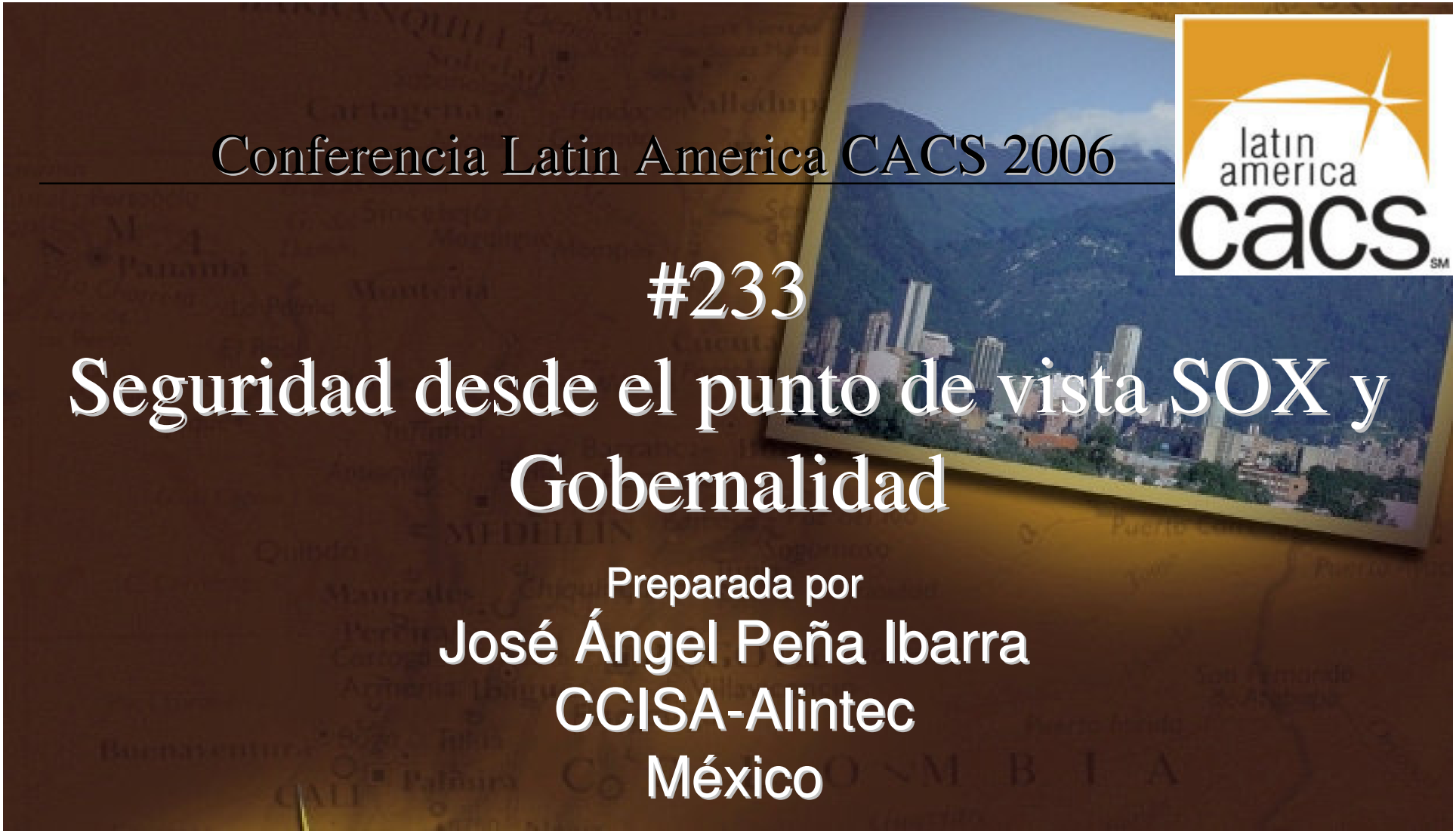


Conferencia Latin America CACS 2006

# #233
# Seguridad desde el punto de vista SOX y Gobernalidad


Preparada por

José Ángel Peña Ibarra

CCISA-Alintec

México


ISACA®
Serving IT Governance Professionals

Consultoría en Comunicaciones e Informática, S.A. de C.V. (CCISA), Firma miembro de

Alintec
IT Governance Consultants
www.alintec.net

# Agenda

1. Sarbanes Oxley
2. Gobierno Corporativo y de TI.
3. Implicaciones de Seguridad en SOX.
4. Utilización de Cobit e ISO 17799 para cumplimiento.
5. Objetivos de control de seguridad para cumplimiento

# 1. Sarbanes Oxley

# Sarbanes Oxley

- El acta Sarbanes Oxley, SOX, fue emitida en el año 2002, para evitar fraudes de cuello blanco, como los ocurridos en Enron y otras empresas..

- SOX requiere:
  - Certificación de la administración acerca del control interno de la compañía.
  - Reporte de controles internos en información financiera.

- El acta incluye varias secciones, las cuales tienen finalidades específicas.

# Secciones de Sarbanes Oxley

***Algunas secciones clave:***

- Sección 302.- Directivos de la compañía deben hacer representaciones relacionadas con el "disclosure" de controles, procedimientos y aseguramiento contra fraude.

- Sección 404.- Directivos deben proveer una evaluación anual de la efectividad de los controles internos para el reporte de información financiera y obtener una certificación "attestation" de los auditores externos respecto a que los controles son efectivos.

# Marco de control para SOX

- Sarbanes Oxley requiere que las compañías adopten un marco de control.
- COSO define un marco de control que ha sido grandemente aceptado para cumplir con Sarbanes Oxley.
- COSO = Comitee of Sponsoring Organizations de la Treadway Commission.

# Marco COSO

- Componentes de control interno.
  - Efectividad de operaciones
  - Confianza de los reportes financieros
  - Cumplimiento con regulaciones aplicables.

- Componentes del marco de control.
  - **Evaluación de Riesgos** – económicos, operacionales..
  - **Ambiente de control** – disciplina y estructura
  - **Actividades de control** – Aprobación, separación de funciones..
  - **Información y comunicación**
  - **Monitoreo**

# Marco COSO

- Sarbanes Oxley establece penas corporales para los directivos que no cumplan.

- Aunque muchas empresas no están obligadas a cumplir con Sarbanes Oxley, hay una tendencia a establecer leyes similares en varios países fuera de los Estados Unidos.

# Agenda

1. Sarbanes Oxley
2. **Gobierno Corporativo y de TI.**
3. Implicaciones de Seguridad en SOX.
4. Utilización de Cobit e ISO 17799 para cumplimiento.
5. Objetivos de control de seguridad para cumplimiento

# Gobierno Corporativo

- De acuerdo a la **Organización para la Cooperación y el Desarrollo Económico, OCDE**, no existe un modelo único de buen gobierno corporativo
- Pero si existen elementos comunes con los cuáles se pueden establecer los principios que deben servir como guía para un buen gobierno corporativo.

