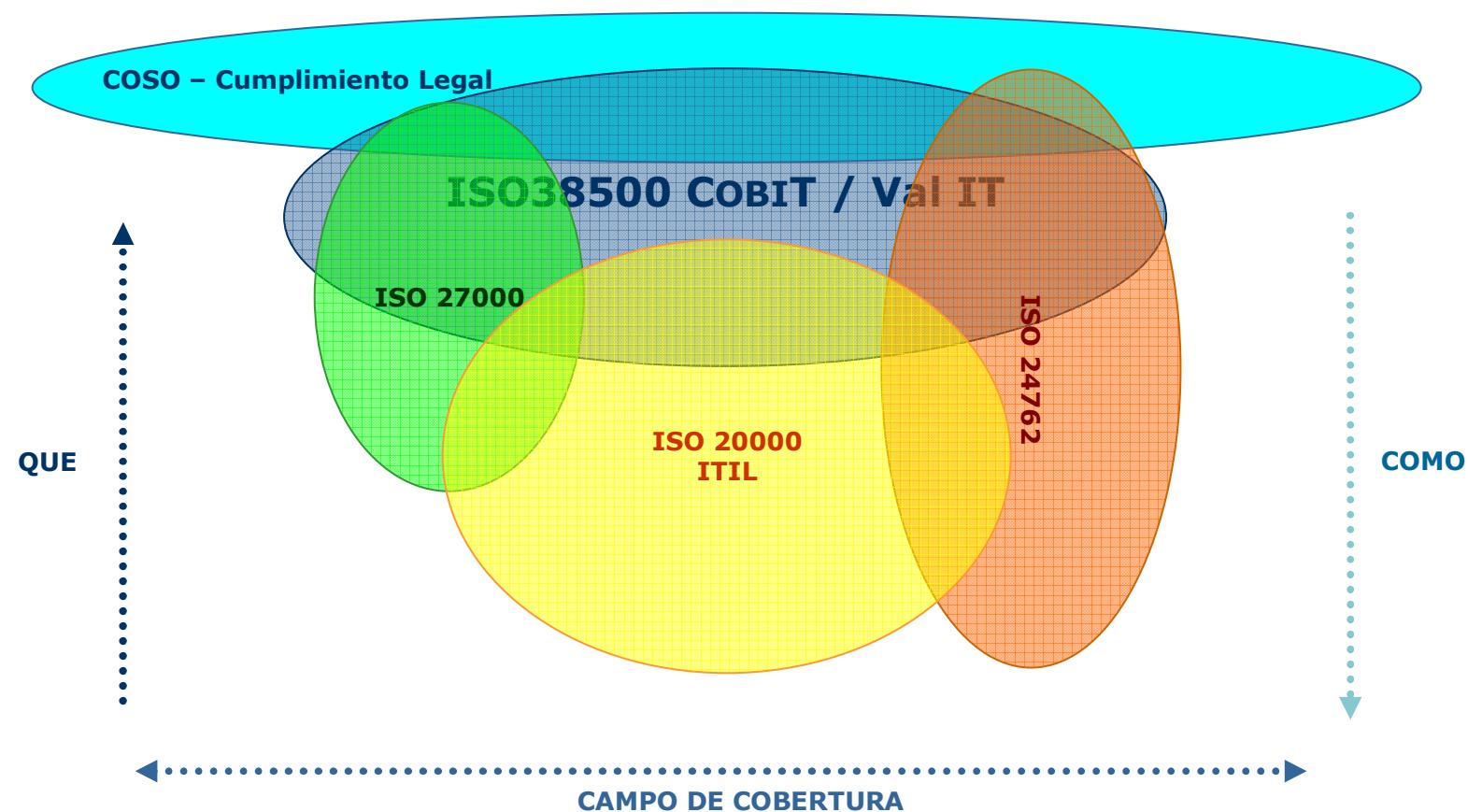
Gobernanza de la Seguridad de la Información y Tecnologías afines

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

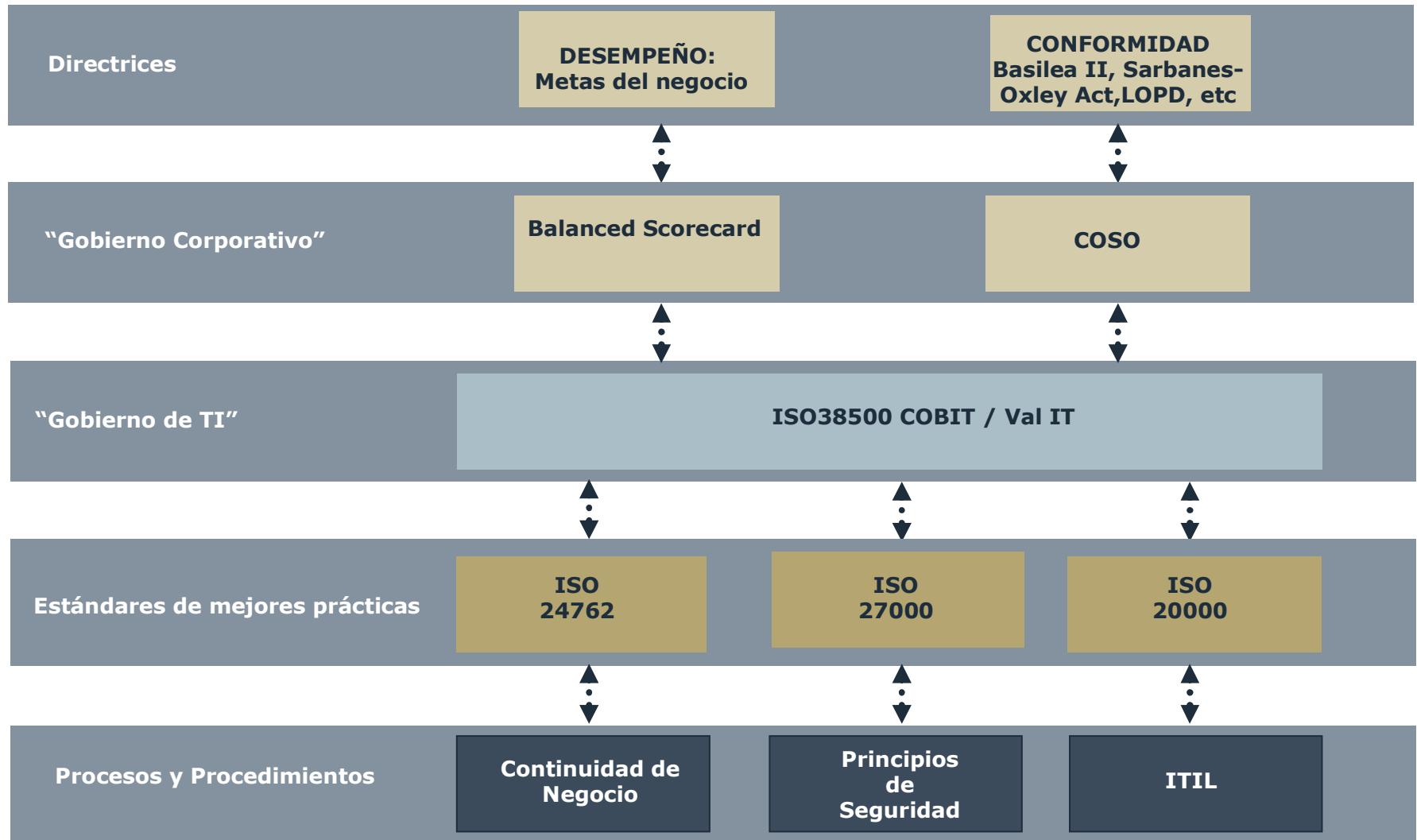
ISACA/CISM BoK (2002)

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



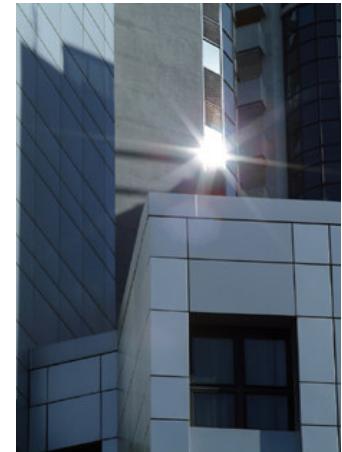
En 1992, COSO publicó el Sistema Integrado de Control Interno, un informe que establece una **definición común de control interno** y proporciona un **estándar** mediante el cual las organizaciones pueden **evaluar y mejorar sus sistemas de control**.



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.

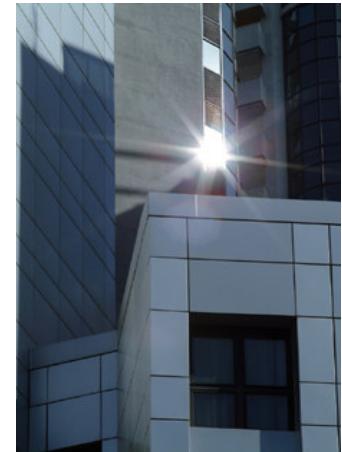


El Gobierno Corporativo incluye las siguientes capacidades:

- 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.

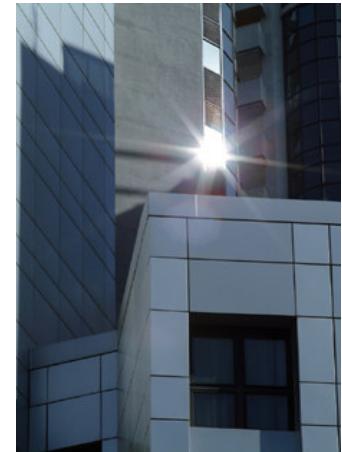


Definición de la Gobierno Corporativo

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:

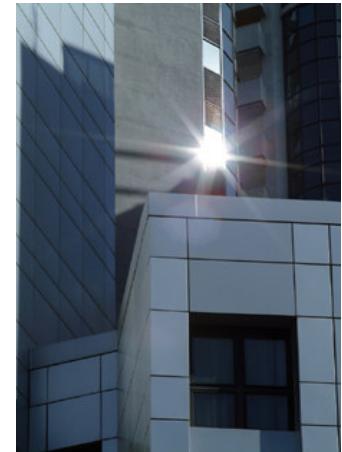
- **Estrategia:** objetivos a alto nivel, alineados con la misión de la entidad y dándole apoyo
- **Operaciones:** objetivos vinculados al uso eficaz y eficiente de los recursos
- **Información:** objetivos de fiabilidad de la información suministrada.
- **Cumplimiento:** objetivos relativos al cumplimiento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

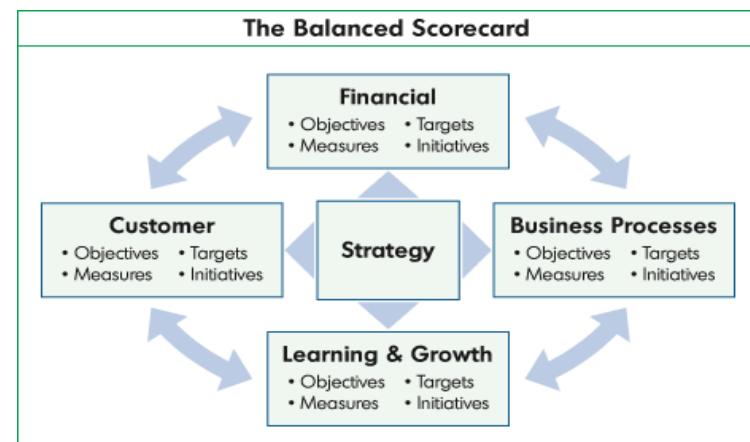
Supervisión

- 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

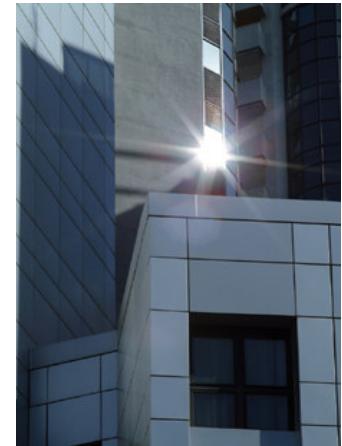
- ISO/IEC 29881:2008 Information technology -- Software and systems engineering -- FISMA 1.1 functional size measurement method
- ISO/IEC 15288:2008 Systems and software engineering -- System life cycle processes
- ISO/IEC 12207:2008 Systems and software engineering -- Software life cycle processes

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.



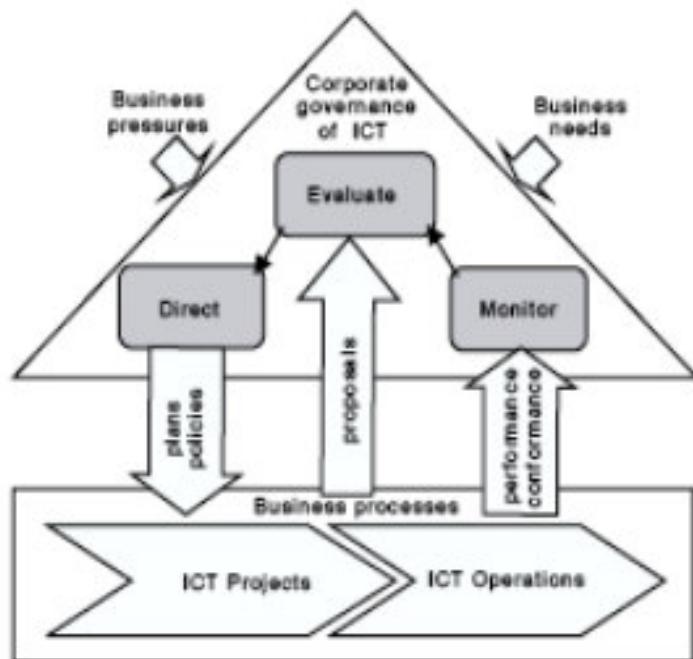
INTERNATIONAL
STANDARD

ISO/IEC
38500

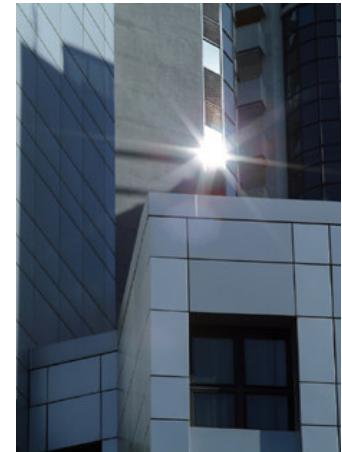
First edition
2009-09-21

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

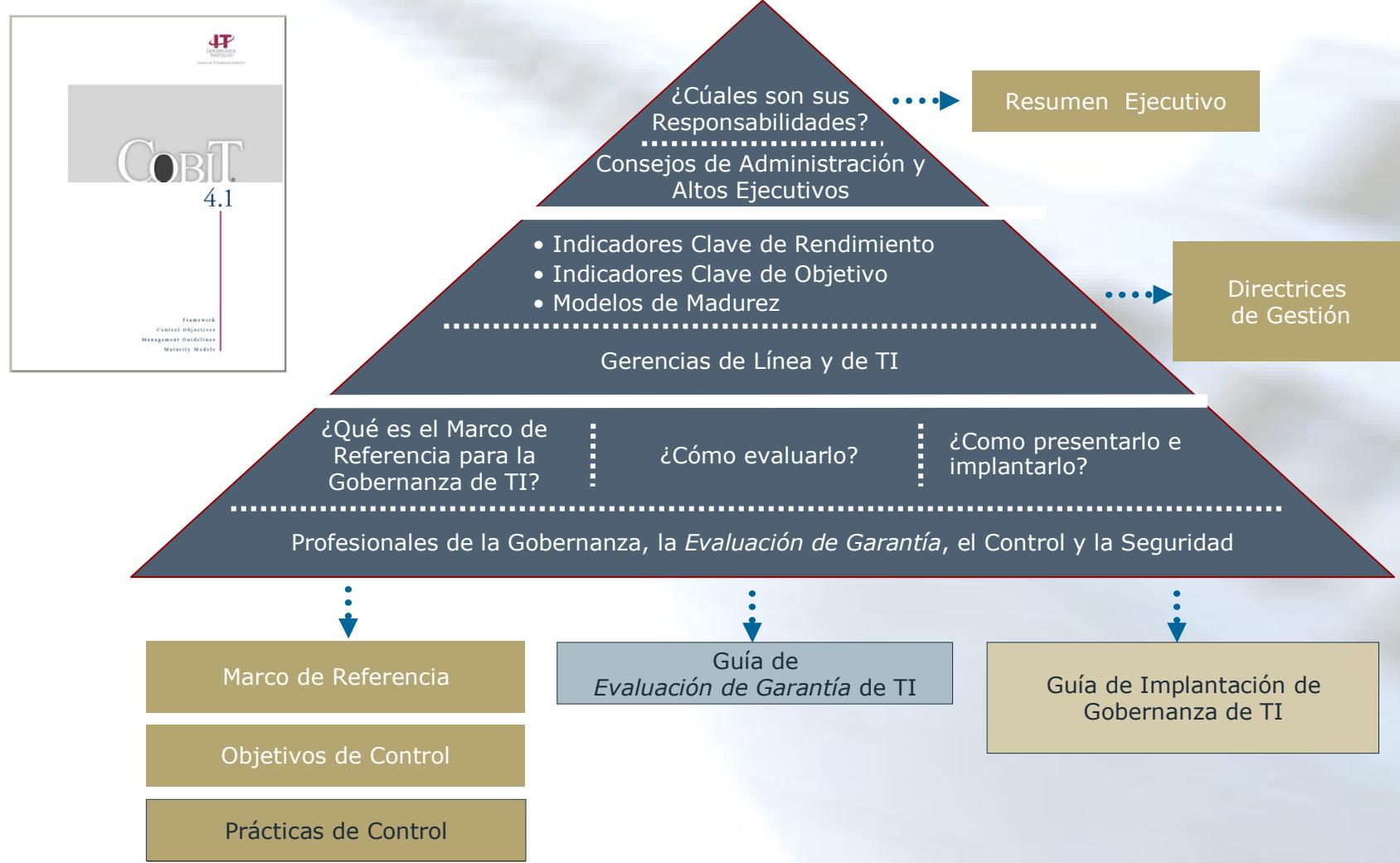
© 2008 ISO Privacy Policy Name and logo Sitemap Contact ISO Guided tour of ISO-Online Print Increase text size

