



**VIII Jornada Nacional de
Seguridad Informática**



**CobiT como promotor de la
seguridad de la Información.**

Hacia el Gobierno de TI

Lucio Augusto Molina Focazzio, CISA

IT Governance Committee member

CobiT Accredited Trainer

Certified ITIL



Agenda

Introducción

Que es el IT Governance

CobiT como apoyo al IT Governance

Procesos relacionados con la Seguridad de la Información

Conclusiones



VIII Jornada Nacional de Seguridad Informática



Agenda

Introducción

Que es el IT Governance

CobiT como apoyo al IT Governance

Procesos relacionados con la Seguridad de la Información

Conclusiones

VIII Jornada Nacional de Seguridad Informática





MAYORES DESASTRES





VIII Jornada Nacional de Seguridad Informática



Introducción

Que es el IT Governance

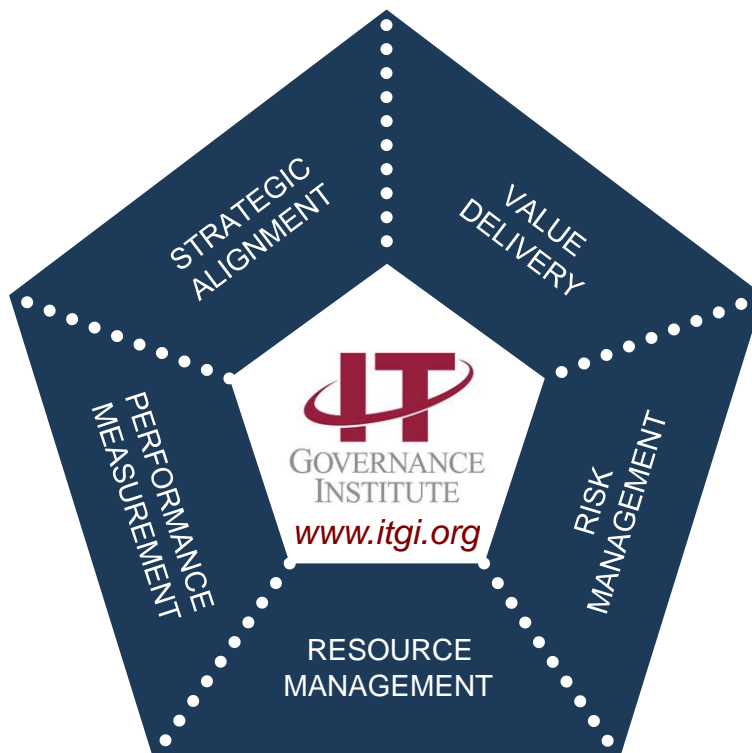
CobiT como apoyo al IT Governance

CobiT y la Seguridad de la Información

Procesos relacionados con la Seguridad de la Información

Conclusiones

La necesidad del Gobierno de TI



El Gobierno Corporativo es un conjunto de responsabilidades y prácticas ejecutadas por la Junta y los Directivos con el objeto de:

- Prover Direccionamiento estratégico
- Asegurar el cumplimiento de los objetivos
- Garantizar que los riesgos son manejados apropiadamente
- Verificar que los recursos de la empresa se utilizan responsablemente

El Gobierno de TI es:

- Responsabilidad del Board de Directores y de los directivos
- Parte integral del Gobierno Corporativo, que consiste en el liderazgo, estructuras organizacionales y procesos que aseguran que el TI de la empresa soportará y complementará las estrategias y objetivos de la empresa



VIII Jornada Nacional de Seguridad Informática



La necesidad del Gobierno de TI



Alinearse con el negocio y proveer soluciones colaborativas

Ejecutar la propuesta de valor a través del ciclo de entrega

Proteger los activos, recuperarse de los desastres y cumplir las leyes, regulaciones y contratos