# Principios de Gobierno Corporativo

- La OCDE estableció una serie de principios con el objetivo de ayudar a los Gobiernos de los países miembros y no-miembros de la OCDE, en la tarea de evaluar y perfeccionar el gobierno corporativo en sus respectivos países.

- Asimismo ofrecer orientación y sugerencias a las Bolsas de valores, los inversores, las sociedades y demás partes que intervienen en el proceso de desarrollo de un modelo de buen gobierno corporativo.

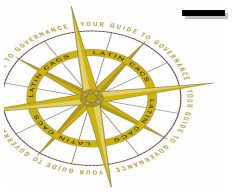
# Principios de Gobierno Corporativo

- Los Principios centran su atención sobre las sociedades con cotización oficial, tanto financieras como no financieras.

- No obstante, y en la medida en que resulten aplicables, **pueden constituir también un instrumento muy útil para mejorar el gobierno corporativo en sociedades sin cotización oficial**, tales como las empresas de propiedad privada y las empresas propiedad del Estado.

# Principios de Gobierno Corporativo

- Los Principios de la OCDE incluyen entre otros, los siguientes aspectos:
  - **Derechos de los accionistas y funciones clave en el ámbito de la propiedad.**
  - Tratamiento equitativo de los accionistas.
  - Rol de las partes interesadas en el Gobierno Corporativo.
  - **Divulgación de datos y transparencia**
  - Responsabilidades del Consejo



• **El Gobierno Corporativo** busca la **transparencia**, objetividad y equidad en el trato de los socios y accionistas de una sociedad, la gestión de su junta directiva, y la responsabilidad frente a terceros que aportan recursos.

• Responde a la voluntad autónoma de la persona jurídica, de establecer estos principios para ser mas **competitiva** y dar garantías a todos los grupos de interés

# Objetivo del Gobierno Corporativo

- El objetivo del Gobierno Corporativo no debe ser intervenir en la autonomía de las empresas, sino el **coadyuvar al logro de los objetivos de productividad, competitividad y permanencia** de la misma, a través de la transparencia y manejo responsable.

# Convergencia con Gobierno corporativo

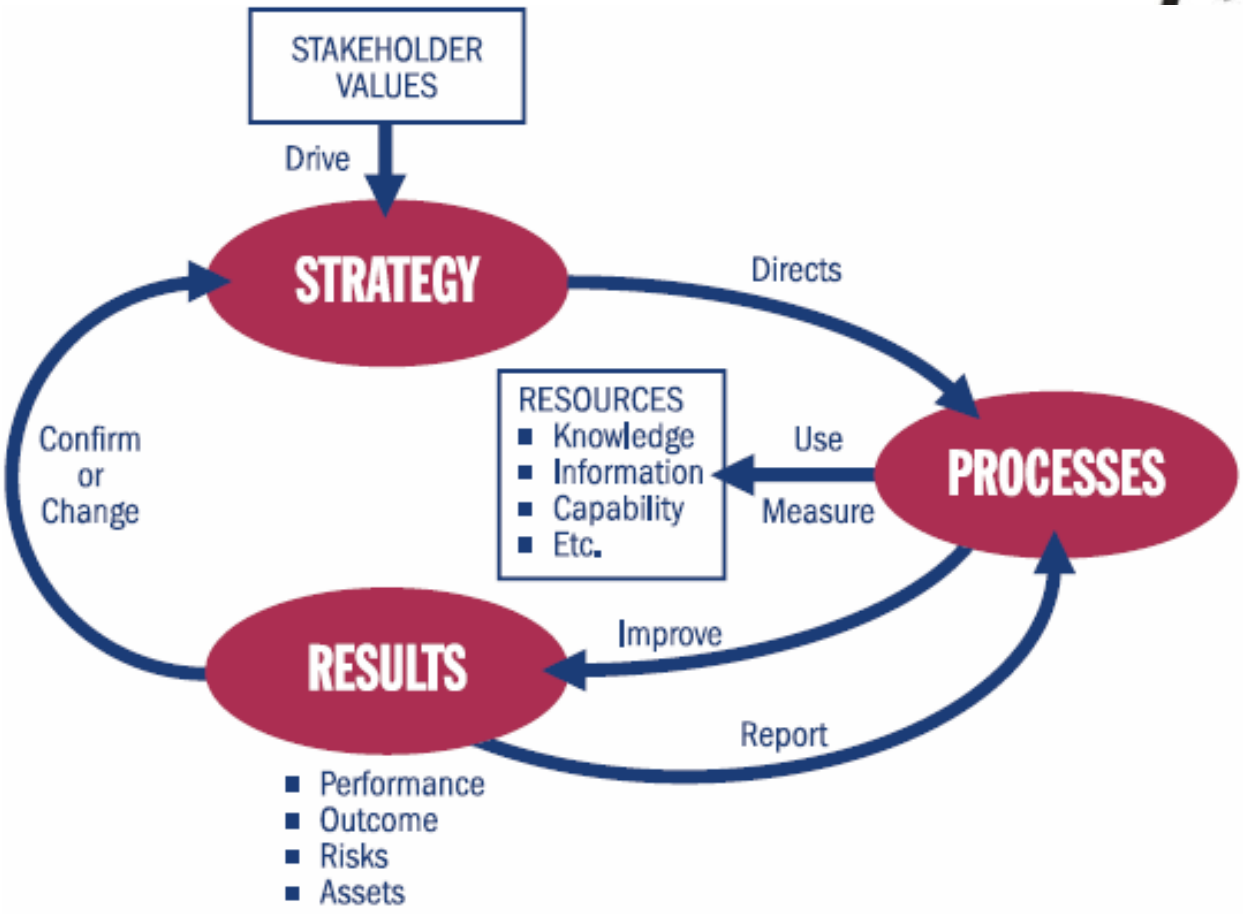
- Inicialmente, SOX es responsabilidad del CEO y el CFO, sin embargo, ellos deben enfocarse en la creación de valor.

- Por eso muchas firmas harán énfasis en el gobierno corporativo para cumplir con SOX y **así mismo** con sus objetivos de negocio.

- El modelo de gobierno corporativo se enfocará en:
  - Administración de riesgo.
  - Cumplimiento de regulaciones
  - Administración de resultados (performance mgmt.)

# Gobierno de TI en el Gobierno Corporativo

- Gobierno de TI no es una disciplina separada. Es un componente del Gobierno Corporativo, con responsabilidades como:
  - Tomar en cuenta a los accionistas al definir las estrategias.
  - Dar dirección a los procesos cuando se implementan las estrategias.
  - Asegurar que los procesos den resultados que puedan ser medidos.
  - Informar acerca de los resultados.