- 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

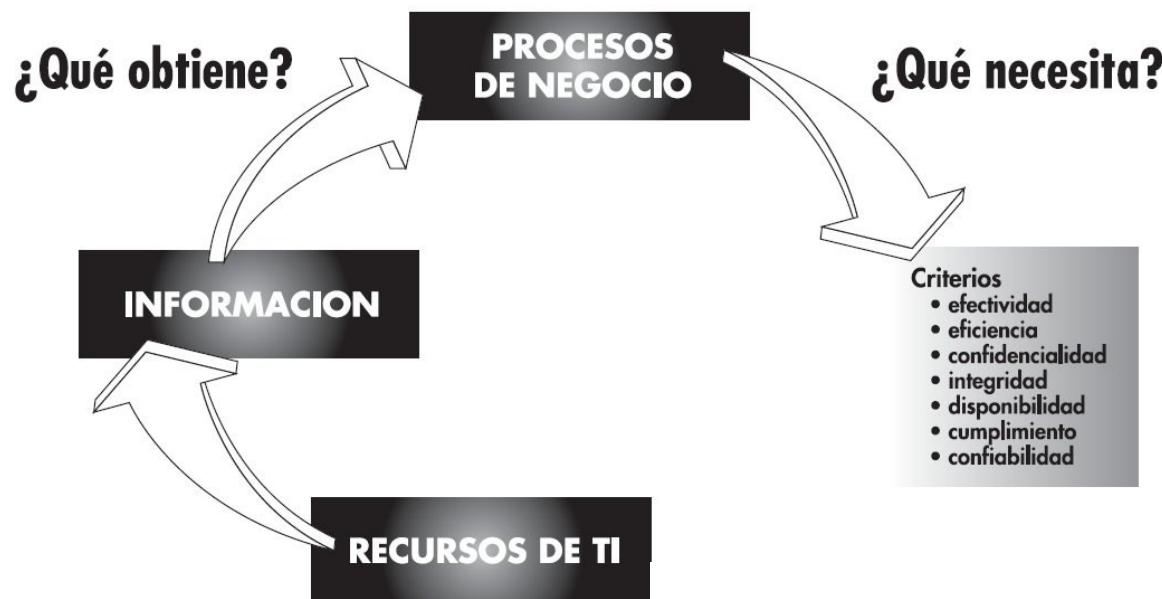
- ◊ ¿Los individuos de su organización entienden y aceptan su responsabilidad sobre las TIC?
- ◊ ¿Sus planes tecnológicos soportan los planes corporativos de su organización y cubren las necesidades presentes y futuras de la misma?
- ◊ ¿Las adquisiciones de TIC se realizan por razones aprobadas y de 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



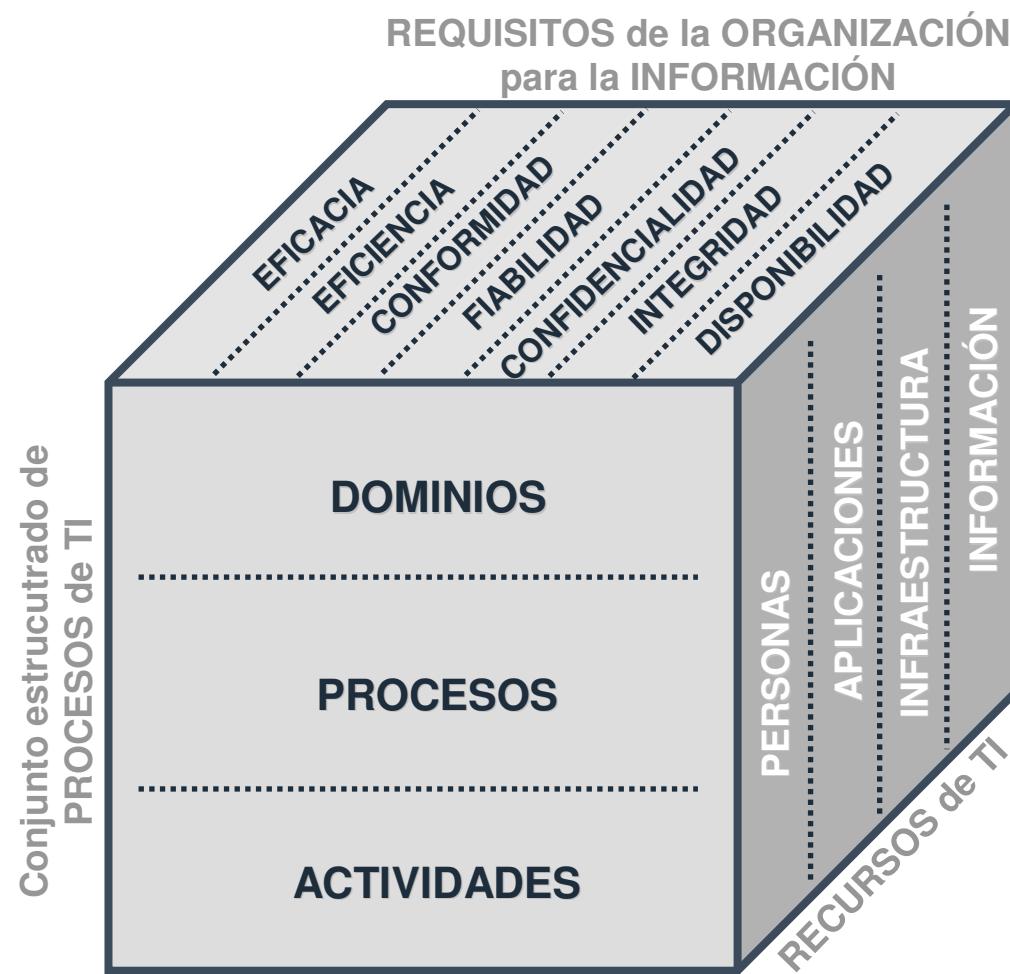
MARCO DE REFERENCIA

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



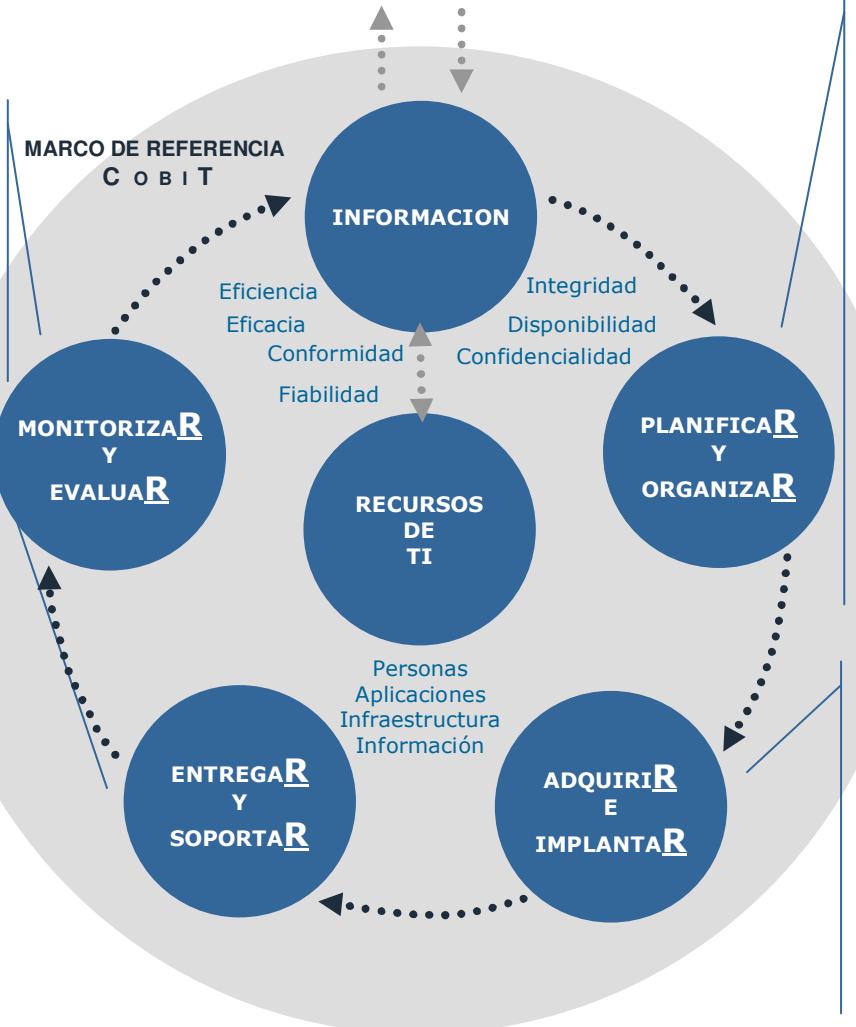


OBJETIVOS DE CONTROL

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.

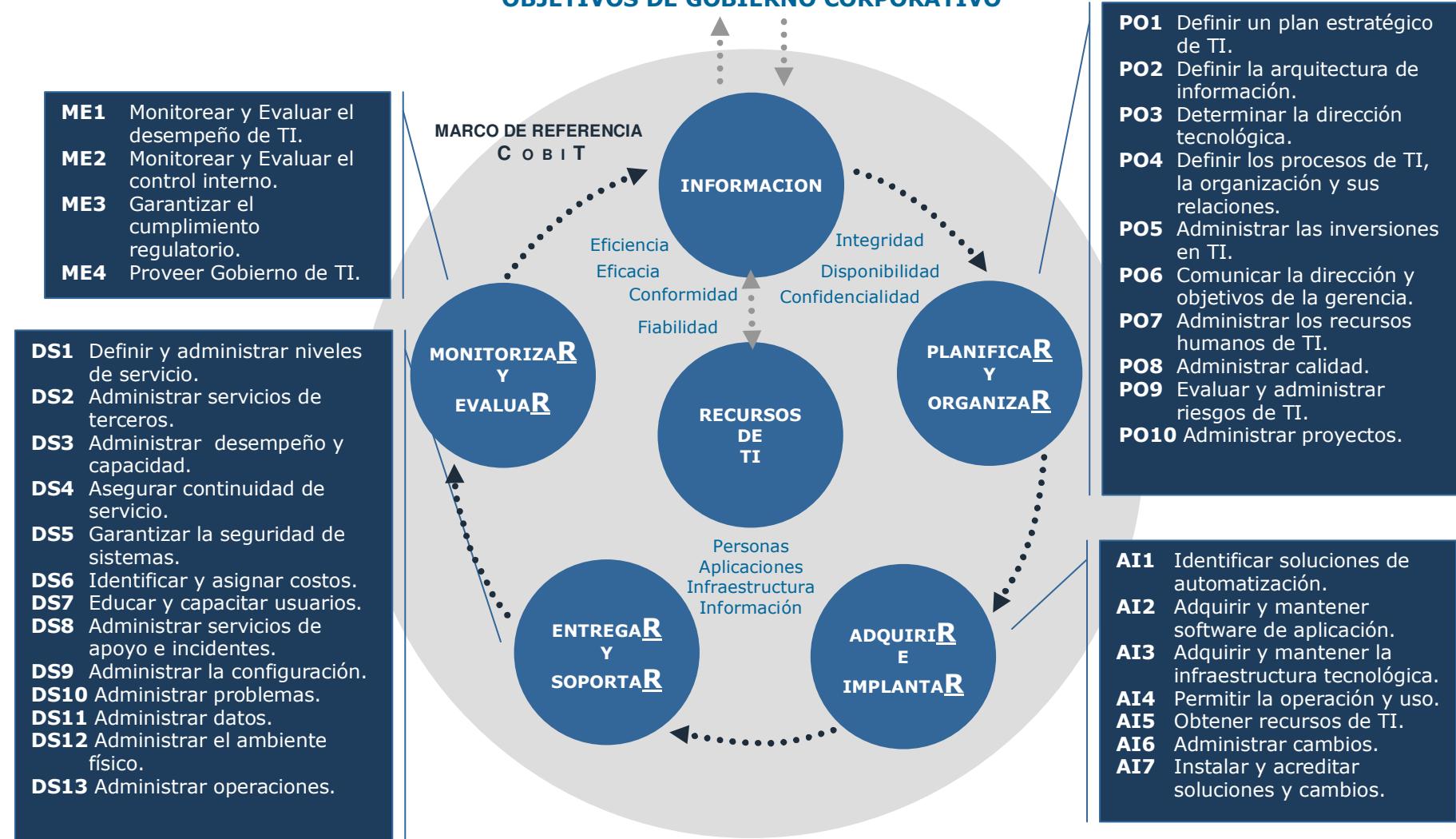
La consecución de la visión estratégica debe planearse, comunicarse y gestionarse desde diferentes perspectivas.

Es necesario establecer una organización e infraestructura tecnológica apropiada.

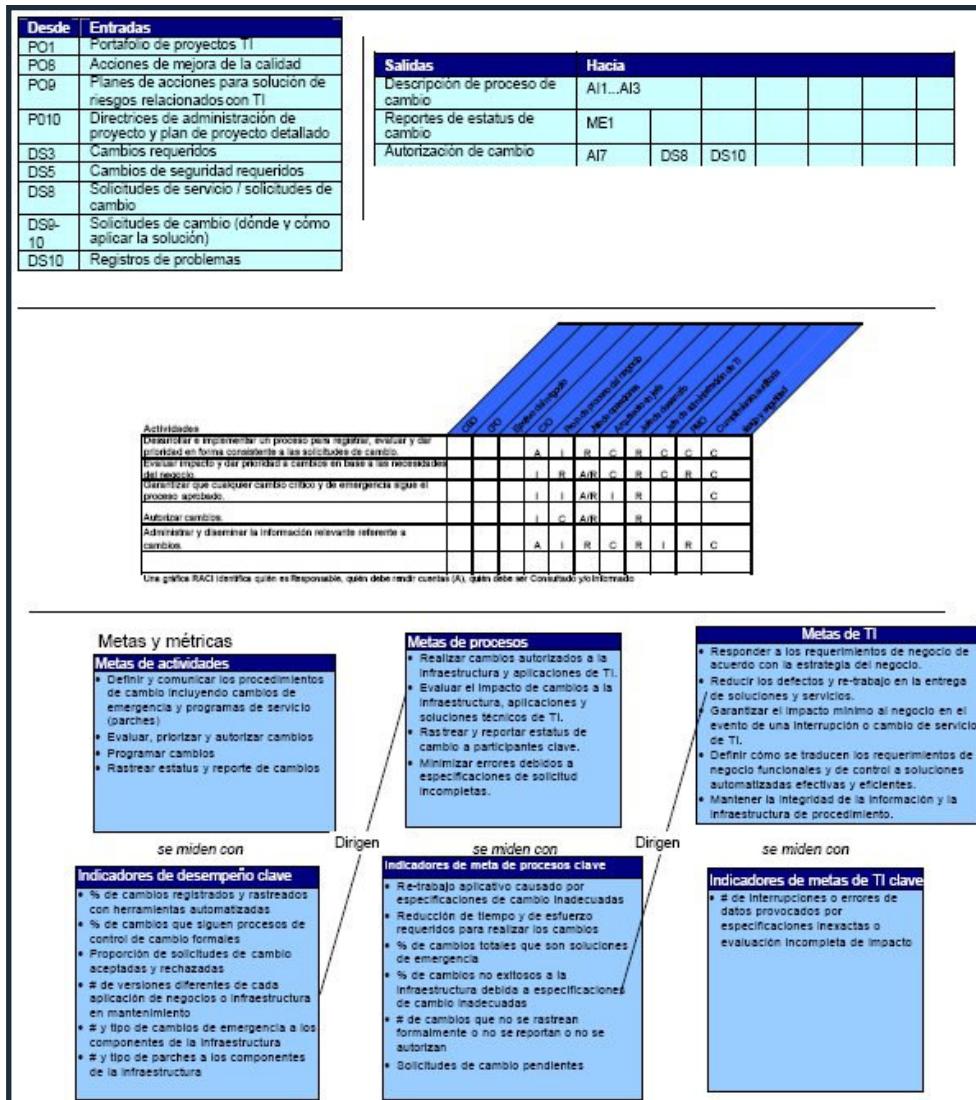
Para llevar a cabo la estrategia de TI, éstas deben identificarse, construirse o adquirirse, implantándose e integrándose en el proceso de la Organización.