Optimizar el desarrollo y uso de los recursos disponibles

Monitoriar los resultados para aplicar acciones correctivas

Agenda

Introducción

Que es el IT Governance

CobIT como apoyo al IT Governance

Procesos relacionados con la Seguridad de la Información

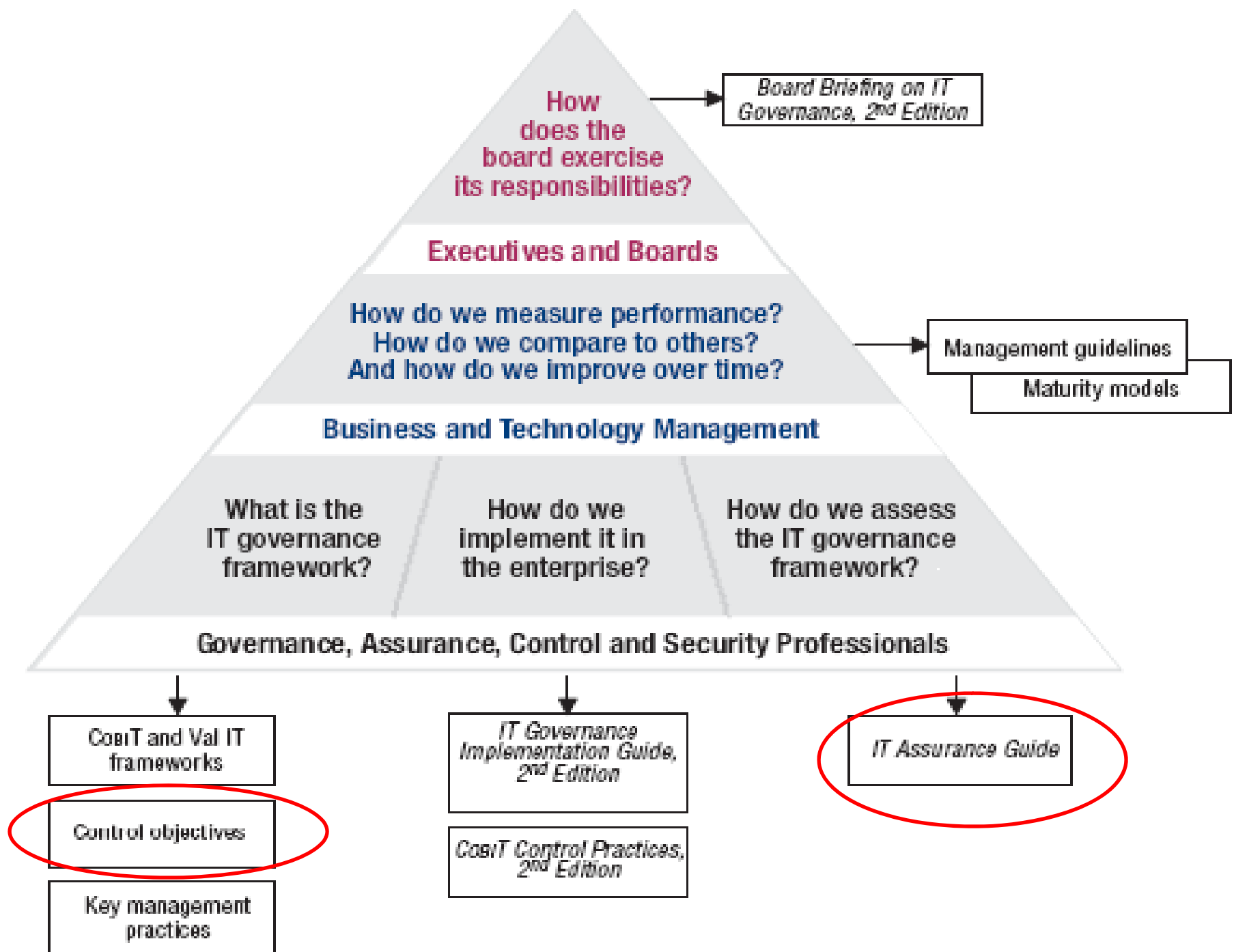
Conclusiones

C **Control**

OB **OB**jectives

I **for I**nformation

T **and Related T**echnology







VIII Jornada Nacional de
Seguridad Informática

Domínios



Planear y organizar - *Plan and organize* - PO

Adquirir e implementar - *Acquire and implement* - AI

Entregar y Soportar - *Deliver and support* - DS

Monitorear y Evaluar – *Monitor and Evaluate* - ME



VIII Jornada Nacional de Seguridad Informática



Introducción

Que es el IT Governance

CobiT como apoyo al IT Governance

CobiT y la Seguridad de la Información

Procesos relacionados con la Seguridad de la Información

Conclusiones

The banner features a dark blue background with a perspective view of a hallway lined with server racks. The racks are illuminated from within, creating a bright glow at the end of the hallway. The text "VIII Jornada Nacional de Seguridad Informática" is written in a bold, yellow, sans-serif font across the top right of the banner.