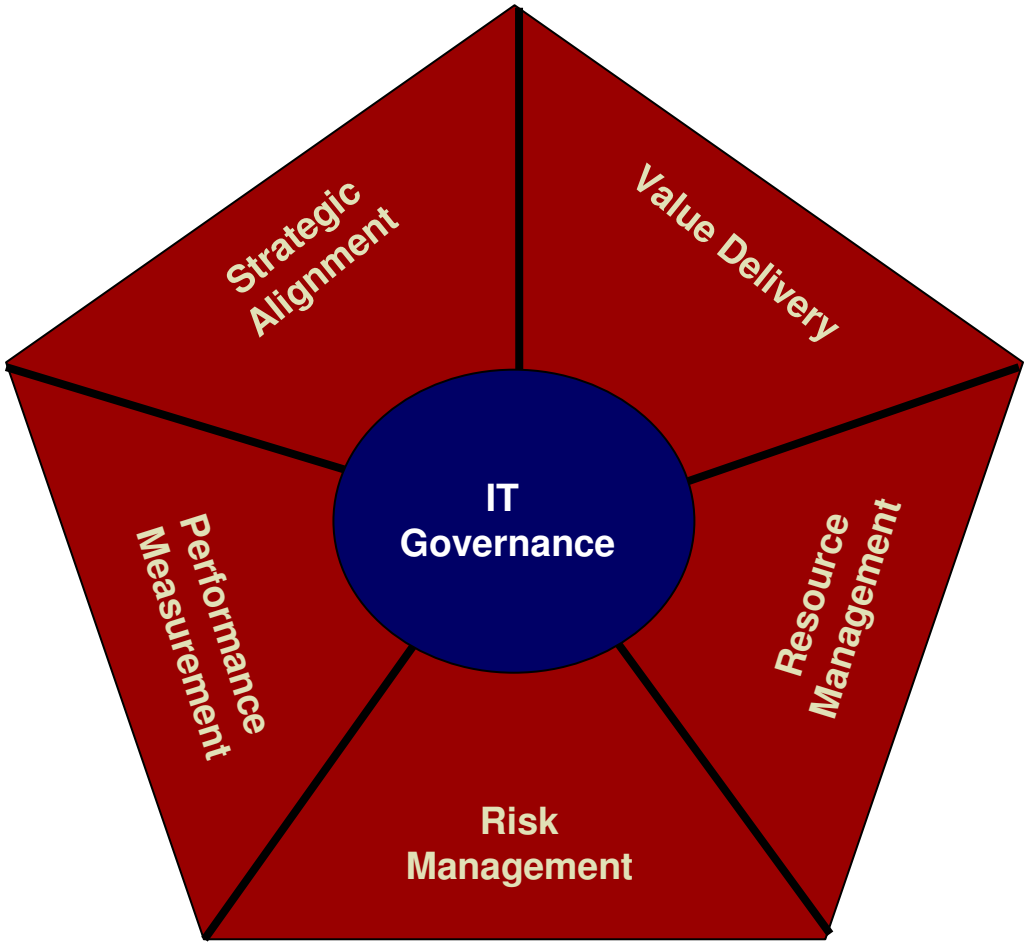

STAKEHOLDER VALUES
Drive
STRATEGY
Directs
RESOURCES
Knowledge
Information
Capability
Etc.
Use
Measure
PROCESSES
Confirm or Change
Improve
RESULTS
Report
Performance
Outcome
Risks
Assets

# Gobierno de TI

- Gobierno de TI aplica los principios de gobierno corporativo para dirigir y controlar la función y aplicaciones de tecnologías de información.

- Hace énfasis en:
  - El potencial de TI para apoyar los objetivos de negocio.
  - El alineamiento de las estrategias de TI con las estrategias de negocio.
  - La revisión y aprobación de las inversiones de TI.
  - El manejo de los riesgos asociados con TI.
  - La medición de resultados de TI.

# The IT Governance Solution



# Gobierno de TI

- Gobierno de TI es fundamental para el cumplimiento de SOX.

- El Gobierno de TI asegura que las políticas y practicas consideren:
  - Integridad de la información
  - Riesgos de negocio
  - Criticidad de los sistemas y datos para soportar los objetivos de la compañía.
  - Cumplimiento de las regulaciones correspondientes.

# Agenda

1. Sarbanes Oxley
2. Gobierno Corporativo y de TI.
3. **Implicaciones de Seguridad en SOX.**
4. Utilización de Cobit e ISO 17799 para cumplimiento.
5. Objetivos de control de seguridad para cumplimiento

# Implicaciones de seguridad en SOX

- SOX no menciona explícitamente seguridad, pero tiene claras implicaciones en esta área.
- De hecho, SOX ha hecho que la seguridad de la información llegue al nivel de Presidencia y de Consejo de Administración.
- El acta exige mejor **integridad de los datos**, lo que implica que se deben reforzar las practicas de seguridad.

# Implicaciones de seguridad en SOX

- SOX demanda un reforzamiento de las practicas de control interno, incluyendo aquellas relacionadas con **control de accesos**, que invariablemente están asociadas a la seguridad.

- La jerarquía de controles recomendada para cumplir con SOX implícita y explícitamente requiere **confidencialidad** y **disponibilidad**