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

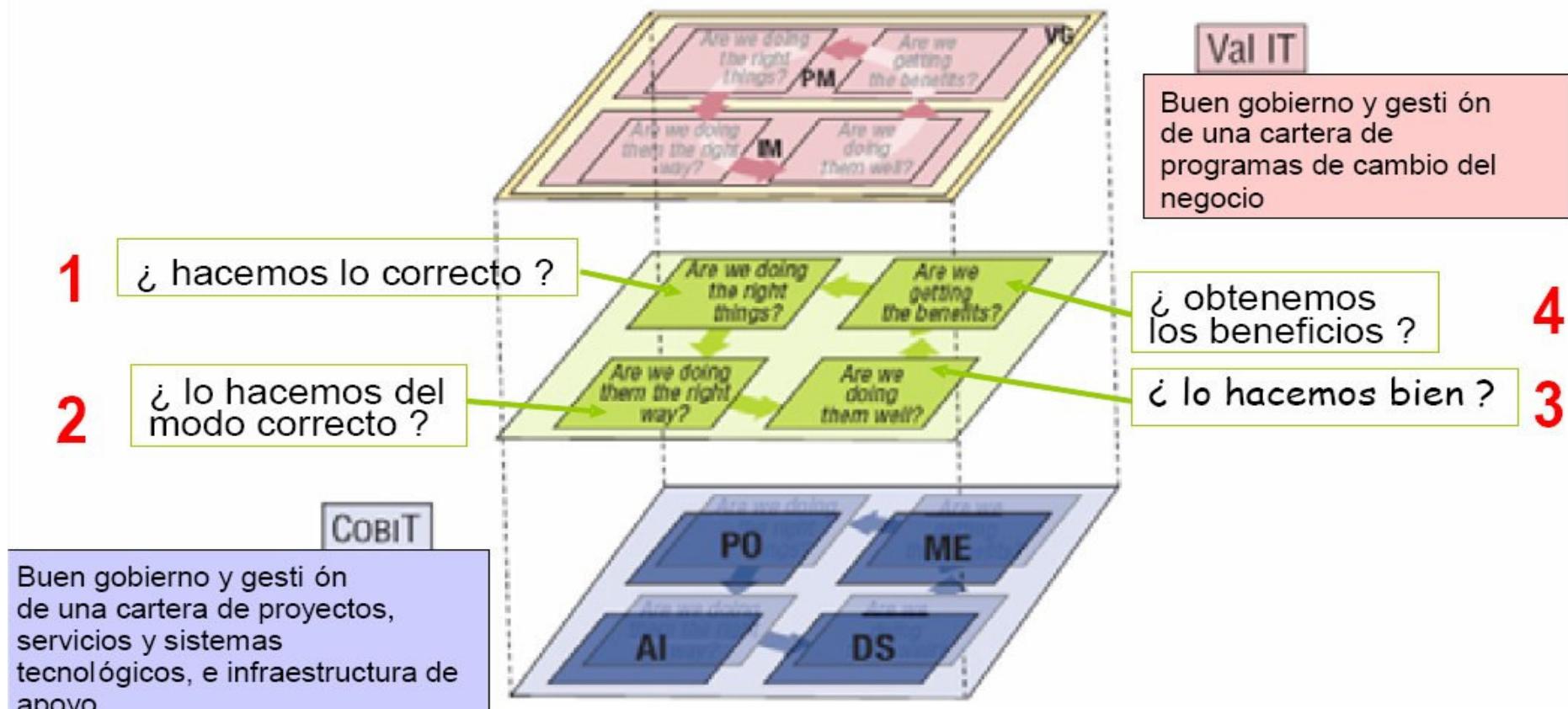
The Val IT Framework







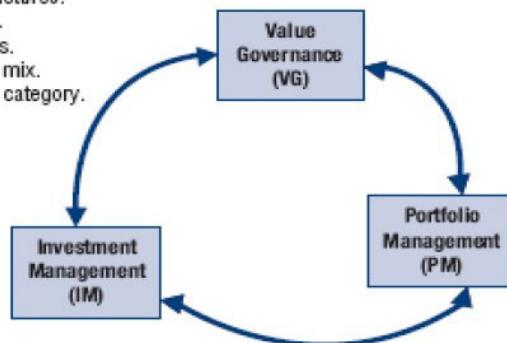
Val IT™ y CobiT®, complementarios; **dos planes distintos**



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.



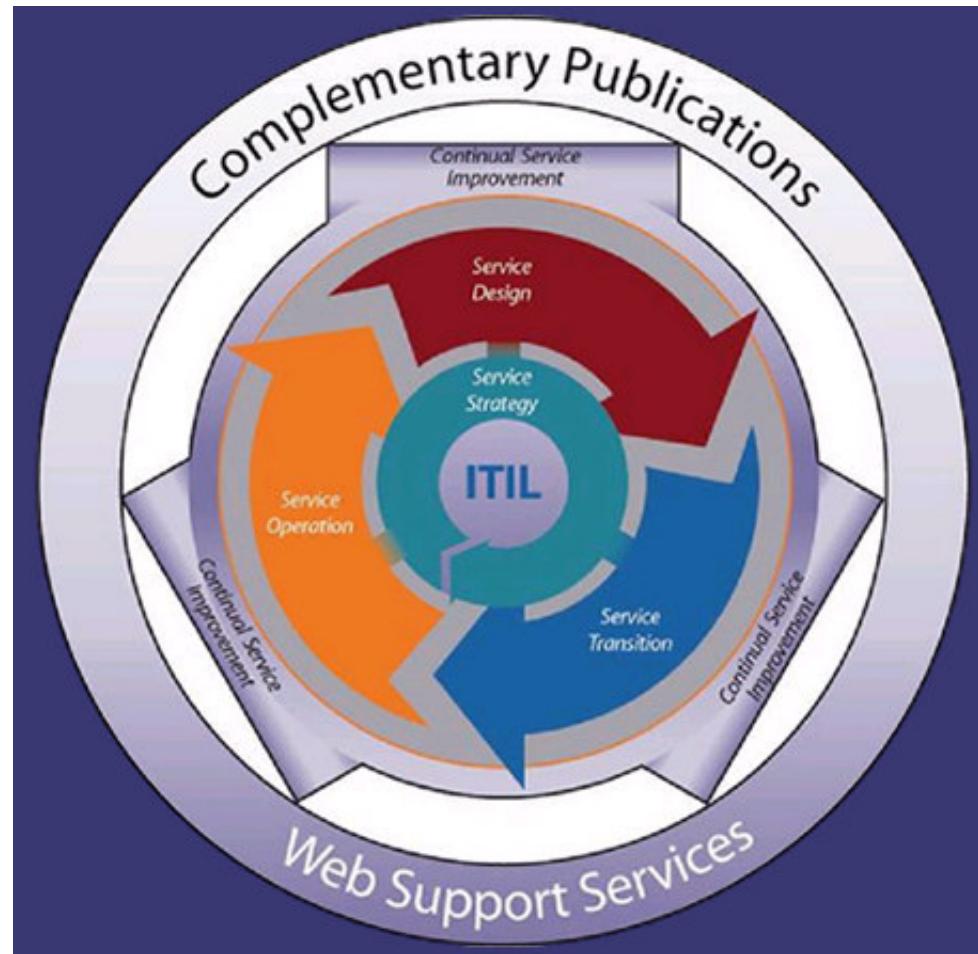
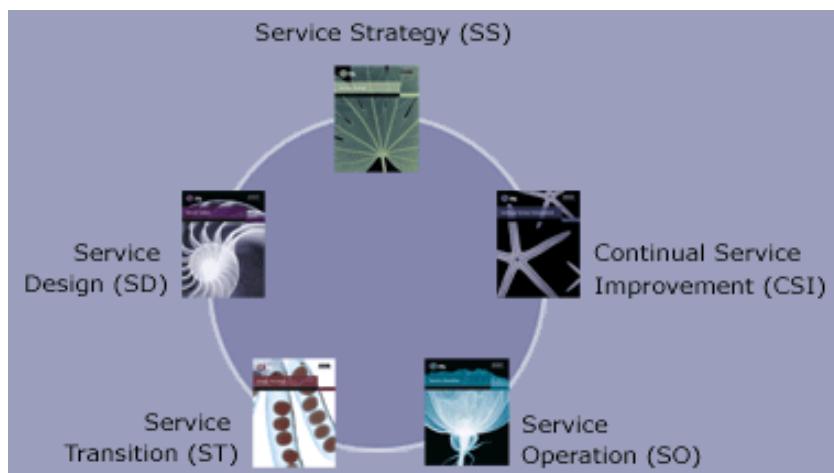
- IM1 Develop a high-level definition of investment opportunity.
- IM2 Develop an initial programme concept business case.
- IM3 Develop a clear understanding of candidate programmes.
- IM4 Perform alternatives analysis.
- IM5 Develop a programme plan.
- IM6 Develop a benefits realisation plan.
- IM7 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>

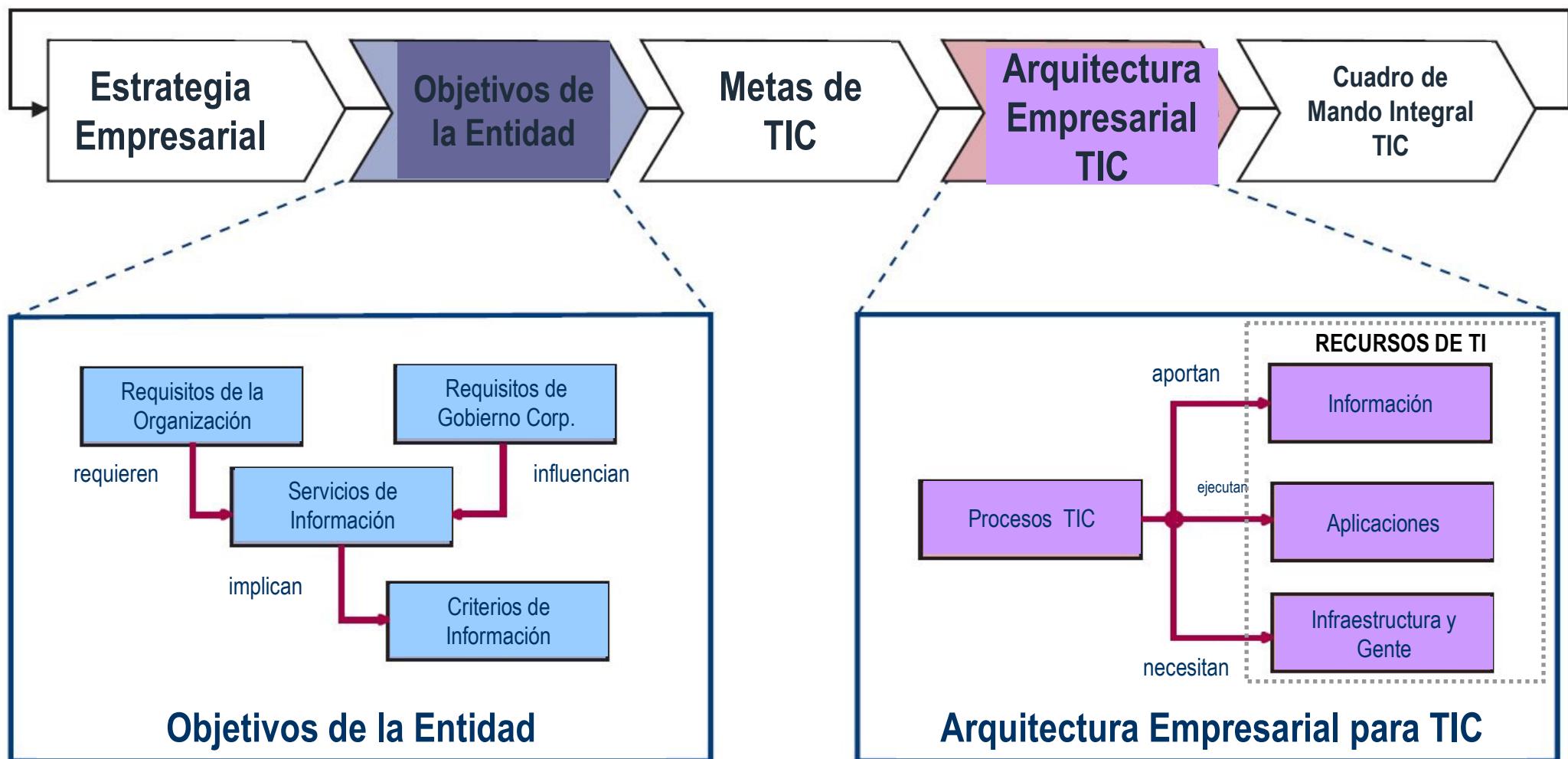
11 Áreas de Control

- 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

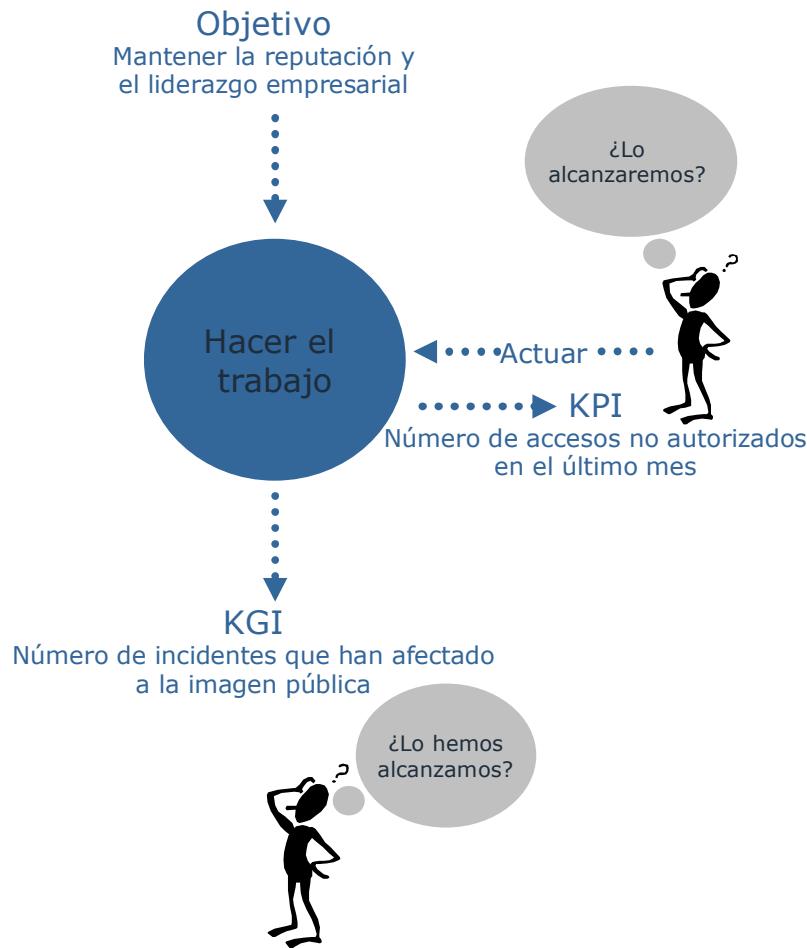
Continuidad de Negocio



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



Objetivos e indicadores

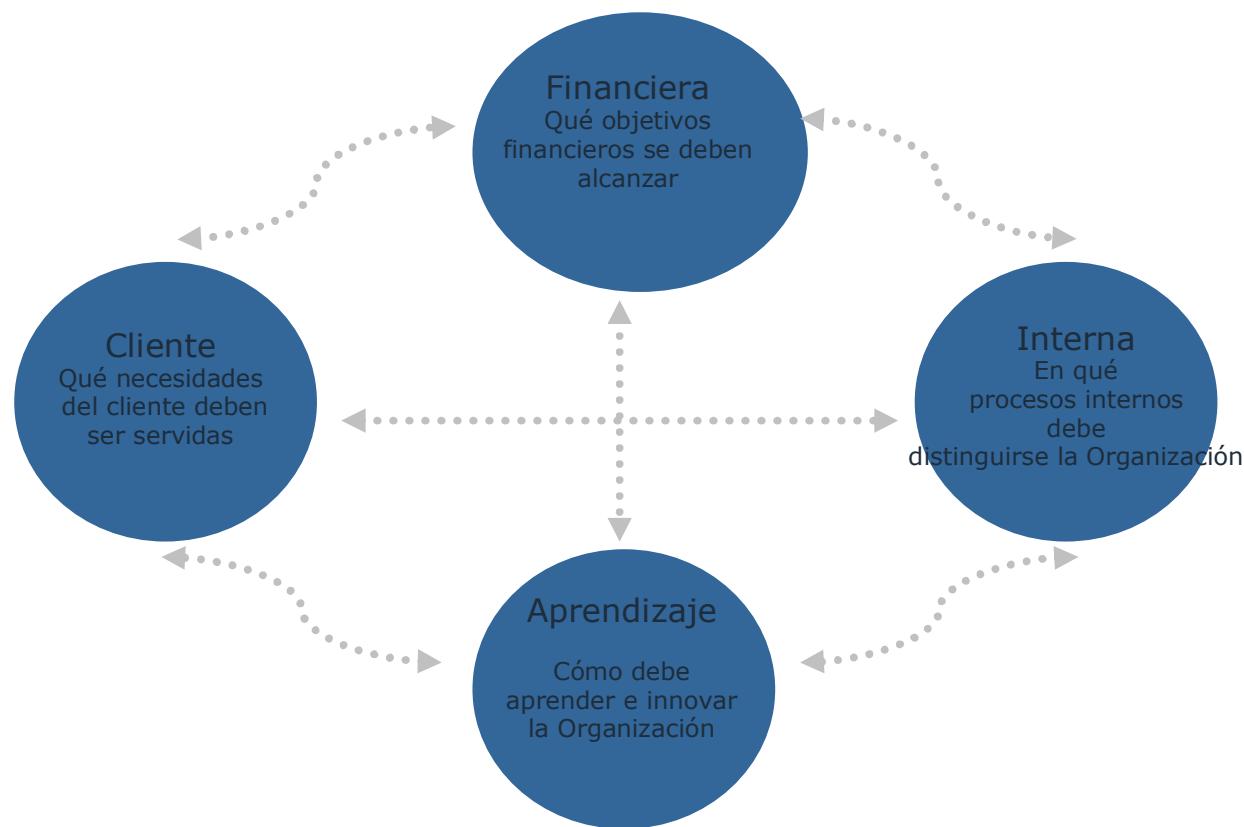


- **KPI (Key Performance Indicator / Indicador Clave de Rendimiento):**

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):**

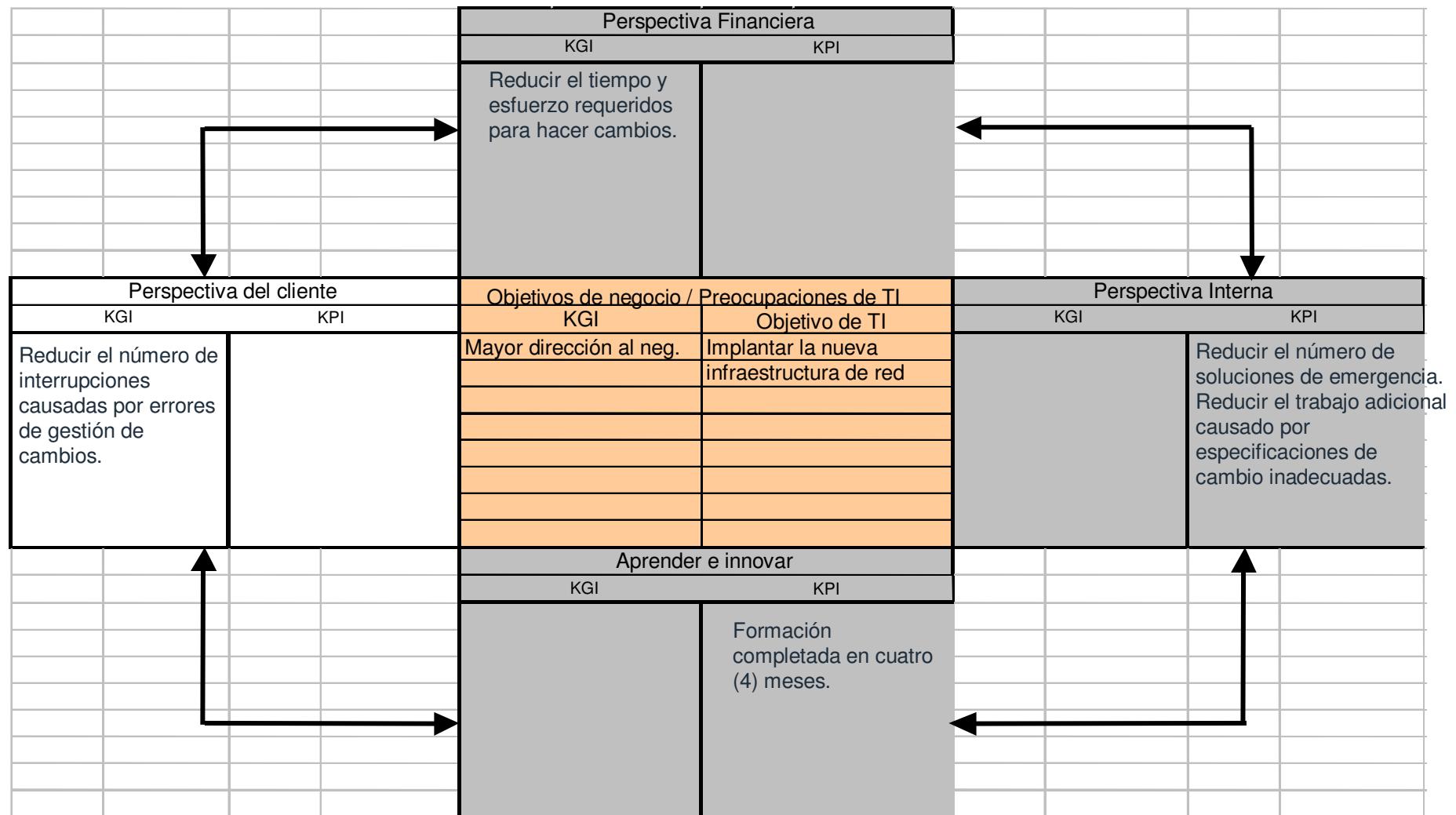
Indican, después del hecho, si un determinado objetivo se ha alcanzado.