VIII Jornada Nacional de
Seguridad Informática



Planear y Organizar PO

**PROCESOS RELACIONADOS CON LA
SEGURIDAD DE LA INFORMACION**

VIII Jornada Nacional de Seguridad Informática



Planear y Organizar PO

- PO1 Definir un Plan Estratégico de Tecnología de Información
- PO2 Definir la Arquitectura de Información
- PO3 Determinar la dirección tecnológica
- PO4 Definir los procesos de TI, su Organización y las Relaciones de TI
- PO5 Manejar la Inversión en TI
- PO6 Comunicar la dirección y aspiraciones de la gerencia
- PO7 Administrar Recursos Humanos
- PO8 Administrar con Calidad
- PO9 Evaluar y administrar los Riesgos
- PO10 Administrar proyectos

PO1. Definir un Plan Estrategico de TI

- Impacto del negocio sobre los riesgos de TI

PO2. Definir la Arquitectura de la Informacion

- Establecer los dueños de la Informacion
- Clasificar la informacion con base en:
 - La Sensibilidad → Confidencialidad
 - La Criticidad → Disponibilidad
- Administrar la Integridad de la Informacion
- Identificar DUEÑOS

PO4. Definir los procesos de TI, su organización y sus relaciones

- Responsabilidad por
 - Los riesgos
 - La seguridad
 - El cumplimiento



PO9. Analizar y administrar los riesgos

- Realizar análisis de riesgos
- Identificar eventos (vulnerabilidades y amenazas)
- Analizar los riesgos
- Responder al riesgo
 - Mitigar
 - Evitar
 - Compartir
 - Aceptar
- Mantener y monitorear los planes de acción para mitigar los riesgos

The banner features a dark blue background with a perspective view of a hallway lined with server racks. A bright light source at the end of the hallway creates a lens flare effect. The text "VIII Jornada Nacional de Seguridad Informática" is written in a bold, yellow, sans-serif font.

VIII Jornada Nacional de
Seguridad Informática



Adquirir e Implementar AI

**PROCESOS RELACIONADOS CON LA
SEGURIDAD DE LA INFORMACION**



VIII Jornada Nacional de Seguridad Informática



Adquirir e Implementar - AI

AI1 Identificar Soluciones

AI2 Adquirir y Mantener Software de Aplicación

AI3 Adquirir y Mantener la Infraestructura de Tecnología

AI4 Facilitar la operación y el uso

AI5 Proveer recursos de TI

AI6 Administrar cambios

AI7 Instalar y acreditar soluciones y cambios

AI2 Adquirir y Mantener Software de Aplicación

- **Control y Auditabilidad de las Aplicaciones**

- Controles

- Procesamiento completo
 - Oportuno
 - Autorizado
 - Auditable
- Seguridad y Disponibilidad de las Aplicaciones

AI3 Adquirir y Mantener la Infraestructura Tecnológica

- **Protección y disponibilidad de los recursos de la infraestructura**
 - Controles
 - Seguridad
 - Auditabilidad
- **Mantenimiento de la Infraestructura**
 - Cambios autorizados
 - Análisis de vulnerabilidades

AI4 Facilitar la operación y el uso

- Transferir el conocimiento a:
 - Los directivos
 - Los usuarios
 - Los operadores y personal de soporte

AI5. Proveer los recursos de TI

- Acuerdos de confidencialidad
- Responsabilidad sobre la seguridad y la propiedad intelectual

AI6 Administrar los Cambios

- Procedimientos para los cambios
- Analisis de impacto, priorizacion y autorizacion
- Cambios de emergencia

AI7. Instalar y acreditar soluciones y cambios

- Plan de pruebas
- Ambiente de pruebas
- Conversion de datos y sistemas
- Pruebas a los cambios
- Promocion a produccion

The banner features a dark blue background with a perspective view of a hallway lined with server racks. A bright light emanates from an opening at the end of the hallway. The text "VIII Jornada Nacional de Seguridad Informática" is written in a bold, yellow, sans-serif font.