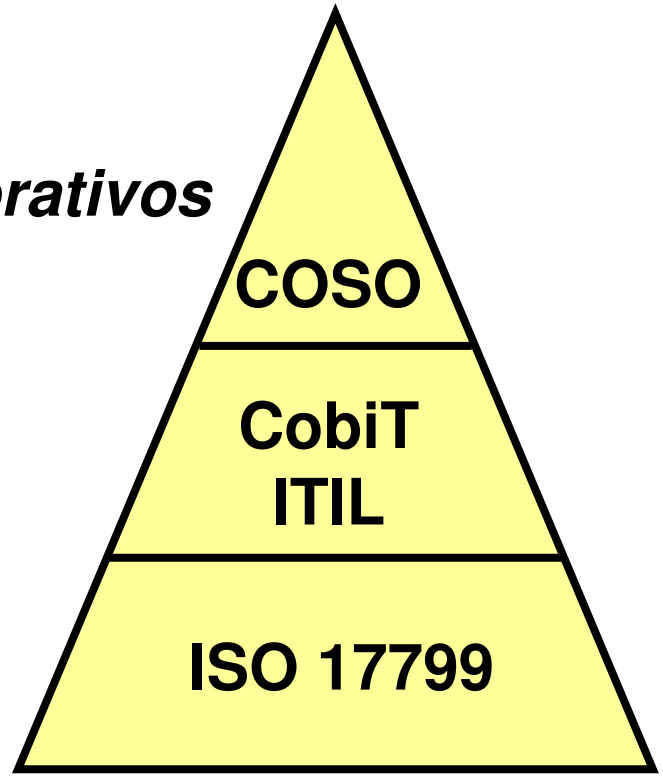
# Jerarquía de control

**Los controles corporativos deben estar soportados por controles de seguridad:**

***Controles Corporativos***

***Controles de TI***

***Controles de seguridad***

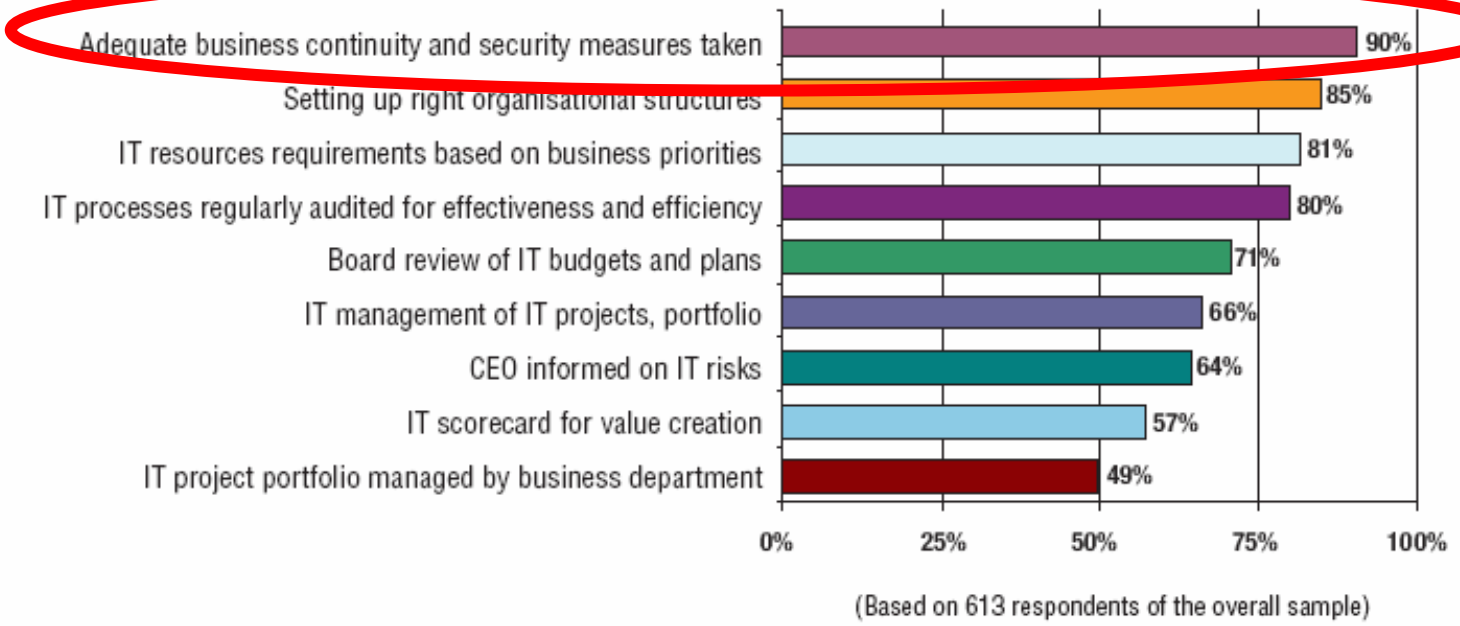


- Seguridad de la información provee los procesos y tecnología necesarios para asegurar que las transacciones de negocios son confiables, que los servicios de TI son utilizables y que pueden resistir o recuperarse de fallas debidas a errores, ataques deliberados o desastres.

- Seguridad de la información protege información crítica de aquellos que no deben tener acceso a ella.

*2.3.4 Which of the following statements do you believe to be good IT governance practices?*

**Figure 22—IT Governance Practices**




Fuente: IT Governance Global Status Report – 2006.

# Agenda

1. Sarbanes Oxley
2. Gobierno Corporativo y de TI.
3. Implicaciones de Seguridad en SOX.
4. **Utilización de Cobit e ISO 17799 para cumplimiento.**
5. Objetivos de control de seguridad para cumplimiento

# CobiT

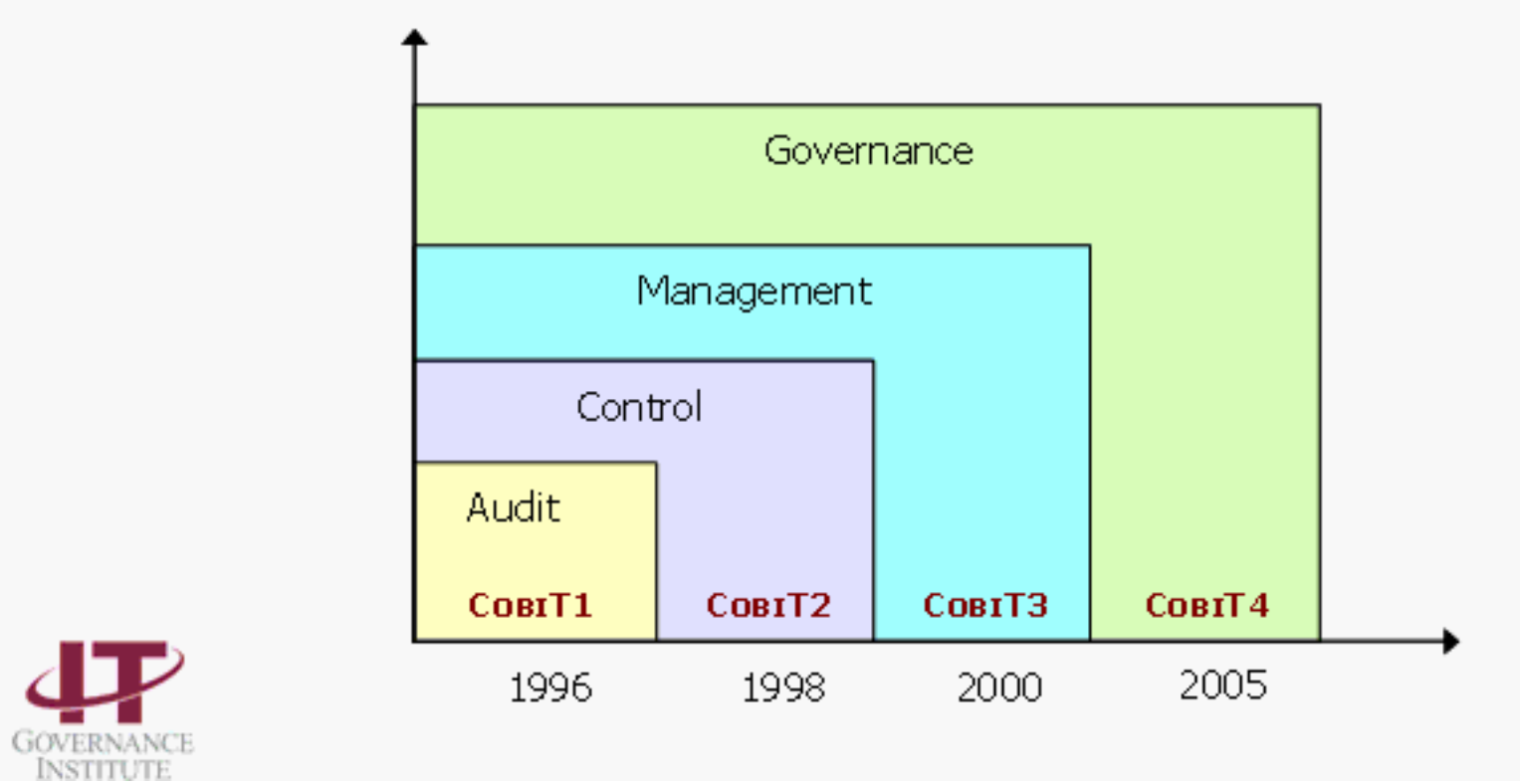
- Control Objectives for Information and related Technology, **CobiT**, fue desarrollado por la Information Systems Audit and Control Association, **ISACA**, con el propósito de contar con un **conjunto de mejores prácticas en el campo de control interno en TI.**