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

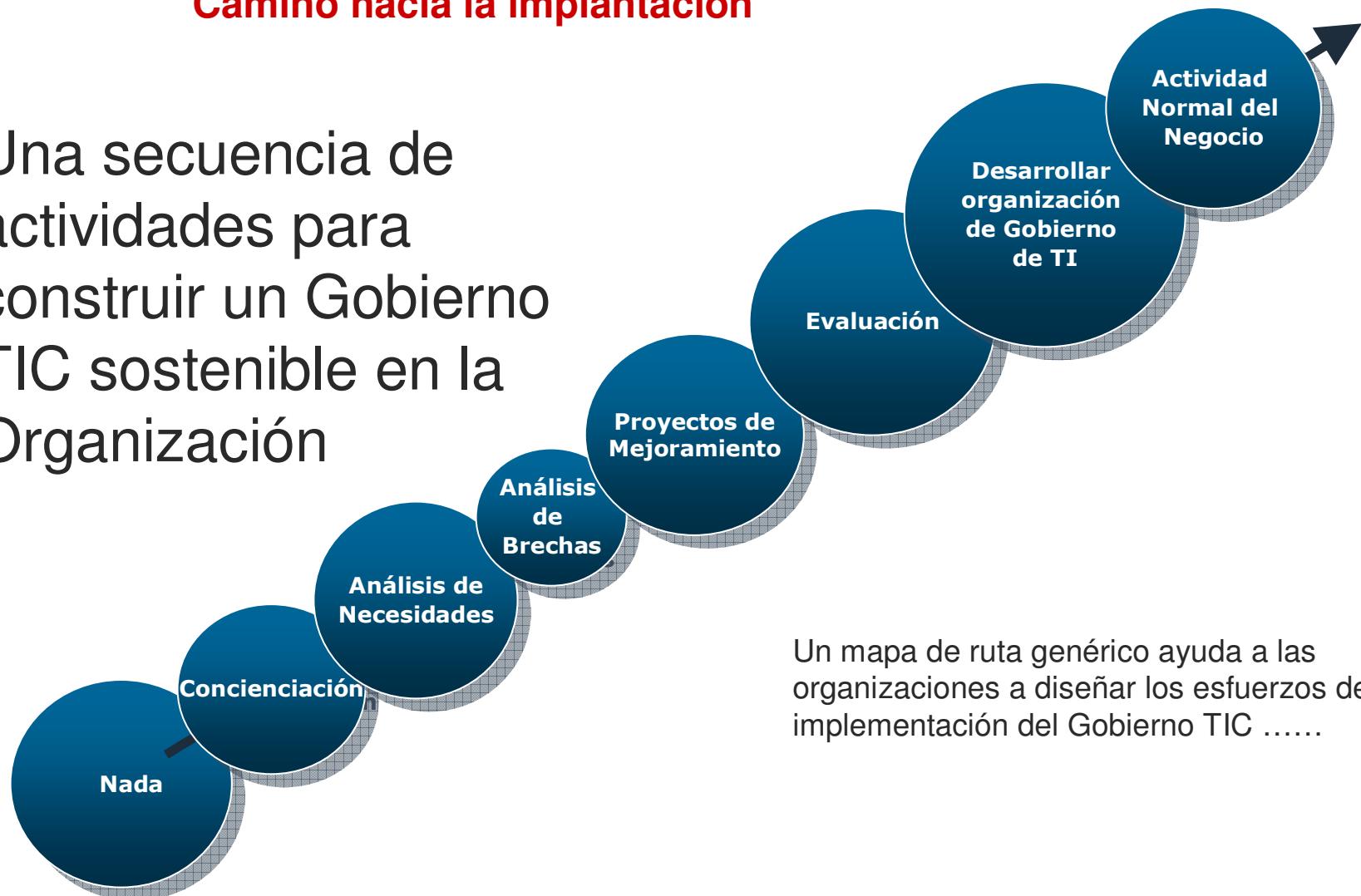
- Code of Professional Ethics
- IS Auditing Standards, Guidelines and Procedures
- IS Control Professionals Standards



Current as of 1 May 2003

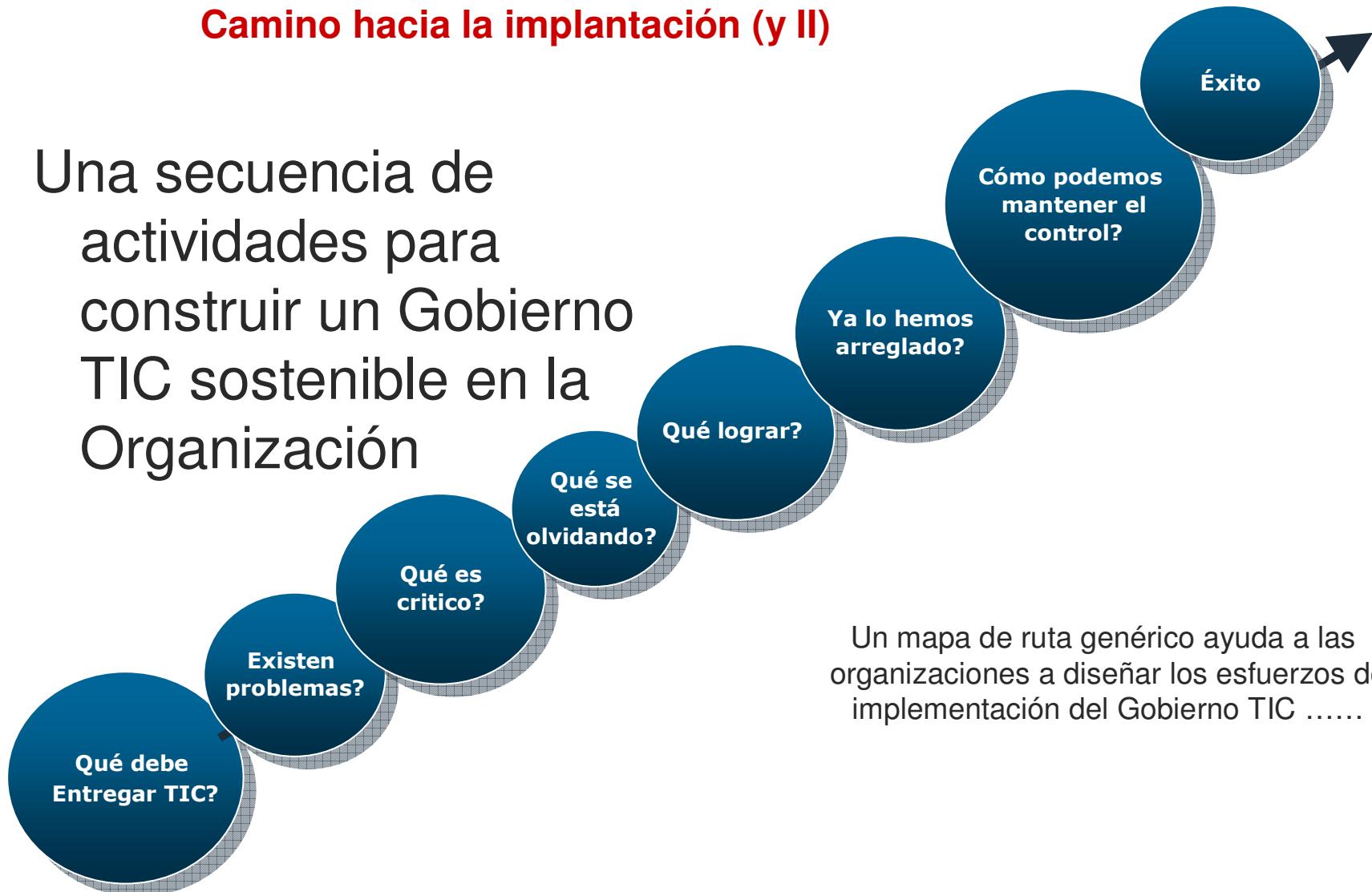
Camino hacia la implantación

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



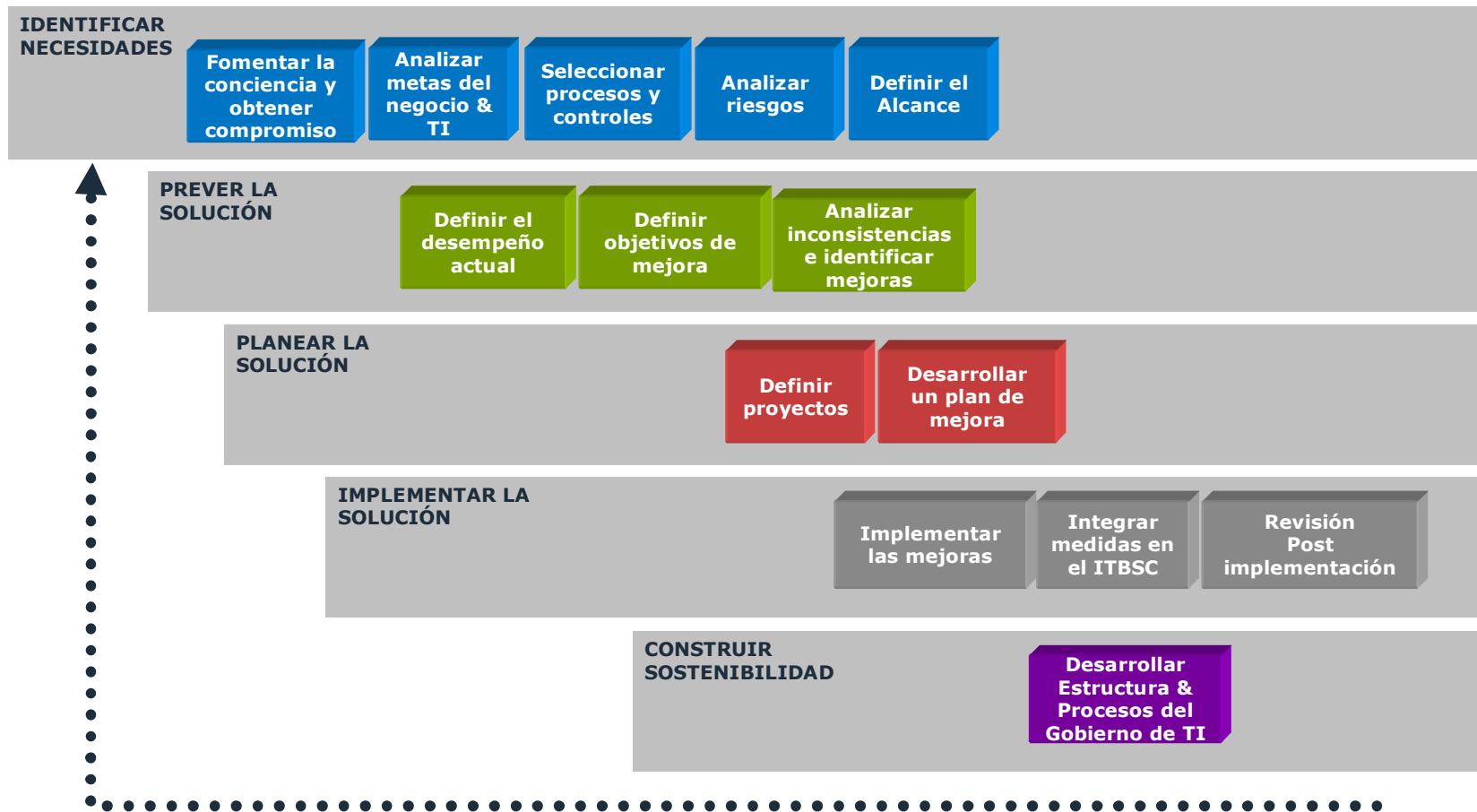
Camino hacia la implantación (y II)

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

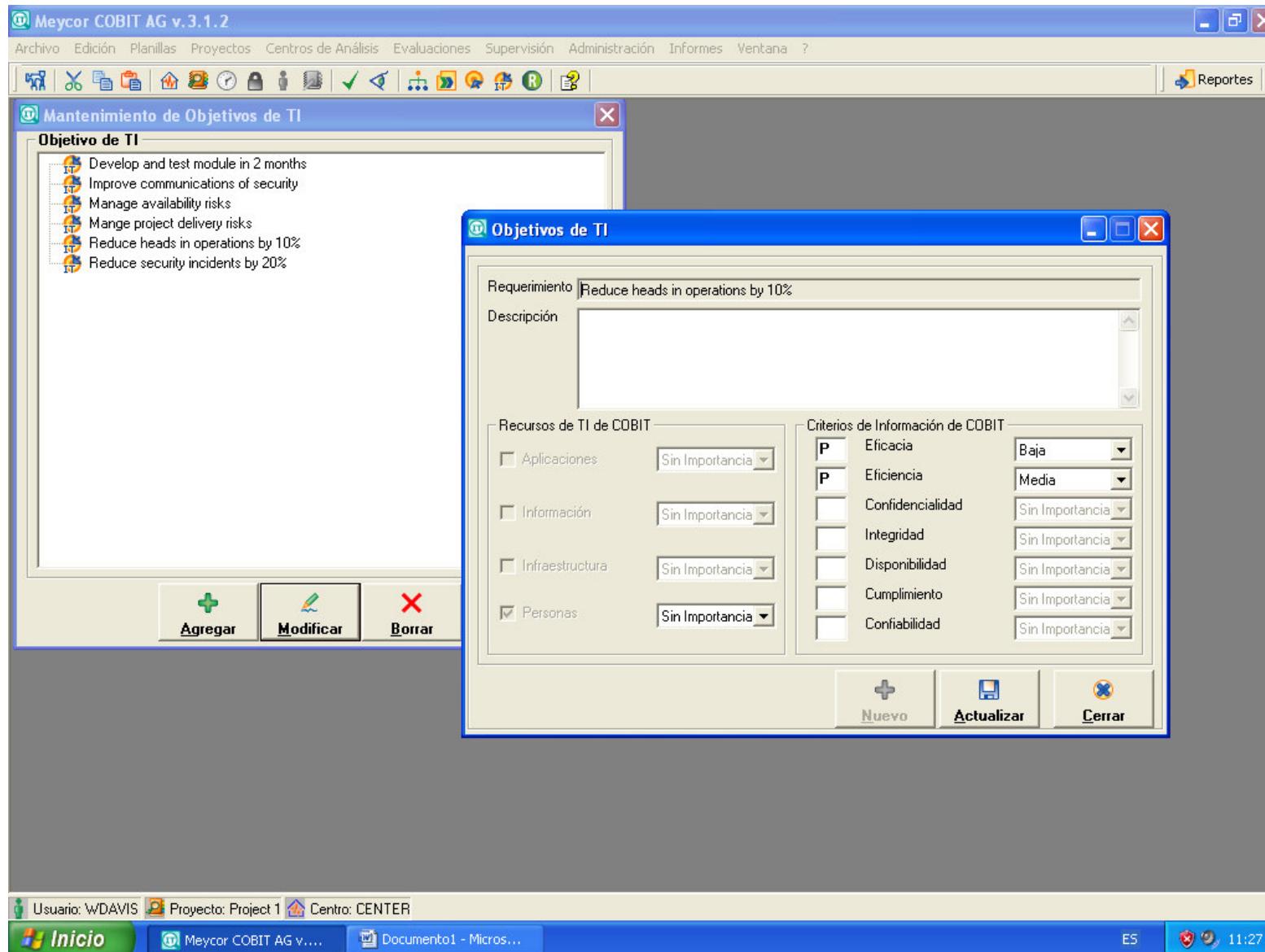
Agregar Modificar Borrar Actualizar Desasignar Cerrar