VIII Jornada Nacional de
Seguridad Informática



Entregar y Soportar - DS

**PROCESOS RELACIONADOS CON LA
SEGURIDAD DE LA INFORMACION**



VIII Jornada Nacional de Seguridad Informática



Entregar y Soportar - DS

- DS1 Definir y administrar Niveles de Servicio
- DS2 Administrar Servicios prestados por Terceros
- DS3 Administrar Desempeño y Capacidad
- DS4 Asegurar un Servicio Continuo
- DS5 Garantizar la Seguridad de Sistemas
- DS6 Identificar y Asignar Costos
- DS7 Educar y Entrenar a Usuarios

DS8 Administrar la Mesa de Servicio y los Incidentes

DS9 Administrar la Configuración

DS10 Administrar los problemas

DS11 Administrar los datos

DS12 Administrar el ambiente físico

DS13 Administrar las Operaciones

DS1. Definir y Administrar Niveles de Servicios

- Acuerdos de nivel de servicio
 - Disponibilidad
 - Seguridad
 - Confiabilidad

DS2. Administrar servicios prestados por terceros

- Administrar los riesgos de los proveedores

DS3. Administrar el desempeño y la capacidad

- Disponibilidad de los recursos de TI
 - Contingencias
 - Almacenamiento
 - Sobrecarga de trabajo

DS4. Asegurar el servicio continuo

- Plan de Continuidad de TI
- Recursos críticos de TI
- Almacenamiento externo
- Prueba al plan de Continuidad
- Recuperación y reinicio de las operaciones

DS5. Garantizar la Seguridad de los Sistemas

- Gestion de la seguridad de TI
- Plan de seguridad de TI
- Administracion de Identidad
- Administracion de usuarios
- Prueba y monitoreo a la seguridad
- Definicion de incidentes de seguridad
- Proteccion de las tecnologias de seguridad
- Seguridad en la red
- Intercambio de datos sensitivos

DS8. Administrar la Mesa de Servicio y los Incidentes

- Mesa de Servicio
- Escalamiento de incidentes
- Cierre de los incidentes

DS9. Administrar la configuración

- Identificar y mantener los elementos de la configuración

DS10. Administrar Problemas

- Identificar y Clasificar los Problemas
- Seguimiento y solución de los problemas
- Integración de la administración de incidentes, configuración y problemas

DS11. Administrar los Datos

- Acuerdos de retención y almacenamiento
- Sistema de administración de medios
- Desechar datos
- Backup y recuperación
- Requerimientos de seguridad para la administración de datos

DS12. Administrar el Ambiente Fisico

- Planos y selección del sitio
- Medidas de seguridad fisica
- Acceso fisico
- Proteccion contra factores ambientales

DS13. Administrar las Operaciones

- Monitoreo de la Infraestructura de TI
- Documentos sensitivos y dispositivos de salida
- Mantenimiento preventivo

The banner features a dark blue background with a perspective view of a hallway lined with server racks. The racks are illuminated from within, creating a bright glow at the end of the hallway. The text "VIII Jornada Nacional de Seguridad Informática" is written in a bold, yellow, sans-serif font across the top right of the banner.

VIII Jornada Nacional de
Seguridad Informática



Monitorear y Evaluar - ME

**PROCESOS RELACIONADOS CON LA
SEGURIDAD DE LA INFORMACION**

ME1 Monitorear y Evaluar el desempeño de TI

ME2 Monitorear y Evaluar el Control Interno

ME3 Asegurar el cumplimiento con
requerimientos externos

ME4 Proporcionar Gobierno de TI



VIII Jornada Nacional de Seguridad Informática

Agenda



Introducción

Que es el IT Governance

CobiT como apoyo al IT Governance

CobiT y la Seguridad de la Información

Procesos relacionados con la Seguridad de la Información

Conclusiones



VIII Jornada Nacional de
Seguridad Informática

Conclusiones

ACIS

- El Gobierno de TI es responsabilidad de todos
- CobiT es un marco de referencia contra el cual se puede comparar los controles de TI con el fin de mejorarlos
- CobiT ofrece un marco de trabajo para incrementar y fortalecer la seguridad de la información en la Organización

I will not shut down major e-commerce sites
I will not shut down major e-commerce sites
I will not shut down major e-commerce sites
I will not shut down major e-commerce sites
I will not shut down major e-commerce sites
I will not shut down major e-commerce sites



© 2000 The Halifax Herald Limited



VIII Jornada Nacional de
Seguridad Informática



Gracias

Lucio Augusto Molina Focazzio

Certified Information Systems Auditor

Certified ITIL Essentials

IT Governance Committee Member

CobIT Accredited Trainer

Consultor Independiente

lucio_molina@etb.net.co