Serving IT Governance Professionals

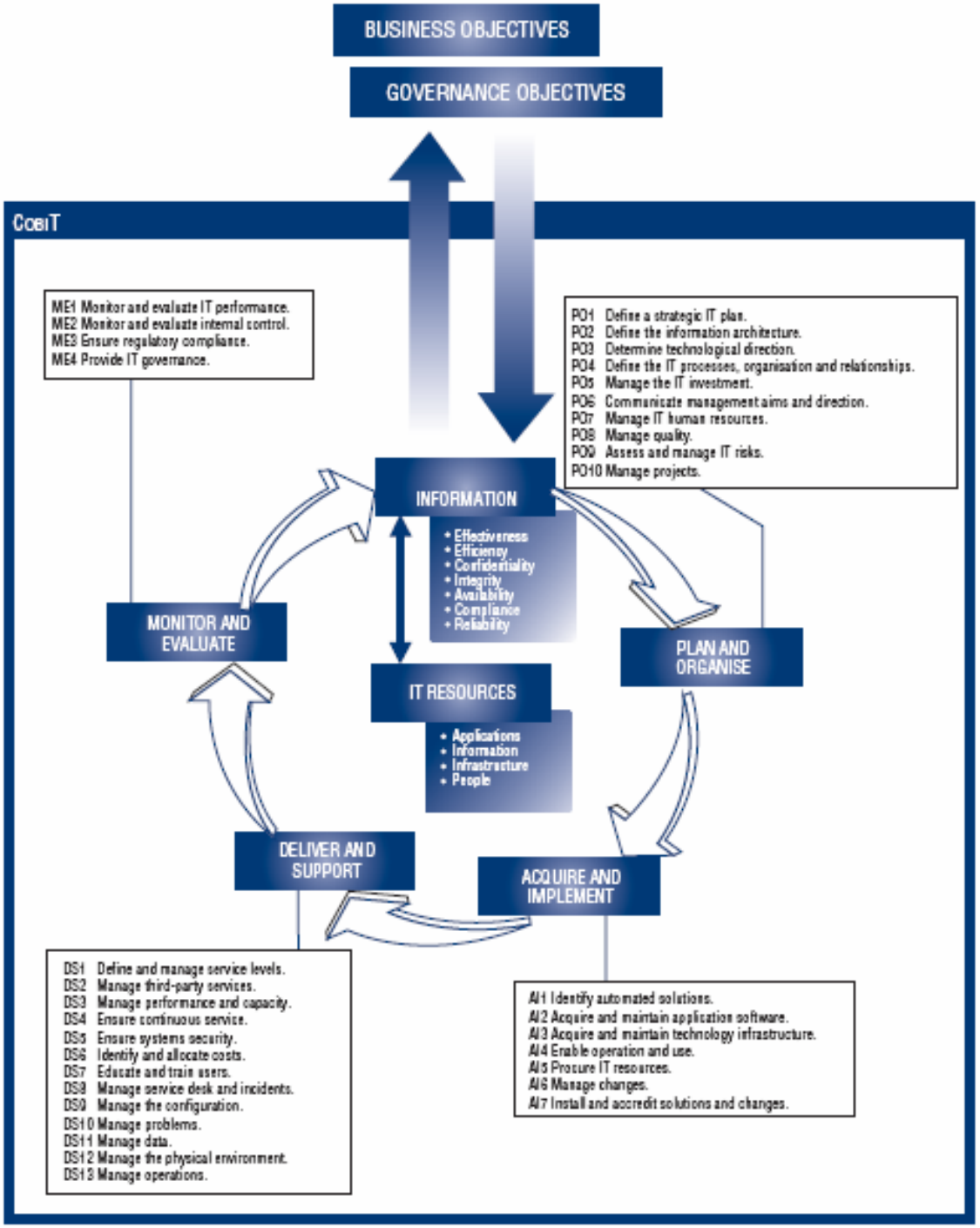
# CobiT

***CobiT ha evolucionado de ser una herramienta de auditoría a ser un marco de referencia de gobierno de TI.***



# Enfoque de CobiT 4.0

- **En gobierno de TI.**
- **Armonización con otros estándares.**
- **Flujo de procesos.**
- **Lenguaje más conciso y orientado a la acción.**