Usuario: WDAVIS Proyecto: Project 1 Centro: CENTER

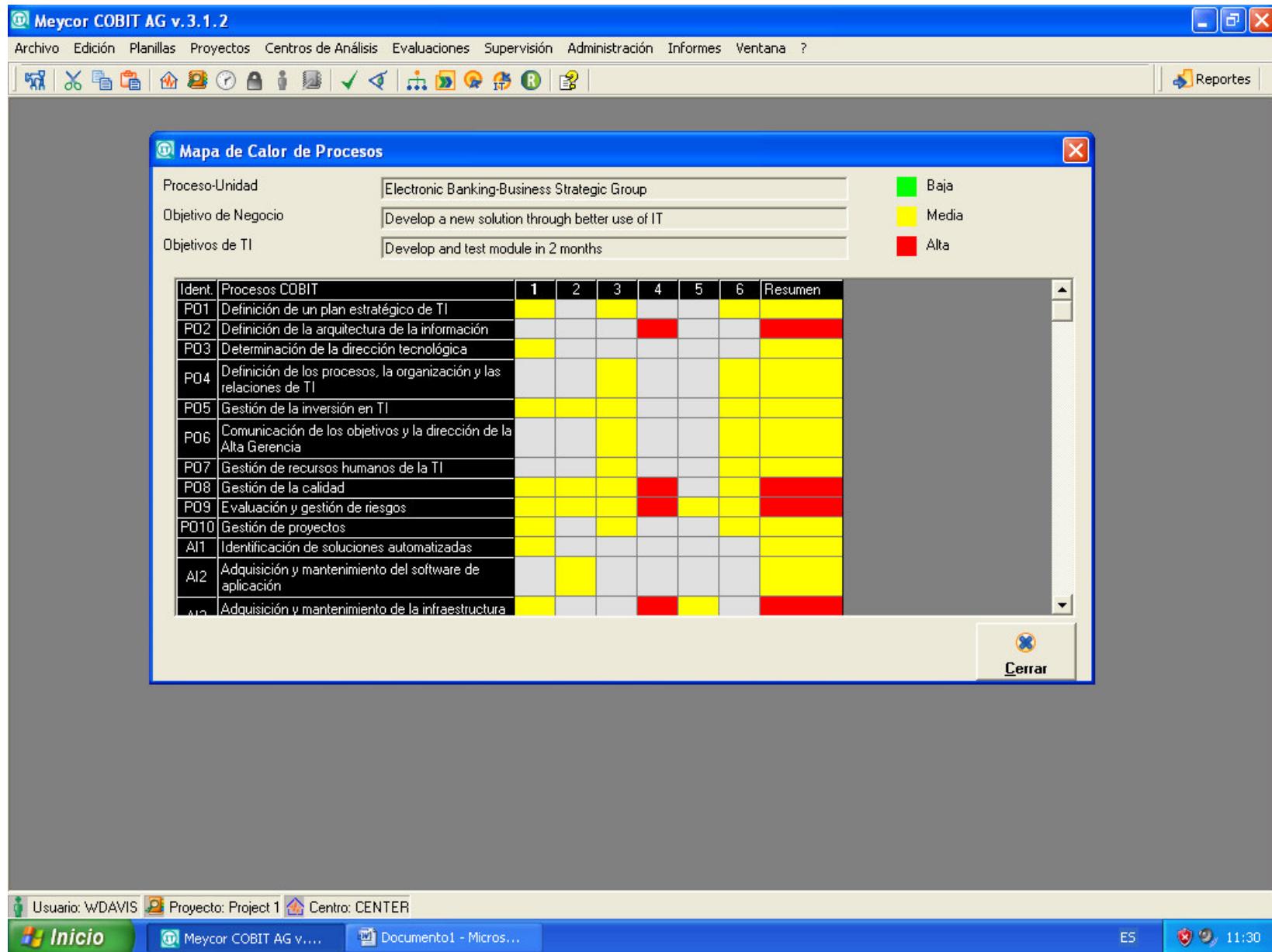
Inicio Meycor COBIT AG v.... Documento1 - Micros... ES 11:26

The screenshot displays the 'Mantenimiento de Recursos de TI' (IT Resource Management) module of the Meycor COBIT AG v.3.1.2 application. The interface is divided into two main panes: 'Recursos de TI' (left) and 'Objetivo de TI' (right). The 'Recursos de TI' pane lists various IT assets and personnel, including 'Aplicaciones' (CRM, WebOp), 'Infraestructura' (Servidores, Software de Base, Telecomunicaciones), and 'Personas' (IT Development Team, IT Manager). The 'Objetivo de TI' pane lists several IT objectives with associated icons: 'Develop and test module in 2 months', 'Improve communications of security', 'Manage availability risks', 'Manage project delivery risks', 'Reduce heads in operations by 10%' (with a 'Personas' sub-item listing 'IT Development Team' and 'IT Manager'), and 'Reduce security incidents by 20%'. At the bottom, there are buttons for 'Agregar' (Add), 'Modificar' (Modify), 'Borrar' (Delete), 'Actualizar' (Update), 'Desasignar' (Unassign), and 'Cerrar' (Close). The system tray at the bottom shows the user 'WDAVIS', project 'Project 1', center 'CENTER', and the date/time '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	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	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

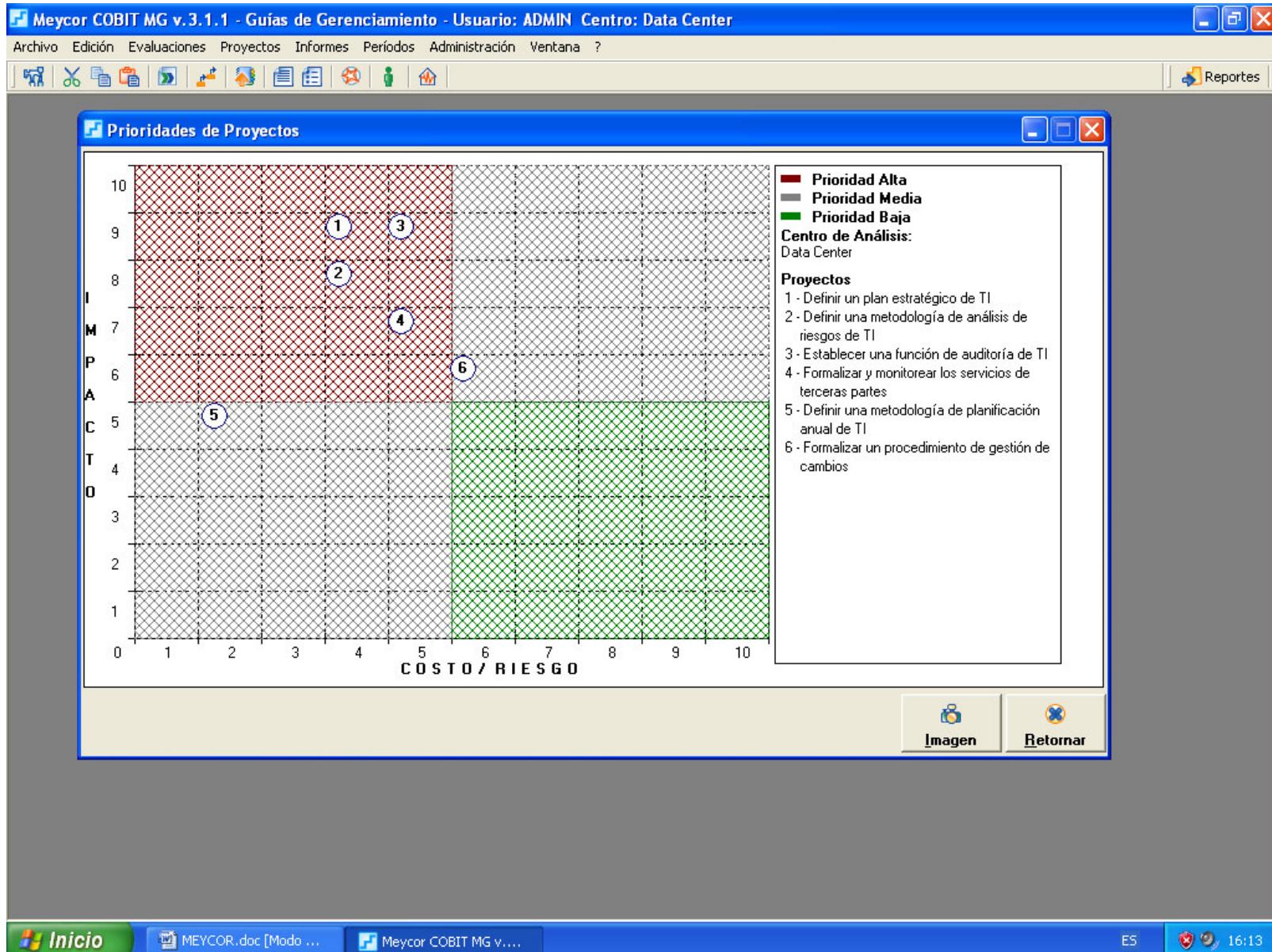
Descripción | Recursos | Responsables | Comentarios |

Agregar Actualizar Borrar Cancelar Graficar Retornar

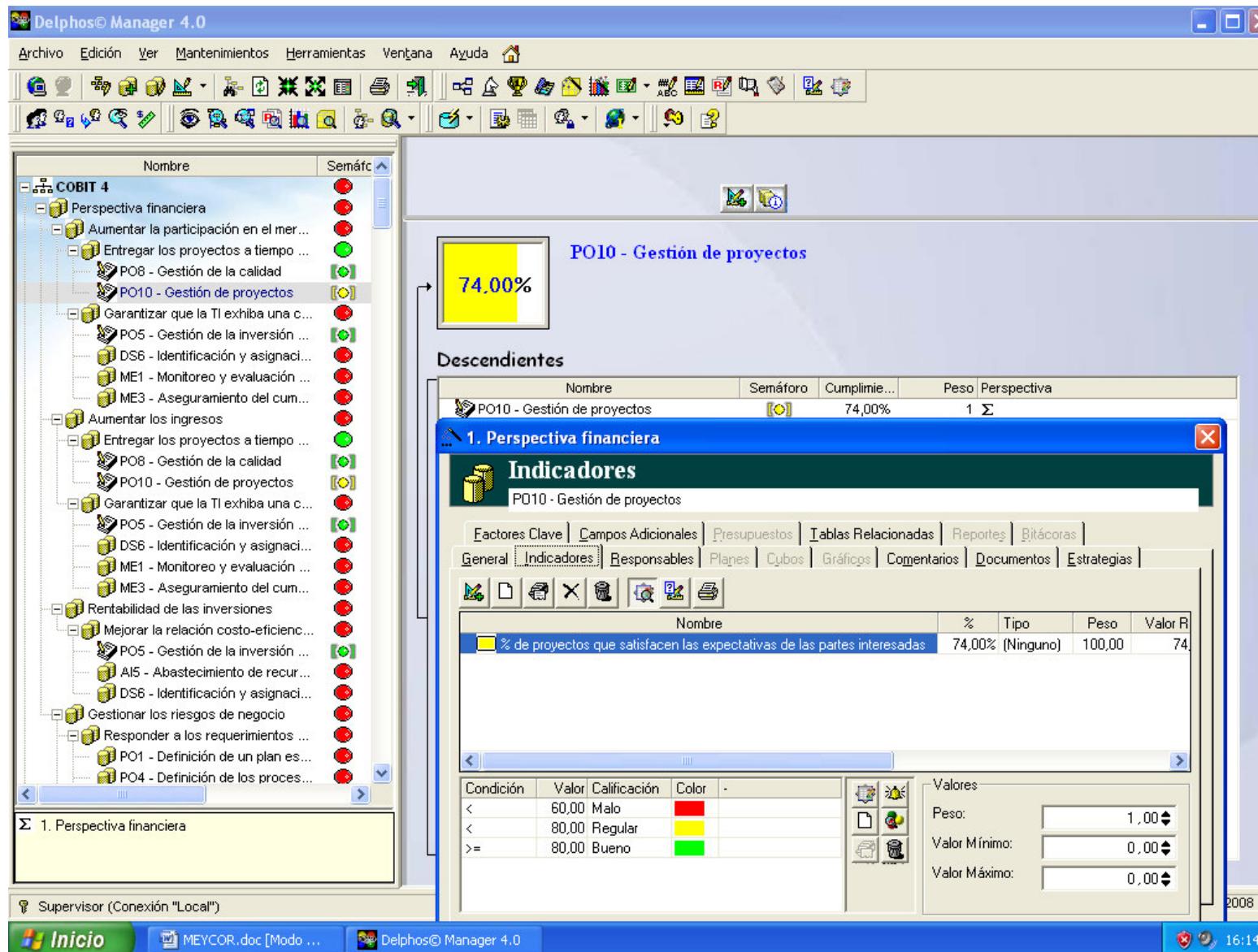
MEYCOR.doc [Modo ...] Meycor COBIT MG v....

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.

NORMA TÉCNICA COLOMBIANA

NTC-ISO
28000

2008-11-26

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO



E: SPECIFICATION FOR SECURITY MANAGEMENT SYSTEMS
FOR THE SUPPLY CHAIN

CORRESPONDENCIA: esta norma es una adopción idéntica por traducción (IDT), respecto a su documento de referencia, la norma ISO 28000:2007.

DESCRIPTORES: logística; cadena; suministro; sistema de gestión.

I.C.S.: 47.020.99

Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)
Apartado 14237 Bogotá, D.C. - Tel. (571) 6078888 - Fax (571) 2221435

PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 2269 de 1993.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La norma NTC-ISO 28000 fue ratificada por el Consejo Directivo de 2008-11-26.

Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se relacionan las empresas que colaboraron en el estudio de esta norma a través de su participación en el Comité Técnico 172 Transporte terrestre de carga.

ALMACENES GENERALES DE DEPÓSITO
GRAN COLOMBIA S.A. -ALMAGRAN-
ALPINA S.A.
ASOCIACIÓN COLOMBIANA DE
EMPRESAS CARROCERAS -ASCECAR-
AXÓNICA
C.I DISAN S.A.
CARROCERÍAS BENFOR
CARROCERÍAS EL SOL
COLFECAR
COLOMBIANA DE TANQUES LTDA.
-COLTANQUES LTDA.-

COLSEGUROS
ICOLLANTAS
INLAC
METROPYME
QUALITAS INGENIERÍA
SERVIENTREGA S.A.
SOANSES. LTDA.
SOCIEDAD TRACTEC
TITADSU
TRANSPORTE BOTERO SOTO
VALENTINA S.A.

Además de las anteriores, en Consulta Pública el Proyecto se puso a consideración de las siguientes empresas:

3M COLOMBIA
ABBOTT LABORATORIOS DE COLOMBIA S.A.
ACCIÓN SOCIAL - PRESIDENCIA DE LA
REPÚBLICA
ACERÍAS DE CALDAS S.A.
ACERÍAS DE COLOMBIA -ACESCO-
ACUAVIVA S.A. E.S.P.
ACUEDUCTO DE BOGOTÁ
ALCALDÍA MUNICIPAL DE CALI
ALDÍA LOGÍSTICA

ALFA SERVICIOS DE GESTIÓN
EMPRESARIAL
ALIMENTOS KRAFT
ALKOSTO
ALMACENAR
ALMACENES ÉXITO
ALTHVIZ & CÍA. LTDA.
ANALDEX
ASESORÍAS TÉCNICAS CORREDORES
DE SEGUROS -ASTEC-

ASOCIACIÓN COLOMBIANA DE LA MICRO,
PEQUEÑAS Y MEDIANAS EMPRESAS -ACOPI-
ASOCIACIÓN COLOMBIANA DEL PESAJE
-ASOPESAJE-
ASOCIACIÓN DE TRANSPORTADORES
INDEPENDIENTES -ATRIN-
ASOCIACIÓN NACIONAL DE INDUSTRIALES
-ANDI-
ASOCIACIÓN NACIONAL DE TRANSPORTADORES
-ASOTRANS-
ASOCIADOS DISTRIBUIDORES DE
DERIVADOS DEL PETRÓLEO -ADISPETROL-
ATENCIÓN TÉCNICA EN CALIDAD LTDA.
AUTO AIRES S.A.
AUTO FUSA S.A.
AVON
BAVARIA S.A.
BEC INTERNATIONAL LTDA.
BUREAU VERITAS CERTIFICATION
C.I. DE AZÚCARES Y MIELES S.A.
C.I. DISAN S.A.
CAFAM
CAJA DE COMPENSACIÓN FAMILIAR
-COMPENSAR-
CAJAS Y SUPLEMENTOS
CÁMARA DE COMERCIO DE CALI
CAMIONES Y REMOLQUES LTDA.
CARULLA
CARVAJAL S.A.
CASA LUKER S.A.
CENTELSA
CENTRALES DE TRANSPORTES S.A.
CENTROORIENTE S.A.
CHALLENGER
CHALLENGER S.A.
CIA COLOMBIANA DE TRANSPORTES S.A.
-COLDETRANS S.A.-
CLÍNICA DE OCCIDENTE S.A.
COCA-COLA - PANAMCO COLOMBIA S.A.
COLCERÁMICA
COLGATE PALMOLIVE
COLOMBIANA KIMBERLY COLPAPEL S.A.
COMFAMA
COMFENALCO SANTANDER
COMPAÑÍA COLOMBIANA AUTOMOTRIZ
COMPAÑÍA DE CARGA MOVITRSPORTES
LTDA.
COMPAÑÍA DE DISTRIBUCIÓN Y
TRANSPORTE S.A. -DITRANSA S.A.-
COMPAÑÍA DE GALLETAS NOEL

COMPAÑÍA ESPECIALIZADA EN TRANSPORTES
TERRESTRES LTDA -CETTA LTDA-
COMPAÑÍA NACIONAL DE CHOCOLATES
COMPAÑÍA NACIONAL DE TRANSPORTE
-CONALTRA-
CONCALIDAD LTDA.
CONCRETO S.A.
COOPERATIVA DE TRANSPORTADORES
DEL SUR COTRASUR
COOPERATIVA DE TRANSPORTADORES
VELOTAX LTDA.
COOPERATIVA DE TRANSPORTE DE
CARGA Y LOGÍSTICA
COORDINADORA DE CALIDAD
COORDINADORA INTERNACIONAL DE
CARGA -CORDICARGAS-
CORPORACIÓN ANDINA DE FOMENTO
-CAF-
CORPORACIÓN COLOMBIANA DE LOGÍSTICA
S.A. ALMADELCO -LÓGICA O.T.M.
CORPORACIÓN CYGA
CORPORACIÓN EDUCATIVA MINUTO DE
DIOS
CREDIBANCO VISA
CRITICAL CARGOS ENTER PRICE LTDA.
DESPACHADORA INTERNACIONAL DE
COLOMBIA
DIRECCIÓN DE IMPUESTOS Y ADUANAS
NACIONALES -DIAN-
DUPONT DE COLOMBIA S.A.
ECOPETROL S.A.
EDUARDO BOTERO SOTO Y CÍA LTDA.
EMPRESA COLOMBIANA DE SOPLADO E
INYECCIÓN ECSI S.A.
EMPRESA DE TELECOMUNICACIONES
DE BOGOTÁ -ETB-
ENCLAN S.A.
ENLACE OPERATIVO
EPM BOGOTÁ ESP
ESCUELA COLOMBIANA DE
INGENIERÍA/FACULTAD DE INGENIERÍA
INDUSTRIAL
EXPRESS DEL FUTURO S.A.
EXTRUPLASTIK LTDA.
FABRICATO S.A.
FEDECAME
FEDERACIÓN NACIONAL DE
COMERCIANTES -FENALCO-
FLEXO SPRING S.A.
FORD MOTOR DE COLOMBIA