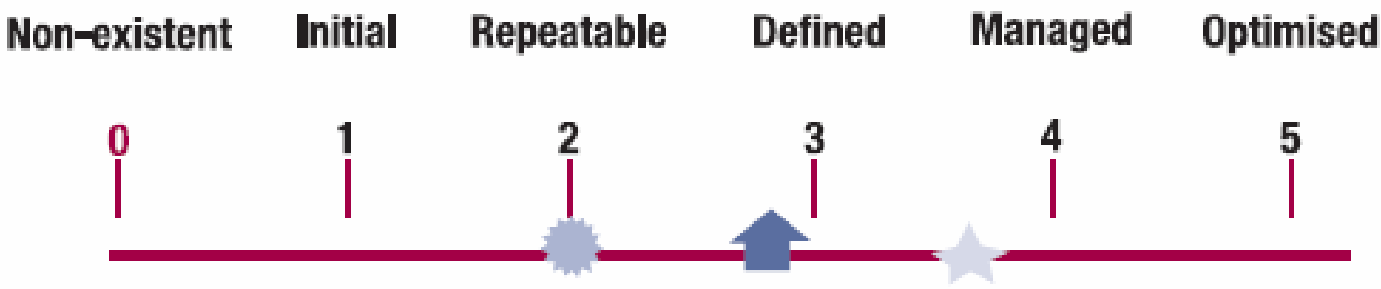




latin america cacs SM

- **4 dominios**
- **34 procesos**

ISACA®
Serving IT Governance Professionals

# Modelo de madurez




**LEGEND FOR SYMBOLS USED**

- Enterprise current status
- Industry average
- Enterprise target

**LEGEND FOR RANKINGS USED**

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

# Modelo de madurez genérico

**0 Non-existent.** Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.

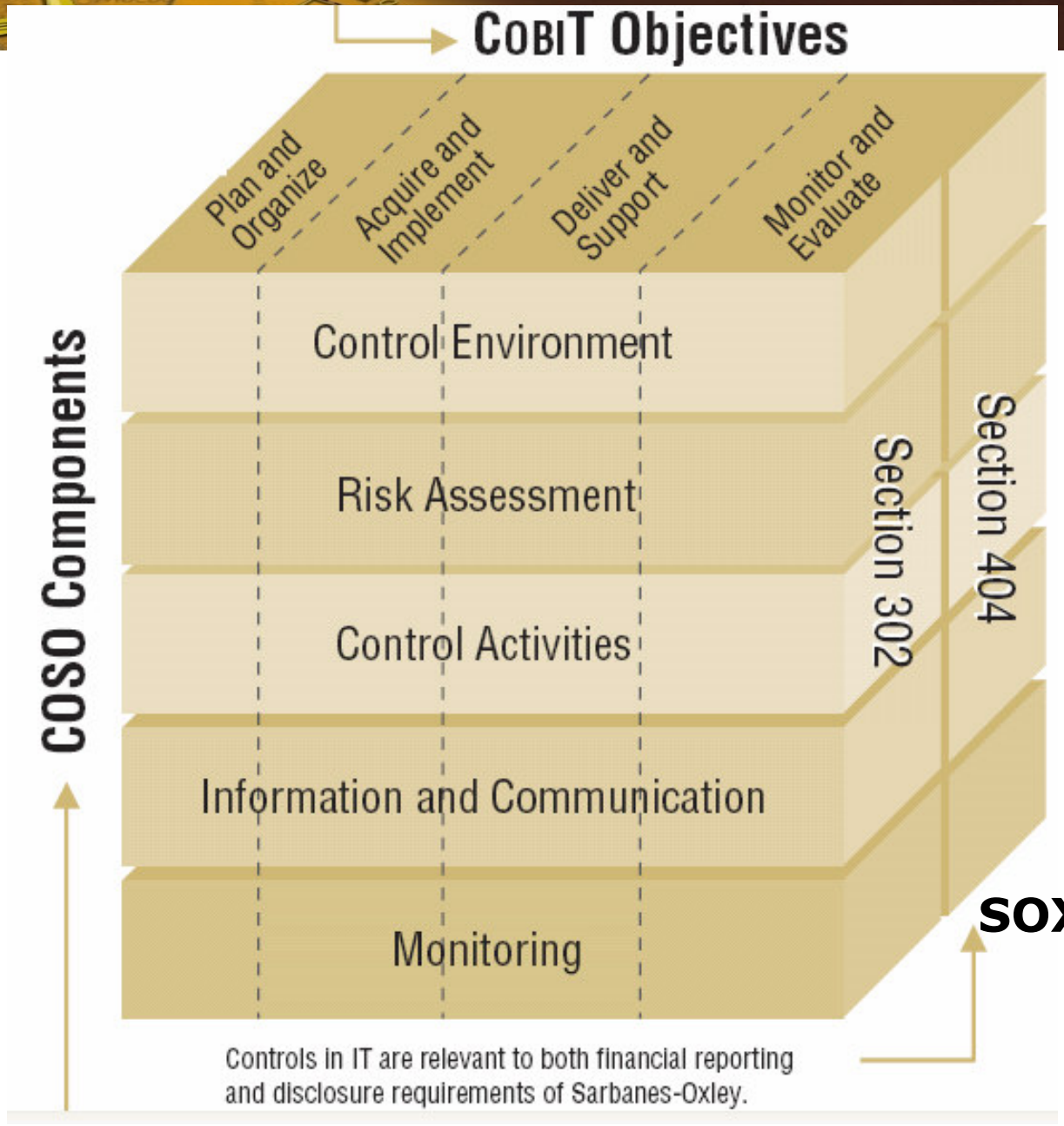
**1 Initial.** There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.

**2 Repeatable.** Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

**3 Defined**. Procedures have been standardised and documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

**4 Managed.** It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

**5 Optimised.** Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.


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

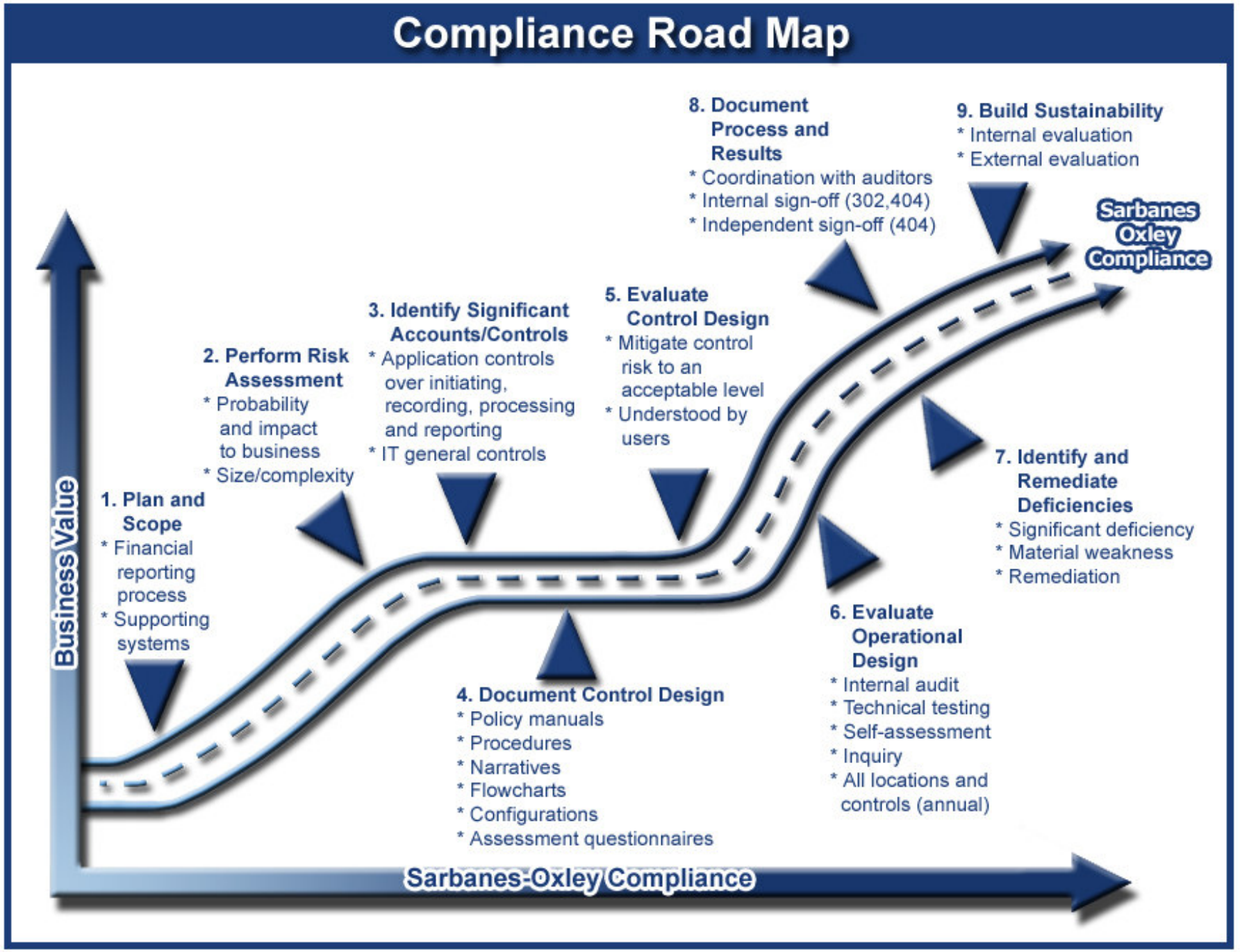
# ISO 17799

- El conjunto de recomendaciones **ISO 17799**, fue desarrollado por la ISO, con el propósito de contar con un conjunto de mejores prácticas en el campo de seguridad de la información.
- El **ISO 17799** incluye 10 dominios.