FORTALEZA DE TRANSPORTES LTDA.
-FORTRANS LTDA.-
G2 CONSULTORES
GASES DEL LLANO S.A. E.S.P. LLANOGAS
GCO SISTEMAS DE GESTIÓN INTEGRAL S.A.
GENERAL MOTORS COLMOTORES
GEOMATRIX S.A.
GESTIÓN DE TECNOLOGÍA LTDA.
GESTIONARTE CONSULTORES
GIMNASIO FEMENINO
GRASCO
GRUPO SIS LTDA.
HOSPITAL SAN VICENTE ESE DE MONTENEGRO
IAC
IBM DE COLOMBIA S.A.
INCELT S.A.
INDEPENDIENTE -CARLOS JULIO ROCHA-
INDUSTRIA COLOMBIANA DE LOGÍSTICA Y
TRANSPORTE LTDA. -ICOLTRANS LTDA.-
INDUSTRIA FARMACÉUTICA SYNTOFARMA
S.A.
INDUSTRIA PARA LABORATORIOS S.A.
INDUSTRIAS ALIMENTICIAS NOEL
INDUSTRIAS HACEB S.A.
INDUSTRIAS PHILIPS DE COLOMBIA S.A.
INMOBILIARIA LLERAS E.U.
INTERANDINA DE TRANSPORTE. LTDA.
-INANTRA-
INTERCARGUEROS ANDINOS LTDA.
JOHNSON & JOHNSON DE COLOMBIA S.A.
KENWORTH DE LA MONTAÑA
LABORATORIOS PFIZER S.A.
LAFAYETTE S.A -ZYLETTE S.A.-
LEXCO S.A. CANON
LOGÍSTICA DE TRANSPORTE
LUMINEX S.A.
MARQUES Y URIZA LTDA.
MICHELIN COLOMBIA
MINISTERIO DE COMERCIO, INDUSTRIA Y
TURISMO
MINISTERIO DE TRANSPORTE
MOTORIZADOS EXPRESS LTDA.
MOTOTRANSPORTAR S.A.
MOVISTAR
MULTINACIONAL TRANSPORTADORA LTDA.
MUNDIAL DE ALUMINIOS
MURALLA SEGURIDAD LTDA.
NESTLE DE COLOMBIA
OFIXPRESS
OMNITRACS COLOMBIA
OPEN MARKET
ORGANIZACIÓN TERPEL

PARQUES Y FUNERARIAS S.A.
PETROCOMBUSTIBLES LTDA.
PINTURAS TERINSA
POLICÍA NACIONAL CARRETERAS
PRODUCTOS ALIMENTICIOS DORIA
PROFESIONALES EN DEPORTE
PRODEPORT LTDA. / CGS LTDA.
PROPIETARIOS DE CAMIONES S.A.
-PROCAM S.A.-
PROPILCO S.A.
PROVEEDOR & SERCARGA S.A.
PROVEMEL LTDA.
PROYECTANDO - ASESORÍAS EN GESTIÓN
ORGANIZACIONAL LTDA.
QMS ASESORES
QUINTERO HERMANOS
REDES HUMANAS LTDA.
RETAR INGENIEROS LTDA.
ROJAS TRASTEOS SERVICIO URBANO
BOGOTÁ
SAC
SAMSUNG
SCHRADER CAMARGO S.A.
SECRETARIA DE TRÁNSITO Y
TRANSPORTE
SENA - CENTRO DE GESTIÓN INDUSTRIAL
SIEMENS
SIKA COLOMBIA S.A.
SMS CALIDAD & PROCEDIMIENTOS EU
SOANSES LTDA.
SOLETANCHE BACHY CIMAS S.A.
SSI-SERVICIO DE SALUD INMEDIATO
SUPERINTENDENCIA DE INDUSTRIA Y
COMERCIO
SUPERPOLO S.A.
SURAMERICANA DE TRANSPORTES S.A.
T.D.M. TRANSPORTES S.A.
TANQUES DEL NORDESTE LTDA.
TANQUES Y CAMIONES
TECNICONTROL S.A.
TECNOQUÍMICAS S.A.
TRACTOCARGA LTDA
TRACTOMULAS Y CAMIONES DEL CARIBE
TRÁFICOS Y FLETES S.A.
TRAMAQ
TRANSERVICIOS LTDA.
TRANSGRANOS DE COLOMBIA
TRANSILVHER LTDA.
TRANSPARENCIA POR COLOMBIA
TRANSPORTADORA COMERCIAL COLOMBIANA
-T.C.C.-

TRANSPORTE DE CARGA EXPRESS DE COLOMBIA LTDA. TRACEXCOL
TRANSPORTES EGO LTDA.
TRANSPORTES ESPECIALIZADOS RTR LTDA.
TRANSPORTES J.R. LTDA.
TRANSPORTES LA PETROLERA VLIMAR LTDA.
TRANSPORTES M & S S.A.
TRANSPORTES MONRUB & CIA. LTDA.
TRANSPORTES MULTIGRANEL S.A.
TRANSPORTES PREMMIER LTDA.
TRANSPORTES SIVAL

TRANSPORTES TERRESTRES DE CARGA LTDA.
TRANSPORTES VIGIA S.A.
TRANSPORTES VILLAGÓMEZ LTDA.
TRANSPORTES Y SERVICIOS LTDA.
-TRANSER LTDA.-
UNIAGRARIA
UNISYS DE COLOMBIA
UNIVERSIDAD AMÉRICA
UNIVERSIDAD CATÓLICA DE COLOMBIA
UNIVERSIDAD DEL MAGDALENA
YANBAL DE COLOMBIA S.A.

I CONTEC cuenta con un Centro de Información que pone a disposición de los interesados normas internacionales, regionales y nacionales y otros documentos relacionados.

DIRECCIÓN DE NORMALIZACIÓN

CONTENIDO

	Página
0. INTRODUCCIÓN	1
1. OBJETO Y CAMPO DE APLICACIÓN	2
2. REFERENCIAS NORMATIVAS	3
3. TÉRMINOS Y DEFINICIONES	3
4. ELEMENTOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD	4
4.1 REQUISITOS GENERALES.....	5
4.2 POLÍTICA DE GESTIÓN DE LA SEGURIDAD.....	5
4.3 EVALUACIÓN DEL RIESGO DE SEGURIDAD Y PLANIFICACIÓN	6
4.4 IMPLEMENTACIÓN Y OPERACIÓN	9
4.5 VERIFICACIÓN Y ACCIÓN CORRECTIVA	12
4.6 REVISIÓN POR LA DIRECCIÓN Y MEJORA CONTINUA	14
BIBLIOGRAFÍA.....	19
DOCUMENTO DE REFERENCIA.....	20
FIGURAS	
Figura 1. Relación entre la ISO 28000 y otras normas pertinentes.....	1
Figura 2. Elementos del sistema de gestión de la seguridad.....	4
ANEXOS	
ANEXO A (Informativo) CORRESPONDENCIA ENTRE LAS NORMAS ISO 28000:2007, ISO 14001:2004 E ISO 9001:2000	16

SISTEMAS DE GESTIÓN DE LA SEGURIDAD PARA LA CADENA DE SUMINISTRO

0. INTRODUCCIÓN

Esta norma ha sido desarrollada en respuesta a la exigencia de la industria de una norma de gestión de la seguridad. Su objetivo esencial es mejorar la seguridad de las cadenas de suministro. Esta es una norma de gestión de alto nivel que posibilita a una organización establecer un sistema de gestión de la seguridad de la cadena de suministro en general. Exige a la organización evaluar el ambiente de seguridad en el que opera y determinar si se han implementado medidas de seguridad adecuadas y si ya existen otros requisitos de reglamentación que la organización cumple. Si se identifican necesidades de seguridad mediante este proceso, la organización debería implementar mecanismos y procesos para satisfacerlas. Puesto que las cadenas de suministro son dinámicas por naturaleza, algunas organizaciones que manejan múltiples cadenas de suministro pueden buscar que sus proveedores de servicios cumplan las normas ISO de seguridad para la cadena de suministro o las normas gubernamentales relacionadas, como condición para ser incluidos en dicha cadena de suministro a fin de simplificar la gestión de la seguridad, como se ilustra en la Figura 1.

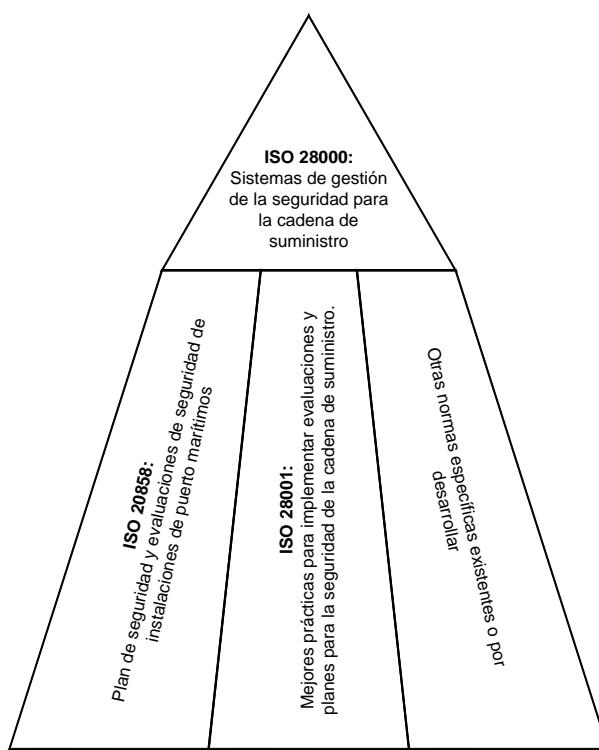


Figura 1. Relación entre la ISO 28000 y otras normas pertinentes

Se prevé la aplicación de la presente norma en casos donde las cadenas de suministro de una organización deben manejarse de manera segura. Un enfoque formal hacia la gestión de la seguridad puede contribuir directamente a la capacidad empresarial y a la credibilidad de la organización.

La conformidad con esta norma no confiere por sí misma exención de las obligaciones legales. Para organizaciones que así lo deseen, pueden verificar la conformidad del sistema de gestión de la seguridad con esta norma mediante un proceso de auditoría externa o interna.

La presente norma se basa en el formato ISO adoptado por la ISO 14001:2004 debido a su enfoque de sistemas de gestión basado en el riesgo. Sin embargo, las organizaciones que han adoptado un enfoque de procesos hacia los sistemas de gestión (por ejemplo ISO 9001:2000) pueden usar su sistema de gestión existente como fundamento para un sistema de gestión de la seguridad, según se prescribe en esta norma. Con esta norma no se pretende duplicar los requisitos y normas gubernamentales concernientes a la gestión de la seguridad de la cadena de suministro con base en las cuales la organización ya se ha certificado o se ha verificado su conformidad. La verificación puede realizarla una organización aceptable por primera, segunda o tercera parte.

NOTA Esta norma se basa en la metodología conocida como Planificar-Hacer-Verificar-Actuar (PHVA). PHVA se puede describir de la siguiente manera:

- Planificar: Establecer los objetivos y procesos necesarios para entregar resultados de acuerdo con la política de seguridad de la organización.
- Hacer: Implementar los procesos.
- Verificar: Supervisar y medir procesos contra la política de seguridad, objetivos, metas, requisitos legales y otros y reportar resultados.
- Actuar: Tomar acciones para mejorar continuamente el desempeño del sistema de gestión de la seguridad.

1. OBJETO Y CAMPO DE APLICACIÓN

Esta norma especifica los requisitos para un sistema de gestión de la seguridad, incluidos aquellos aspectos críticos para el aseguramiento de la seguridad de la cadena de suministro. La gestión de la seguridad está relacionada con muchos otros aspectos de la gestión empresarial, que incluyen todas las actividades controladas o influenciadas por organizaciones que impacta en la seguridad de la cadena de suministro. Estos otros aspectos se deberían considerar directamente cuando y donde tengan impacto en la gestión de la seguridad, incluido el transporte de estos bienes a lo largo de la cadena de suministro.

La presente norma es aplicable a organizaciones de todos los tamaños, desde las pequeñas hasta las multinacionales, de manufactura, servicios, almacenamiento o transporte en cualquier etapa de la producción o la cadena de suministro que deseé:

- a) establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad;
- b) asegurar la conformidad con la política de gestión de la seguridad establecida;
- c) demostrar dicha conformidad ante otros;
- d) buscar certificación/registro de su sistema de gestión de la seguridad por un organismo de certificación de tercera parte, acreditado; o

- e) realizar una auto-determinación y auto-declaración de la conformidad con esta norma.

Existen códigos legislativos y de reglamentación que abordan algunos de los requisitos de esta norma.

Esta norma no pretende exigir una doble demostración de la conformidad.

Las organizaciones que optan por la certificación por una tercera parte pueden demostrar además que están contribuyendo significativamente a la seguridad de la cadena de suministro.

2. REFERENCIAS NORMATIVAS

No se citan normas de referencia. Se incluye este numeral para conservar el esquema de numerales similar a otras normas de sistemas de gestión.

3. TÉRMINOS Y DEFINICIONES

Para los propósitos de esta norma se aplican los términos y definiciones siguientes:

3.1 Instalación. Planta, maquinaria, propiedad, edificios, vehículos, embarcaciones, instalaciones portuarias y otros elementos de infraestructura o plantas y sistemas relacionados que cumplen una función o servicio empresarial distintivo y cuantificable.

NOTA Esta definición incluye cualquier código de software que sea crítico para la obtención de seguridad y la aplicación de gestión de la seguridad.

3.2 Seguridad. Resistencia a actos intencionales, sin autorización, destinados a causar perjuicio o daño a, o mediante, la cadena de suministro.

3.3 Gestión de la seguridad. Actividades y prácticas sistemáticas y coordinadas por medio de las cuales una organización maneja óptimamente sus riesgos y las amenazas e impactos potenciales asociados derivados de ellos.

3.4 Objetivo de gestión de la seguridad. Resultado o logro específico de seguridad requerido a fin de cumplir la política de gestión de la seguridad.

NOTA Es esencial que dichos resultados se relacionen directa o indirectamente con la entrega de productos, suministros o servicios prestados por la totalidad de la empresa a sus clientes o usuarios finales.

3.5 Política de gestión de la seguridad. Intenciones y direcciones generales de una organización, relacionadas con la seguridad y la estructura para el control de los procesos y actividades que tienen que ver con la seguridad, que se derivan de la política y los requisitos de reglamentación de la organización y son coherentes con ellos.

3.6 Programas de gestión de la seguridad. Medios por los cuales se logra un objetivo de gestión de la seguridad.

3.7 Meta de la gestión de la seguridad. Nivel de desempeño específico requerido para alcanzar un objetivo de gestión de la seguridad.

3.8 Parte involucrada. Persona o entidad con un interés establecido en el desempeño de la organización, su éxito o el impacto de sus actividades.

NOTA Son ejemplos: los clientes, accionistas, entidades financieras, aseguradoras, reglamentadores, organismos estatutarios, empleados, contratistas, proveedores, agremiaciones laborales, o la sociedad.

3.9 Cadena de suministro. Conjunto relacionado de recursos y procesos que comienza con el suministro de materias primas y se extiende hasta la entrega de productos o servicios al usuario final, incluidos los medios de transporte.

NOTA La cadena de suministro puede incluir vendedores, instalaciones de manufactura, proveedores de logística, centros de distribución interna, distribuidores, mayoristas y otras entidades que conducen al usuario final.

3.9.1 Aguas abajo. Se refiere a las acciones, procesos y movimientos de la carga en la cadena de suministro, que ocurren después de que la carga sale del control operacional directo de la organización, incluidas la gestión de los seguros, las finanzas y los datos, y el empaque, almacenamiento y transferencia de la carga, entre otros.

3.9.2 Aguas arriba. Se refiere a las acciones, procesos y movimientos de la carga en la cadena de suministro, que ocurren antes de que la carga se encuentre bajo el control operacional de la organización, incluida la gestión de datos, las finanzas y los seguros y el empaque, almacenamiento y transferencia de la carga, entre otros.

3.10 Alta dirección. Persona o grupo de personas que dirige y controla una organización en el nivel superior.

NOTA Es posible que la alta dirección, especialmente en una gran organización multinacional, no esté involucrada personalmente como se describe en la presente norma; sin embargo, la responsabilidad de la alta dirección a través de la cadena de mando debe ser manifiesta.

3.11 Mejora continua. Proceso recurrente de fortalecer el sistema de gestión de la seguridad a fin de lograr mejoras en el desempeño de la seguridad en general de manera coherente con la política de seguridad de la organización.

4. ELEMENTOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD



Figura 2. Elementos del sistema de gestión de la seguridad

4.1 REQUISITOS GENERALES

La organización debe establecer, documentar, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad eficaz para identificar las amenazas a la seguridad, evaluar los riesgos y controlar y mitigar sus consecuencias.

La organización debe mejorar continuamente su eficacia de acuerdo con los requisitos establecidos en todo el numeral 4.

La organización debe definir el alcance de su sistema de gestión de la seguridad. Cuando la organización opte por contratar externamente cualquier proceso que afecte la conformidad con estos requisitos, la organización debe asegurar que se controlen dichos procesos. Se deben identificar dentro del sistema de gestión de la seguridad los controles y responsabilidades necesarios para dichos procesos contratados externamente.