# Marco Metodológico ISO 17799

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

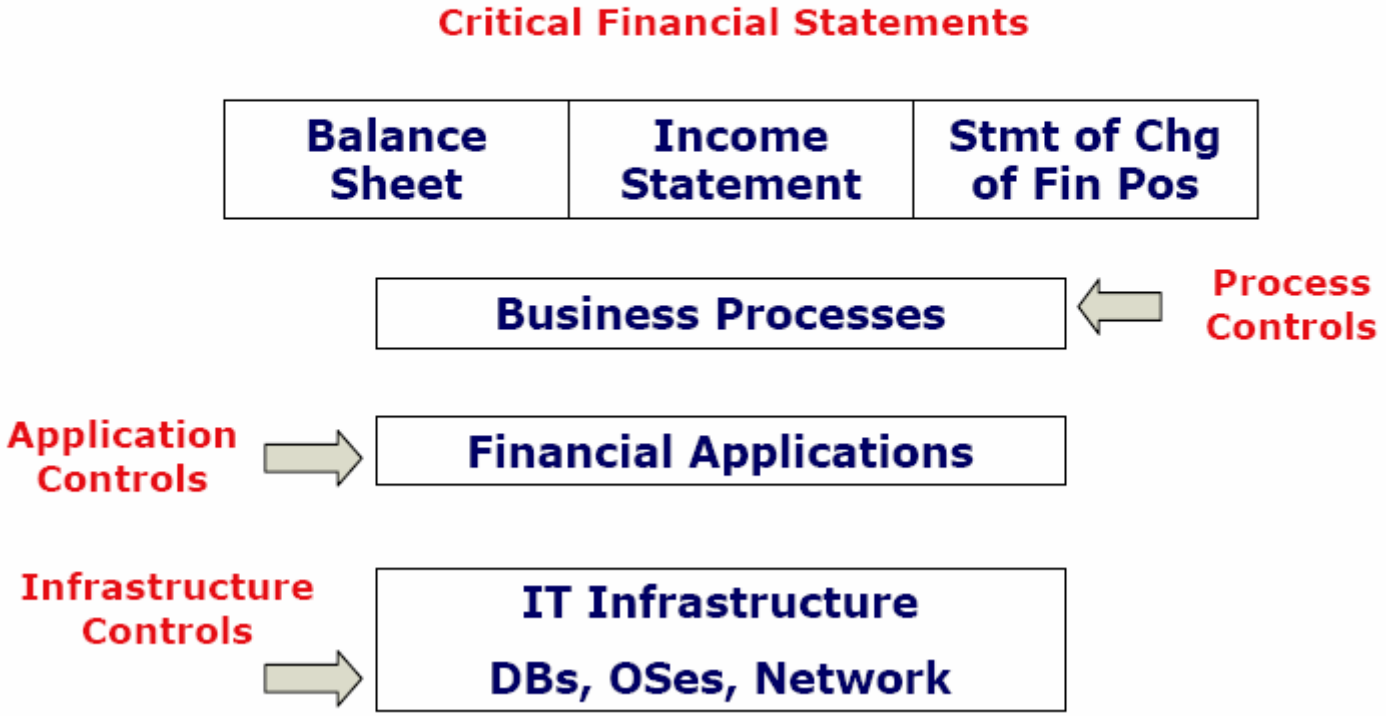
**Modelo ISO 17799**


Compliance Road Map
8. Document Process and Results
* Coordination with auditors
* Internal sign-off (302,404)
* Independent sign-off (404)
9. Build Sustainability
* Internal evaluation
* External evaluation
Sarbanes Oxley Compliance
5. Evaluate Control Design
* Mitigate control risk to an acceptable level
* Understood by users
3. Identify Significant Accounts/Controls
* Application controls over initiating, recording, processing and reporting
* IT general controls
2. Perform Risk Assessment
* Probability and impact to business
* Size/complexity
1. Plan and Scope
* Financial reporting process
* Supporting systems
Business Value
7. Identify and Remediate Deficiencies
* Significant deficiency
* Material weakness
* Remediation
6. Evaluate Operational Design
* Internal audit
* Technical testing
* Self-assessment
* Inquiry
* All locations and controls (annual)
4. Document Control Design
* Policy manuals
* Procedures
* Narratives
* Flowcharts
* Configurations
* Assessment questionnaires
Sarbanes-Oxley Compliance

# Agenda

1. Sarbanes Oxley
2. Gobierno Corporativo y de TI.
3. Implicaciones de Seguridad en SOX.
4. Utilización de Cobit e ISO 17799 para cumplimiento.
5. **Objetivos de control de seguridad para cumplimiento**

# SOX scope drivers and controls






Fuente: System Experts

# Funciones Críticas de TI para seguridad

- Administración de identidad y privilegios.
- Control de cambios.
  - Aplicaciones.
  - Cuentas.
  - Equipo de cómputo y comunicaciones.
  - Documentación.
- Registro.
  - Uso.
  - Fallas.
  - Accesos.
- Monitoreo.


latin america cacs℠

## Control Processes

| CobiT Control Objective Heading | PCAOB IT General Control Heading: Program Development | Program Changes | Computer Operations | Access to Programs and Data |
|---|---|---|---|---|
| 1. Acquire or develop application software (AI2) | ● | ● | ● | ● |
| 2. Acquire technology infrastructure (AI3) | ● | ● | ● | |
| 3. Develop and maintain policies and procedures (AI4) | ● | ● | ● | ● |
| 4. Install and test application software and technology infrastructure (AI5) | ● | ● | ● | ● |
| 5. Manage changes (AI6) | | ● | | ● |
| 6. Define and manage service levels (DS1) | ● | ● | ● | ● |
| 7. Manage third-party services (DS2) | ● | ● | ● | ● |
| 8. Ensure systems security (DS5) | | | ● | ● |
| 9. Manage the configuration (DS9) | | | ● | ● |
| 10. Manage problems and incidents (DS10) | | | ● | |
| 11. Manage data (DS11) | | | ● | ● |
| 12. Manage operations (DS13) | | | ● | ● |