4.2 POLÍTICA DE GESTIÓN DE LA SEGURIDAD

La alta dirección de la organización debe autorizar una política de gestión de la seguridad general. La política debe:

- a) ser coherente con otras políticas organizacionales;
- b) proporcionar el marco de referencia para establecer objetivos, metas y programas específicos de gestión de la seguridad;
- c) ser coherente con la estructura de la gestión de amenazas y riesgos de la seguridad general de la organización;
- d) ser apropiada para las amenazas de la organización y la naturaleza y escala de sus operaciones;
- e) determinar claramente los objetivos generales/amplios de gestión de la seguridad;
- f) incluir un compromiso con la mejora continua del proceso de gestión de la seguridad;
- g) incluir un compromiso de cumplir con la legislación actual aplicable, los requisitos de reglamentación y estatutarios y otros requisitos que suscribe la organización;
- h) tener el respaldo visible de la alta dirección;
- i) ser documentada, implementada y mantenida;
- j) comunicarse a todos los empleados y terceras partes pertinentes, incluidos los contratistas y visitantes, con la intención de que estas personas sean conscientes de sus obligaciones individuales relacionadas con la gestión de la seguridad;
- k) estar disponible para las partes interesadas, cuando resulte apropiado;
- l) poderse revisar en caso de adquisición o fusión con otras organizaciones, u otro cambio en el alcance del negocio de la organización que pueda afectar la continuidad o pertinencia del sistema de gestión de la seguridad.

NOTA Las organizaciones pueden optar por una política de gestión de la seguridad detallada para uso interno que ofrezca suficiente información y dirección para orientar el sistema de gestión de la seguridad (algunas partes de éste pueden ser confidenciales) y una versión resumida (no confidencial) que contenga los objetivos generales para divulgación entre sus partes involucradas y otras partes interesadas.

4.3 EVALUACIÓN DEL RIESGO DE SEGURIDAD Y PLANIFICACIÓN

4.3.1 Evaluación del riesgo de seguridad

La organización debe establecer y mantener procedimientos para la identificación y evaluación continua de las amenazas a la seguridad y de las amenazas y riesgos relacionados con la gestión de la seguridad y la implementación de medidas necesarias de control de gestión. La identificación, evaluación y los métodos de control de amenazas y riesgos de la seguridad deberían, como mínimo, ser apropiados a la naturaleza y escala de las operaciones. Esta evaluación debe considerar la probabilidad de un evento y todas sus consecuencias, que deben incluir:

- a) amenazas y riesgos de falla física, tales como falla funcional, daño incidental, daño malicioso o terrorista o acción criminal;
- b) amenazas y riesgos operacionales, incluidos el control de la seguridad, los factores humanos y otras actividades que afectan el desempeño, la condición o la seguridad de las organizaciones;
- c) eventos del medio ambiente natural (tormentas, inundaciones, etc.) que pueden hacer que las medidas y equipos de seguridad resulten ineficaces;
- d) factores por fuera del control de la organización, tales como fallas en el equipo y servicios suministrados externamente;
- e) amenazas y riesgos de las partes involucradas, tales como falla en cumplir los requisitos de reglamentación o daño a la reputación o la marca;
- f) diseño e instalación del equipo de seguridad, incluido su reemplazo, mantenimiento, etc.;
- g) gestión de datos e información y comunicaciones;
- h) una amenaza a la continuidad de las operaciones.

La organización debe asegurar que se consideren los resultados de estas evaluaciones y los efectos de estos controles y, cuando resulte apropiado, debe proporcionar elementos de entrada a:

- a) los objetivos y metas de gestión de la seguridad;
- b) los programas de gestión de la seguridad;
- c) la determinación de requisitos para el diseño, especificación e instalación;
- d) la identificación de recursos adecuados, incluidos los niveles de contratación de personal;
- e) la identificación de necesidades de formación y habilidades (véase el numeral 4.4.2);
- f) el desarrollo de controles operacionales (véase el numeral 4.4.6);

- g) la estructura general de gestión de amenazas y riesgos de la organización.

La organización debe documentar y mantener actualizada la anterior información.

La metodología de la organización para la identificación y evaluación de riesgos debe:

- a) estar definida con respecto a su alcance, naturaleza y programación en el tiempo, para asegurar que sea proactiva en vez de reactiva;
- b) incluir la información recolectada acerca de las amenazas y riesgos de la seguridad;
- c) proporcionar la clasificación de amenazas y riesgos y la identificación de aquellos que deben evitarse, eliminarse o controlarse;
- d) proporcionar el seguimiento de las acciones para garantizar su eficacia y oportuna implementación (véase el numeral 4.5.1).

4.3.2 Requisitos de seguridad legales, estatutarios y otros regulatorios

La organización debe establecer, implementar y mantener un procedimiento:

- a) para identificar y tener acceso a los requisitos legales aplicables y otros requisitos que suscribe la organización en relación con sus amenazas y riesgos para la seguridad, y
- b) para determinar cómo se aplican estos requisitos a sus amenazas y riesgos para la seguridad.

La organización debe mantener actualizada esta información, y debe comunicar la información pertinente sobre requisitos legales y otros a sus empleados y otras terceras partes pertinentes, incluidos los contratistas.

4.3.3 Objetivos de gestión de la seguridad

La organización debe establecer, implementar y mantener objetivos de gestión de la seguridad documentados, en las funciones y niveles pertinentes dentro de la organización. Los objetivos deben derivarse de la política y ser coherentes con ella. Al establecer y revisar sus objetivos, una organización debe tener en cuenta:

- a) requisitos legales, estatutarios y otros de reglamentación sobre seguridad;
- b) amenazas y riesgos relacionados con la seguridad;
- c) opciones tecnológicas y otras;
- d) requisitos financieros, operacionales y empresariales;
- e) puntos de vista de las partes interesadas apropiadas.

Los objetivos de gestión de la seguridad deben:

- a) ser coherentes con el compromiso de la organización con la mejora continua;
- b) cuantificarse (cuando sea posible);

- c) comunicarse a todos los empleados y terceras partes pertinentes, incluidos los contratistas, con la intención de que tales personas sean conscientes de sus obligaciones individuales;
- d) revisarse periódicamente para garantizar que sigan siendo pertinentes y coherentes con la política de gestión de la seguridad. Cuando sea necesario, se deben corregir de acuerdo con los objetivos de gestión de la seguridad.

4.3.4 Metas de gestión de la seguridad

La organización debe establecer, implementar y mantener las metas de gestión de la seguridad documentadas, apropiadas para las necesidades de la organización. Las metas deben derivarse de los objetivos de gestión de la seguridad y ser coherentes con ellos.

Estas metas deben:

- a) tener un nivel apropiado de detalles;
- b) ser específicos, medibles, obtenibles, pertinentes y con base en el tiempo (cuando sea aplicable);
- c) comunicarse a todos los empleados y terceras partes pertinentes, incluidos los contratistas, con la intención de que tales personas sean conscientes de sus obligaciones individuales;
- d) revisarse periódicamente para asegurar que sigan siendo pertinentes y coherentes con los objetivos de gestión de la seguridad. Donde sea necesario las metas se deben ajustar consecuentemente.

4.3.5 Programas de gestión de la seguridad

La organización debe establecer, implementar y mantener programas de gestión de la seguridad para lograr sus objetivos y metas.

Los programas deben optimizarse y luego priorizarse y la organización debe prever el uso de los costos de manera eficiente y eficaz en la implementación de estos programas.

Se debe incluir documentación que describa:

- a) la responsabilidad y autoridad designada para lograr objetivos y metas de gestión de la seguridad;
- b) los medios y la escala en el tiempo por medio de los cuales se logran los objetivos y metas de gestión de la seguridad.

Los programas de gestión de la seguridad deben revisarse periódicamente para asegurar que se mantienen efectivos y coherentes con los objetivos y metas. Cuando sea necesario, los programas se deben ajustar consecuentemente.

4.4 IMPLEMENTACIÓN Y OPERACIÓN

4.4.1 Estructura, autoridad y responsabilidades para la gestión de la seguridad

La organización debe establecer y mantener una estructura organizacional de funciones, responsabilidades y autoridad, de manera coherente con el logro de su política, objetivos, metas y programas de gestión de la seguridad.

Estas funciones, responsabilidades y autoridades se deben definir, documentar y comunicar a los individuos responsables de la implementación y mantenimiento.

La alta dirección debe presentar evidencia de su compromiso con el desarrollo e implementación del sistema de gestión de la seguridad (procesos) y mejorar continuamente su eficacia mediante las siguientes acciones:

- a) nombrar un miembro de la alta dirección quien, independientemente de sus otras responsabilidades, debe ser responsable del diseño, mantenimiento, documentación y mejora generales del sistema de gestión de la seguridad de la organización;
- b) nombrar un miembro (o varios) de la dirección, con la autoridad necesaria para garantizar que se implementen los objetivos y metas;
- c) identificar y hacer seguimiento a los requisitos y expectativas de las partes interesadas de la organización y emprender las acciones apropiadas y oportunas para manejar dichas expectativas;
- d) garantizar la disponibilidad de recursos adecuados;
- e) considerar el impacto adverso que la política, los objetivos, las metas, los programas, etc., de gestión de la seguridad pueden tener en otros aspectos de la organización;
- f) garantizar que cualquier programa de seguridad generado por otras partes de la organización complementa el sistema de gestión de la seguridad;
- g) comunicar a la organización la importancia de cumplir sus requisitos de gestión de la seguridad a fin de cumplir con su política;
- h) garantizar que las amenazas y riesgos relacionados con la seguridad sean evaluados y se incluyan en evaluaciones de amenazas y riesgos organizacionales, según resulte apropiado;
- i) garantizar la viabilidad de los objetivos, metas y programas de gestión de la seguridad.

4.4.2 Competencia, entrenamiento y toma de conciencia

La organización debe garantizar que el personal responsable del diseño, operación y gestión de equipos y procesos de seguridad esté calificado adecuadamente en lo relativo a educación, entrenamiento o experiencia o ambas. La organización debe establecer y mantener procedimientos para que las personas que trabajan para ella o en su nombre sean conscientes de:

- a) la importancia del cumplimiento de la política y procedimientos de gestión de la seguridad y los requisitos del sistema de gestión de la seguridad;

- b) sus funciones y responsabilidades en el logro de la conformidad con la política y procedimientos de gestión de la seguridad y con los requisitos del sistema de gestión de la seguridad, incluidos los requisitos de preparación y respuesta ante emergencias;
- c) las consecuencias potenciales que tiene para la seguridad de la organización desviarse de los procedimientos de operación especificados.

Se deben llevar registros de competencia y entrenamiento.

4.4.3 Comunicación

La organización debe contar con procedimientos para asegurar que la información pertinente de gestión de la seguridad se comunica hacia y desde los empleados relevantes, contratistas y otras partes interesadas.

Debido a la naturaleza confidencial de alguna información relacionada con la seguridad, se debería considerar adecuadamente la sensibilidad de la información antes de su divulgación.

4.4.4 Documentación

La organización debe establecer y mantener un sistema de documentación de gestión de la seguridad que incluya los siguientes aspectos (sin limitarse a ellos):

- a) la política, objetivos y metas de seguridad;
- b) la descripción del alcance del sistema de gestión de la seguridad;
- c) la descripción de los elementos principales del sistema de gestión de la seguridad y su interacción y referencia con documentos relacionados;
- d) los documentos, incluidos registros, exigidos en la presente norma, y
- e) los documentos, incluidos los registros, determinados por la organización como necesarios para garantizar la planificación, operación y control eficaces de los procesos relacionados con sus amenazas y riesgos para la seguridad significativos.

La organización debe determinar la confidencialidad de la información de seguridad y tomar las medidas para evitar el acceso no autorizado a ella.

4.4.5 Control de documentos y datos

La organización debe establecer y mantener procedimientos para controlar todos los documentos, datos e información exigidos en el numeral 4 de la presente norma a fin de garantizar que:

- a) sólo individuos autorizados puedan localizar y tener acceso a estos documentos, datos e información;
- b) personal autorizado revise periódicamente estos documentos, datos e información, los actualice según sea necesario y apruebe su conveniencia;
- c) se encuentren disponibles versiones actuales de los documentos, datos e información pertinentes en todos los lugares donde se realicen operaciones esenciales para el funcionamiento efectivo del sistema de gestión de la seguridad;

- d) los documentos, datos e información obsoletos sean retirados con prontitud de todos los puntos de emisión y de uso, o se asegure de otro modo que no se haga uso indeseado de ellos;
- e) se identifiquen adecuadamente los documentos de archivo, datos e información que se conservan con propósitos legales o de preservación del conocimiento, o ambos;
- f) dichos documentos, datos e información sean seguros y si se encuentran en formato electrónico, deben tener copia de seguridad adecuada y se puedan recuperar.

4.4.6 Control operacional

La organización debe identificar aquellas operaciones y actividades que sean necesarias para lograr:

- a) su política de gestión de la seguridad;
- b) el control de las actividades y la mitigación de amenazas identificadas como un riesgo significativo;
- c) la conformidad con requisitos legales, estatutarios y otros requisitos de reglamentación sobre seguridad;
- d) sus objetivos de gestión de la seguridad;
- e) la ejecución de sus programas de gestión de la seguridad;
- f) el nivel requerido de seguridad de la cadena de suministro.

La organización debe garantizar que estas operaciones y actividades se realicen bajo las condiciones especificadas mediante:

- a) el establecimiento, implementación y mantenimiento de procedimientos documentados para controlar situaciones en las que su ausencia podría conducir a falla en el logro de las operaciones y actividades enunciadas en el numeral 4.4.6, literales a) a f);
- b) la evaluación de cualquier amenaza que surja de las actividades aguas arriba de la cadena de suministro, y aplicación de controles para mitigar estos impactos en la organización y otros operadores aguas abajo de la cadena de suministro;
- c) el establecimiento y mantenimiento de los requisitos para bienes y servicios que tienen impacto en la seguridad, y comunicación de estos a proveedores y contratistas.

Estos procedimientos deben incluir controles para el diseño, instalación, operación, renovación y modificación de elementos de equipos, instrumentación etc., relacionados con la seguridad, según resulte apropiado. Cuando se actualicen las disposiciones existentes o se introduzcan nuevas que puedan causar impacto en las operaciones y actividades de gestión de la seguridad, la organización debe considerar las amenazas y riesgos de la seguridad asociados antes de su implementación. Las disposiciones nuevas o actualizadas que se vayan a considerar deben incluir:

- a) la estructura, funciones o responsabilidades organizacionales actualizadas;
- b) la política, objetivos, metas o programas de gestión de la seguridad actualizados;

- c) los procesos y procedimientos actualizados;
- d) la introducción de nueva infraestructura, equipos o tecnología de seguridad que pueden incluir hardware o software, o ambos;
- e) la introducción de nuevos contratistas, proveedores o personal, según sea apropiado.

4.4.7 Preparación y respuesta ante emergencias y recuperación de la seguridad

La organización debe establecer, implementar y mantener planes y procedimientos apropiados para identificar el potencial y las respuestas ante incidentes de seguridad y situaciones de emergencia, y para evitar y mitigar las consecuencias probables que se puedan asociar con ellos. Los planes y procedimientos deben incluir información acerca de la disposición y mantenimiento de cualquier equipo, instalaciones o servicios identificados que puedan requerirse durante o después de los incidentes o situaciones de emergencia.

La organización debe revisar periódicamente la eficacia de sus planes y procedimientos de preparación y respuesta ante emergencias y recuperación de la seguridad, en especial después de que ocurren incidentes o situaciones de emergencia causados por infracciones y amenazas a la seguridad. La organización debe poner a prueba periódicamente estos procedimientos, cuando sea aplicable.

4.5 VERIFICACIÓN Y ACCIÓN CORRECTIVA

4.5.1 Medición y seguimiento del desempeño de la seguridad

La organización debe establecer y mantener procedimientos para hacer seguimiento y medir el desempeño de su sistema de gestión de la seguridad. Además, debe establecer y mantener procedimientos para el seguimiento y medición del desempeño de la seguridad. Al establecer la frecuencia de medición y seguimiento de los parámetros de desempeño clave, la organización debe considerar las amenazas y riesgos de seguridad asociados, incluidos los mecanismos de deterioro potencial y sus consecuencias. Estos procedimientos deben proporcionar:

- a) medidas tanto cualitativas como cuantitativas, apropiadas para las necesidades de la organización;
- b) seguimiento del grado en el que se cumplen la política, objetivos y metas de la gestión de la seguridad de la organización;
- c) medidas proactivas de desempeño para hacer el seguimiento a la conformidad con los programas de gestión de la seguridad, los criterios de control operacionales y la legislación aplicable, los requisitos estatutarios y otros requisitos de reglamentación sobre seguridad;
- d) medidas reactivas de desempeño para hacer el seguimiento de deterioro, fallas, incidentes, no conformidades (incluidas las fallas que estuvieron a punto de ocurrir y las falsas alarmas) relacionadas con la seguridad y otra evidencia histórica de desempeño deficiente del sistema de gestión de la seguridad;
- e) registro de datos y resultados de seguimiento y medición suficientes para facilitar el análisis de las acciones preventivas y correctivas posteriores. Si se requiere equipo de seguimiento para el desempeño, y la medición o seguimiento, o todos ellos, la organización debe exigir que se establezcan y mantengan procedimientos para la calibración y mantenimiento de dicho equipo. Se deben conservar registros de las

actividades de calibración y mantenimiento durante tiempo suficiente, para cumplir con la legislación y la política de la organización.

4.5.2 Evaluación del sistema

La organización debe evaluar los planes, procedimientos y capacidades de gestión de la seguridad por medio de revisiones periódicas, ensayos, informes posteriores a los incidentes, lecciones aprendidas, evaluaciones de desempeño y ejercicios. Los cambios significativos en estos factores deben reflejarse de inmediato en el (los) procedimiento(s).

La organización debe evaluar periódicamente la conformidad con la legislación y las reglamentaciones pertinentes, las mejores prácticas industriales y la conformidad con su propia política y objetivos.

La organización debe llevar registros de los resultados de las evaluaciones periódicas.

4.5.3 Fallas relacionadas con la seguridad, incidentes, no conformidades y acciones correctivas y preventivas

La organización debe establecer, implementar y mantener procedimientos para definir la responsabilidad y autoridad para:

- a) evaluar e iniciar acciones preventivas para identificar las fallas potenciales en la seguridad, a fin de que se pueda evitar que ocurran;
- b) investigar los siguientes aspectos relacionados con la seguridad:
 - 1) fallas, incluidas las que estuvieron a punto de ocurrir, y las falsas alarmas;
 - 2) incidentes y situaciones de emergencia;
 - 3) no conformidades;
- c) emprender acciones para mitigar cualquier consecuencia de dichas fallas, incidentes o no conformidades;
- d) iniciar y completar las acciones correctivas;
- e) confirmar la eficacia de las acciones correctivas emprendidas.

Estos procedimientos deben exigir que se revisen todas las acciones correctivas y preventivas propuestas por medio del proceso de evaluación de amenazas y riesgos de seguridad antes de la implementación, a menos que la implementación inmediata impida exposiciones inminentes para la vida o seguridad pública.

Cualquier acción correctiva o preventiva emprendida para eliminar las causas de no conformidades reales y potenciales debe ser apropiada para la magnitud de los problemas y proporcional a las amenazas y riesgos de la seguridad que probablemente se encuentren. La organización debe implementar y registrar cualquier cambio en los procedimientos documentados que resulten de la acción correctiva y preventiva y debe incluir el entrenamiento requerido cuando fuera necesario.

4.5.4 Control de registros

La organización debe establecer y mantener registros, según sea necesario, para demostrar conformidad con los requisitos de su sistema de gestión de la seguridad y de esta norma, y de los resultados logrados.

La organización debe establecer, implementar y mantener un procedimiento (o varios) para la identificación, almacenamiento, protección, recuperación, retención y disposición de registros.

Los registros deben ser legibles y permanecer así, y deben ser identificables y trazables.

La documentación electrónica y digital debería estar protegida contra alteración, tener copia de seguridad y ser accesible sólo a personal autorizado.

4.5.5 Auditoría

La organización debe establecer, implementar y mantener un programa de auditoría de gestión de la seguridad y debe garantizar que las auditorías del sistema de gestión de la seguridad se realicen a intervalos planificados, a fin de:

- a) determinar si el sistema de gestión de la seguridad:
 - 1) cumple las disposiciones planificadas para gestión de la seguridad, incluidos los requisitos de la totalidad del numeral 4 de la presente norma;
 - 2) ha sido implementado y se mantiene adecuadamente;
 - 3) es eficaz para cumplir la política y objetivos de gestión de la seguridad de la organización;
- b) revisar los resultados de auditorías anteriores y las acciones emprendidas para rectificar las no-conformidades;
- c) proporcionar información a la dirección sobre los resultados de las auditorías;
- d) verificar el despliegue apropiado de los equipos y del personal de seguridad.

El programa de auditoria, incluido cualquier cronograma, debe estar basado en los resultados de las evaluaciones de amenazas y riesgos de las actividades de la organización y en los resultados de auditorías anteriores. Los procedimientos de auditoría deberían comprender el alcance, la frecuencia, las metodologías y competencias, lo mismo que las responsabilidades y requisitos para realizar auditorías y reportar resultados. Cuando sea posible, las auditorías las debe llevar a cabo personal independiente de los que tienen responsabilidad directa en la actividad que se está examinando.

NOTA La frase “personal independiente” no necesariamente significa personal externo a la organización.

4.6 REVISIÓN POR LA DIRECCIÓN Y MEJORA CONTINUA

La alta dirección debe revisar el sistema de gestión de la seguridad de la organización, a intervalos planificados, a fin de garantizar que siga siendo conveniente, suficiente y eficaz. Las revisiones deben incluir la evaluación de oportunidades de mejora y la necesidad de cambios en el sistema de gestión de la seguridad, incluida la política de seguridad, los objetivos, y las amenazas y los riesgos de la seguridad. Se deben retener registros de las revisiones realizadas por la dirección. La información de entrada de las revisiones por la dirección debe incluir:

- a) resultados de las auditorías y evaluaciones de conformidad con los requisitos legales y con otros requisitos que suscribe la organización;
- b) comunicación (es) de partes externas interesadas, incluidas quejas;
- c) el desempeño de la seguridad de la organización;
- d) el grado en el que se cumplen objetivos y metas;
- e) estado de las acciones correctivas y preventivas;
- f) acciones de seguimiento de revisiones por la dirección anteriores;
- g) circunstancias cambiantes, incluidos desarrollos en requisitos legales y otros, relacionados con aspectos de su seguridad, y
- h) recomendaciones de mejora.

La información de salida de las revisiones por la dirección debe incluir cualquier decisión y acción relacionada con cambios posibles a la política, objetivos, metas y otros elementos del sistema de gestión de la seguridad, de manera coherente con el compromiso con la mejora continua.

ANEXO A
(Informativo)

**CORRESPONDENCIA ENTRE LAS NORMAS ISO 28000:2007,
ISO 14001:2004 E ISO 9001:2000**

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
Requisitos del sistema de gestión de la seguridad de la cadena de suministro (sólo título)	4	Requisitos del sistema de gestión ambiental (sólo título)	4	Requisitos del sistema de gestión de la calidad (sólo título)	4
Requisitos generales	4.1	Requisitos generales	4.1	Requisitos generales	4.1
Política de gestión de la seguridad	4.2	Política ambiental	4.2	Compromiso de la dirección	5.1
				Política de la calidad	5.3
				Mejora continua	8.5.1
Evaluación del riesgo de seguridad y planificación (sólo título)	4.3	Planificación (sólo título)	4.3	Planificación (sólo título)	5.4
Evaluación del riesgo de seguridad	4.3.1	Aspectos ambientales	4.3.1	Enfoque al cliente	5.2
				Determinación de los requisitos relacionados con el producto	7.2.1
				Revisión de los requisitos relacionados con el producto	7.2.2
Requisitos legales, estatutarios y otros requisitos reglamentarios sobre seguridad	4.3.2	Requisitos legales y otros	4.3.2	Enfoque al cliente	5.2
				Determinación de los requisitos relacionados con el producto	7.2.1
Objetivos de gestión de la seguridad	4.3.3	Objetivos, metas y programa(s)	4.3.3	Objetivos de la calidad	5.4.1
				Planificación del sistema de gestión de la calidad	5.4.2
				Mejora continua	8.5.1
Objetivos de gestión de la seguridad	4.3.4	Objetivos, metas y programa(s)	4.3.3	Objetivos de la calidad	5.4.1
				Planificación del sistema de gestión de la calidad	5.4.2
				Mejora continua	8.5.1
Programa(s) de gestión de la seguridad	4.3.5	Objetivos, metas y programa(s)	4.3.3	Objetivos de la calidad	5.4.1
				Planificación del sistema de gestión de la calidad	5.4.2
				Mejora continua	8.5.1
Implementación y operación (sólo título)	4.4	Implementación y operación (sólo título)	4.4	Realización del producto (sólo título)	7
Estructura, autoridad y responsabilidades de la gestión de la seguridad	4.4.1	Recursos, funciones, responsabilidad y autoridad	4.4.1	Compromiso de la dirección	5.1
				Responsabilidad y autoridad	5.5.1
				Representante de la dirección	5.5.2
				Provisión de recursos	6.1
				Infraestructura	6.3

Continúa...

(Continuación)

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
Competencia, entrenamiento y toma de conciencia	4.4.2	Competencia, entrenamiento y toma de conciencia	4.4.2	(Recursos humanos) Generalidades	6.2.1
				Competencia, entrenamiento y toma de conciencia	6.2.2
Comunicación	4.4.3	Comunicación	4.4.3	Comunicación interna	5.5.3
				Comunicación con el cliente	7.2.3
Documentación	4.4.4	Documentación	4.4.4	(Requisitos de la documentación) Generalidades	4.2.1
Control de documentos y datos	4.4.5	Control de documentos	4.4.5	Control de documentos	4.2.3
Control operacional	4.4.6	Control operacional	4.4.6	Planificación de la realización del producto	7.1
				Determinación de los requisitos relacionados con el producto	7.2.1
				Revisión de los requisitos relacionados con el producto	7.2.2
				Planificación del diseño y desarrollo	7.3.1
				Elementos de entrada para el diseño y desarrollo	7.3.2
				Resultados del diseño y desarrollo	7.3.3
				Revisión del diseño y desarrollo	7.3.4
				Verificación del diseño y desarrollo	7.3.5
				Validación del diseño y desarrollo	7.3.6
				Control de cambios del diseño y desarrollo	7.3.7
				Proceso de compras	7.4.1
				Información de las compras	7.4.2
				Verificación de los productos comprados	7.4.3
				Control de la producción y de la prestación del servicio	7.5.1
				Validación de los procesos de producción y de prestación del servicio	7.5.2
				Preservación del producto	7.5.5
Preparación y respuesta ante emergencias y recuperación de la seguridad	4.4.7	Preparación y respuesta ante emergencias	4.4.7	Control del producto no conforme	8.3

(Final)

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
Verificación y acción correctiva (sólo título)	4.5	Verificación (sólo título)	4.5	Medición, análisis y mejora (sólo título)	8
Medición y seguimiento del desempeño de la seguridad	4.5.1	Seguimiento y medición	4.5.1	Control de los dispositivos de seguimiento y medición	7.6
				Generalidades (medición, análisis y mejora)	8.1
				Seguimiento y medición de los procesos	8.2.3
				Seguimiento y medición del producto	8.2.4
				Análisis de datos	8.4
Evaluación del sistema	4.5.2	Evaluación de conformidad	4.5.2	Seguimiento y medición de los procesos	8.2.3
				Seguimiento y medición del producto	8.2.4
Fallas relacionadas con la seguridad, incidentes, no conformidades y acciones correctivas y preventivas	4.5.3	No conformidad, acción correctiva y acción preventiva	4.5.3	Control del producto no conforme	8.3
				Análisis de datos	8.4
				Acción correctiva	8.5.2
				Acción preventiva	8.5.3
Control de registros	4.5.4	Control de registros	4.5.4	Control de los registros	4.2.4
Auditoría	4.5.5	Auditoría interna	4.5.5	Auditoría interna	8.2.2
Revisión por la dirección y mejora continua	4.6	Revisión por la dirección	4.6	Compromiso de la dirección	5.1
				Revisión por la dirección (sólo título)	5.6
				Generalidades	5.6.1
				Información para la revisión	5.6.2
				Resultados de la revisión	5.6.3
				Mejora continua	8.5.1

BIBLIOGRAFÍA

- [1] ISO 9001:2000, Sistemas de gestión de la calidad. Requisitos.
- [2] ISO 14001:2004, Sistemas de gestión ambiental. Requisitos con orientación para su uso.
- [3] ISO 19011:2002, Directrices para la auditoria de los sistemas de gestión de la calidad y/o ambiente.
- [4] ISO/PAS 20858:2004, *Ships and Marine Technology. Maritime Port Facility Security Assessments and Security Plan Development.*
- [5] ISO/PAS 28001, *Security Management Systems for the Supply Chain. Best Practices for Implementing Supply Chain Security. Assessments and Plans.*
- [6] ISO/PAS 28004:2006, *Security Management Systems for the Supply Chain. Guidelines for the Implementation of ISO/PAS 28000.*

DOCUMENTO DE REFERENCIA

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Specification for Security Management Systems for the Supply Chain.* Geneva, Switzerland, ISO: 28000: 2007(E), p 16.

Sistema de Gestión de la Seguridad de la Información

Contenidos

1. ¿Qué es un SGSI?
2. ¿Para qué sirve un SGSI?
3. ¿Qué incluye un SGSI?
4. ¿Cómo se implementa un SGSI?
5. ¿Qué tareas tiene la Gerencia en un SGSI?
6. ¿Se integra un SGSI con otros sistemas de gestión?

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

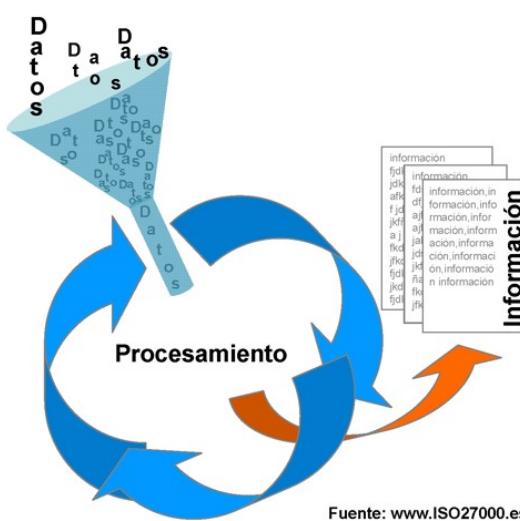
Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En las siguientes secciones, se desarrollarán los conceptos fundamentales de un SGSI según la norma ISO 27001.

1. ¿Qué es un SGSI?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de *Information Security Management System*.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.



La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

2. ¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.



Fuente: www.ISO27000.es

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

4

3. ¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:



Fuente: www.ISO27000.es

Documentos de Nivel 1

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Documentos de Nivel 2

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como *output* que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
- Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables .
- Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de

seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

- Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
- Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- Declaración de aplicabilidad: (SOA -*Statement of Applicability*-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

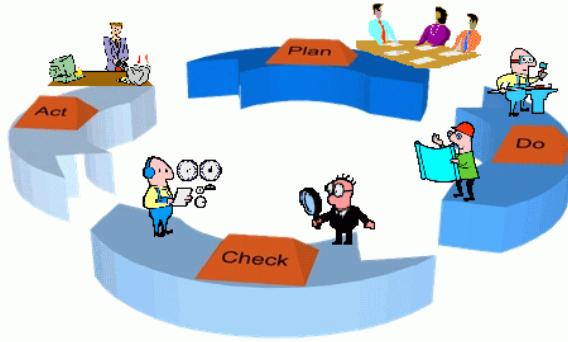
Control de la documentación

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

4. ¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.



- **Plan (planificar):** establecer el SGSI.
- **Do (hacer):** implementar y utilizar el SGSI.
- **Check (verificar):** monitorizar y revisar el SGSI.
- **Act (actuar):** mantener y mejorar el SGSI.

Plan: Establecer el SGSI

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad que:
 - incluya el marco general y los objetivos de seguridad de la información de la organización;
 - considere requerimientos legales o contractuales relativos a la seguridad de la información;
 - esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
 - establezca los criterios con los que se va a evaluar el riesgo;
 - esté aprobada por la dirección.
- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).
- Identificar los riesgos:
 - identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;

- identificar las amenazas en relación a los activos;
 - identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
 - identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- Analizar y evaluar los riesgos:
- evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
 - evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
 - estimar los niveles de riesgo;
 - determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
- aplicar controles adecuados;
 - aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
 - evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;
 - transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de *outsourcing*.



- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.
- Definir una declaración de aplicabilidad que incluya:
 - los objetivos de control y controles seleccionados y los motivos para su elección;
 - los objetivos de control y controles que actualmente ya están implantados;
 - los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO 27001, en su segunda cláusula, en términos de “documento indispensable para la aplicación de este documento” y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares.

Do: Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check: Monitorizar y revisar el SGSI

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
 - detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
 - identificar brechas e incidentes de seguridad;
 - ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
 - detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
 - determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.-.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act: Mantener y mejorar el SGSI

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de *Act* lleva de nuevo a la fase de *Plan* para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

5. ¿Qué tareas tiene la Gerencia en un SGSI?

11

Uno de los componentes primordiales en la implantación exitosa de un Sistema de Gestión de Seguridad de la Información es la implicación de la dirección. No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar un SGSI una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

El término Dirección debe contemplarse siempre desde el punto de vista del alcance del SGSI. Es decir, se refiere al nivel más alto de gerencia de la parte de la organización afectada por el SGSI (recuérdese que el alcance no tiene por qué ser toda la organización).

Algunas de las tareas fundamentales del SGSI que ISO 27001 asigna a la dirección se detallan en los siguientes puntos:

Compromiso de la dirección

La dirección de la organización debe comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. Para ello, debe tomar las siguientes iniciativas:

- Establecer una política de seguridad de la información.

- Asegurarse de que se establecen objetivos y planes del SGSI.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.
- Realizar revisiones del SGSI, como se detalla más adelante.

Asignación de recursos

Para el correcto desarrollo de todas las actividades relacionadas con el SGSI, es imprescindible la asignación de recursos. Es responsabilidad de la dirección garantizar que se asignan los suficientes para:

- Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.
- Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
- Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.
- Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.
- Mejorar la eficacia del SGSI donde sea necesario.

Formación y concienciación

La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la dirección debe asegurar que todo el personal de la organización al que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado. Se deberá:

- Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI.
- Satisfacer dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación de personal ya formado.

- Evaluar la eficacia de las acciones realizadas.
- Mantener registros de estudios, formación, habilidades, experiencia y cualificación.

Además, la dirección debe asegurar que todo el personal relevante esté concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

Revisión del SGSI

A la dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.

Basándose en todas estas informaciones, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:

- Mejora de la eficacia del SGSI.
- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles.

6. ¿Se integra un SGSI con otros sistemas de gestión?

Un SGSI es, en primera instancia, un sistema de gestión, es decir, una herramienta de la que dispone la gerencia para dirigir y controlar un determinado ámbito, en este caso, la seguridad de la información.

La gestión de las actividades de las organizaciones se realiza, cada vez con más frecuencia, según sistemas de gestión basados en estándares internacionales: se gestiona la calidad según ISO 9001, el impacto medio-ambiental según ISO 14001 o la prevención de riesgos laborales según OHSAS 18001. Ahora, se añade ISO 27001 como estándar de gestión de seguridad de la información.

Las empresas tienen la posibilidad de implantar un número variable de estos sistemas de gestión para mejorar la organización y beneficios sin imponer una carga a la organización.

El objetivo último debería ser llegar a un único sistema de gestión que contemple todos los aspectos necesarios para la organización, basándose en el ciclo PDCA de mejora continua común a todos estos estándares. Las facilidades para la integración de las normas ISO son evidentes mediante la consulta de sus anexos.

ISO 27001 detalla en su Anexo C, punto por punto, la correspondencia entre esta norma y la ISO 9001 e ISO 14001. Ahí se observa la alta correlación existente y se puede intuir la posibilidad de integrar el sistema de gestión de seguridad de la información en los sistemas de gestión existentes ya en la organización. Algunos puntos que suponen una novedad en ISO 27001 frente a otros estándares son la evaluación de riesgos y el establecimiento de una declaración de aplicabilidad (SOA), aunque ya se plantea incorporar éstos al resto de normas en un futuro.

En nuestras secciones de [Faqs](#) y de [Artículos](#), podrá encontrar más informaciones acerca de la integración del SGSI con otros sistemas de gestión.