ISACA®
Serving IT Governance Professionals

## Figure 20—Ensure Systems Security

| Control Guidance | |
|---|---|
| **Control Objective—Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.** | |
| **Rationale**—Managing systems security includes both physical and logical controls that prevent unauthorized access. These controls typically support authorization, authentication, nonrepudiation, data classification and security monitoring. Deficiencies in this area could significantly impact financial reporting. For instance, insufficient controls over transaction authorization may result in inaccurate financial reporting. | |
| **Illustrative Controls** | **Illustrative Tests of Controls** |
| An information security policy exists and has been approved by an appropriate level of executive management.  | Obtain a copy of the organization's security policy and evaluate the effectiveness. Points to be taken into consideration include:<br>• Is there an overall statement of the importance of security to the organization?<br>• Have specific policy objectives been defined?<br>• Have employee and contractor security responsibilities been addressed?<br>• Has the policy been approved by an appropriate level of senior management to demonstrate management's commitment to security?<br>• Is there a process to communicate the policy to all levels of management and employees? |

Ejemplos de pruebas al control

Fuente: IT Control Objectives for Sarbanes Oxley, 2nd Edition, ITGI

| Figure 20—Ensure Systems Security (*cont.*) | |
|---|---|
| **Control Guidance** | |
| **Illustrative Controls** | **Illustrative Tests of Controls** |
| A framework of security standards has been developed that supports the objectives of the security policy. | Obtain a copy of the security standards. Determine whether the standards framework effectively meets the objectives of the security policy. Consider whether the following topics, which are often addressed by security standards, have been appropriately covered:<br>• Security organization<br>• Asset classification and control<br>• Personnel security<br>• Software security policy<br>• Physical and environmental security<br>• Workstation security<br>• Computing environment management<br>• Network environment management<br>• System access control<br>• Business continuity planning<br>• Compliance<br>• System development and maintenance<br><br>Determine if there are processes in place to communicate and maintain these standards. |

¿Les recuerda algún conjunto de mejores practicas?

Áreas dónde debe haber estándares

Fuente: IT Control Objectives for Sarbanes Oxley, 2nd Edition, ITGI

**Figure 20—Ensure Systems Security (*cont.*)**

**Control Guidance**

| Illustrative Controls | Illustrative Tests of Controls |
|---|---|
| Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes). | Review security practices to confirm that authentication controls (passwords, IDs, two-factor, etc.) are used appropriately and are subject to common confidentiality requirements (IDs and passwords not shared, alphanumeric passwords used, etc.). |
| Procedures exist and are followed relating to timely action to requesting, establishing, issuing, suspending and closing user accounts. | Confirm that procedures for the registration, change and deletion of users from financial reporting systems and subsystems on a timely basis exist and are followed.<br><br>Validate that attempts to gain unauthorized access to financial reporting systems and subsystems are logged and followed up on a timely basis.<br><br>Select a sample of new users and determine if management approved their access and the access granted agrees with the access privileges that were approved.<br><br>Select a sample of terminated employees and determine if their access has been removed, and the removal was done in a timely manner.<br><br>Select a sample of current users and review their access for appropriateness based upon their job functions. |

ABC oportuno de las cuentas de usuario

**Nota: Asegurarse de que existan y se sigan**

Fuente: IT Control Objectives for Sarbanes Oxley, 2nd Edition, ITGI

| Figure 20—Ensure Systems Security (*cont.*) | |
|---|---|
| **Control Guidance** | |
| **Illustrative Controls** | **Illustrative Tests of Controls** |
| A control process exists and is followed to periodically review and confirm access rights. | Inquire whether access controls are reviewed for financial reporting systems and subsystems on a periodic basis by management.<br><br>Assess the adequacy of how exceptions are reexamined, and if the follow-up occurs in a timely manner. |
| Where appropriate, controls exist so that neither party can deny transactions, and controls are implemented to provide nonrepudiation of origin or receipt, proof of submission, and receipt of transactions. | Determine how the organization establishes accountability for transaction initiation and approval.<br><br>Test the use of accountability controls by observing a user attempting to enter an unauthorized transaction.<br><br>Obtain a sample of transactions, and identify evidence of the accountability or origination of each. |

Control de no-repudiación

Fuente: IT Control Objectives for Sarbanes Oxley, 2nd Edition, ITGI

| Figure 20—Ensure Systems Security (*cont.*) | |
|---|---|
| **Control Guidance** | |
| **Illustrative Controls** | **Illustrative Tests of Controls** |
| Where network connectivity is used, appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access. | Determine the sufficiency and appropriateness of perimeter security controls, including firewalls and intrusion detection systems.<br><br>Inquire whether management has performed an independent assessment of controls within the past year (e.g., ethical hacking, social engineering).<br><br>Obtain a copy of this assessment and review the results, including the appropriateness of follow-up on identified weaknesses.<br><br>Determine if antivirus systems are used to protect the integrity and security of financial reporting systems and subsystems.<br><br>When appropriate, determine if encryption techniques are used to support the confidentiality of financial information sent from one system to another. |

Fuente: IT Control Objectives for Sarbanes Oxley, 2nd Edition, ITGI

| Figure 20—Ensure Systems Security (*cont.*) | |
|---|---|
| **Control Guidance** | |
| **Illustrative Controls** | **Illustrative Tests of Controls** |
| IT security administration monitors and logs security activity at the application and database, and identified security violations are reported to senior management. | Inquire whether a security office exists to monitor for security vulnerabilities at the application and database levels, and related threat events.<br><br>Assess the nature and extent of such events over the past year and discuss with management how they have responded with controls to prevent unauthorized access or manipulation of financial systems and subsystems. |
| Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed. | Review the process to request and grant access to systems and data and confirm that the same person does not perform these functions. |
| Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication. | Obtain polices and procedures as they relate to facility security, key and card reader access, and determine if those procedures account for proper identification and authentication.<br><br>Observe the in-and-out traffic to the organization's facilities to establish that proper access is controlled.<br><br>Select a sample of users and determine if their access is appropriate based upon their job responsibilities. |

Fuente: IT Control Objectives for Sarbanes Oxley, 2nd Edition, ITGI

# En Resumen

- La seguridad de los sistemas de información es crítica para la gobernalidad y para el cumplimiento de regulaciones como Sarbanes Oxley.
- No hay un modelo de gobernalidad o de seguridad “unitalla”
- Sin embargo los principales estándares nos dan la pauta para establecer los controles de seguridad necesarios.

# ¡Gracias!


José Ángel Peña Ibarra

CCISA – Alintec

Monterrey, México

(52) 81 8357-1000

japi@ccisa.com.mx


Consultoria en Comunicaciones e Informática, S.A. de C.V. (CCISA), Firma miembro de

Alintec

IT Governance Consultants

www.alintec.net



Serving IT Governance Professionals

latin america cacs SM

2007

# Monterrey, México

21 a 24 octubre 2007