Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

La Ley Sarbanes-Oxley

Presentación del tema

La Ley Sarbanes-Oxley, conocida como SOX (Sarbanes-Oxley Act), es una normativa estadounidense promulgada en 2002 con el objetivo de fortalecer la transparencia, la confiabilidad de la información financiera y los controles internos de las organizaciones que cotizan en bolsa en los Estados Unidos. Si bien su origen está vinculado a escándalos financieros y contables, su impacto es especialmente significativo en el ámbito de los Sistemas y Tecnologías de la Información (TI), ya que gran parte de la información financiera se genera, procesa, almacena y reporta a través de sistemas informáticos.

Desde la perspectiva de la administración, SOX transforma a los sistemas de información en componentes críticos del control interno, imponiendo responsabilidades claras sobre la forma en que se gestionan los datos, los accesos, los cambios en los sistemas y la trazabilidad de la información financiera. La tecnología no solo soporta el negocio: también puede convertirse en una fuente de riesgo regulatorio si no se gestiona adecuadamente.

Objetivo y fundamento de SOX en TI

SOX establece un marco legal destinado a proteger a los inversores, asegurar la confiabilidad de los estados financieros, reforzar la responsabilidad de la alta dirección y exigir controles internos efectivos. Su premisa central desde los sistemas de información es que si los sistemas que procesan información financiera no son confiables, la información contable tampoco lo será.

Por este motivo, la ley no se limita a controles contables tradicionales, sino que exige controles sobre los procesos tecnológicos que intervienen en la generación de información financiera. Estos se denominan controles generales de tecnología de la información (IT General Controls, ITGC): no validan cifras contables, sino el entorno tecnológico que las produce.

Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Principales áreas de impacto en TI

SOX exige especial atención en cuatro áreas vinculadas a los sistemas de información.

Área	Qué exige desde TI
Control de accesos (Access Controls)	Solo personas autorizadas acceden a sistemas financieros; segregación de funciones; registro de actividades
Gestión de cambios (Change Management)	Cambios en sistemas financieros formalmente autorizados, documentados y probados; ambientes separados
Operación y continuidad (IT Operations)	Respaldos, planes de continuidad (BCP) y planes de recuperación ante desastres (DRP)
Integridad de datos (Data Integrity)	Validaciones, logs de transacciones y protección contra manipulación no autorizada

En el control de accesos, un principio clave es la segregación de funciones (Segregation of Duties): quien registra transacciones no debería poder aprobarlas ni modificar reportes financieros. En la gestión de cambios, una modificación en el cálculo de impuestos dentro de un ERP debe estar aprobada, documentada y registrada. En operación y continuidad, SOX exige que los sistemas críticos estén disponibles y funcionen de manera confiable.

La Sección 404 y la responsabilidad directiva

Uno de los artículos más relevantes de la ley es la Sección 404, que exige que la alta dirección evalúe la efectividad de los controles internos, certifique formalmente su funcionamiento y asuma responsabilidad ante fallas significativas. Desde TI, esto implica que los responsables tecnológicos deben documentar procesos y controles, participar

Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

activamente en auditorías internas y externas y ser corresponsables del cumplimiento regulatorio. La tecnología deja de ser un área puramente operativa para convertirse en un actor clave del gobierno corporativo.

Relación con otros marcos de referencia

En la práctica, SOX no se implementa de forma aislada. Las organizaciones suelen apoyarse en frameworks complementarios:

- COBIT (Control Objectives for Information and Related Technologies) para estructurar controles de TI.
- ITIL (Information Technology Infrastructure Library) para la gestión operativa.
- ISO/IEC 27001 para la seguridad de la información.

Estos marcos facilitan demostrar el cumplimiento y ordenar los procesos tecnológicos exigidos por SOX.

Ejemplo aplicado

Una empresa que cotiza en bolsa utiliza un ERP para su contabilidad. Para cumplir con SOX desde TI define perfiles de acceso estrictos, documenta y aprueba cada cambio en el sistema, registra auditorías de transacciones e implementa respaldos y controles de continuidad. El cumplimiento de SOX no depende solo del área contable, sino del correcto funcionamiento del sistema de información.

Conceptos clave

- SOX como ley que convierte los sistemas de información en componentes del control interno.
- ITGC como controles del entorno tecnológico, no de las cifras contables.
- Cuatro áreas de impacto en TI: accesos, cambios, operación e integridad de datos.

Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

- Segregación de funciones como principio de control de accesos.
- Sección 404: responsabilidad directiva sobre los controles internos.
- Complementariedad con COBIT, ITIL e ISO/IEC 27001.

Preguntas de repaso del tema

1. ¿Cuál es el objetivo principal de la Ley Sarbanes-Oxley?
2. ¿Por qué los sistemas de información son críticos para el cumplimiento de SOX?
3. ¿Qué son los controles generales de TI (ITGC) y en qué se diferencian de los controles contables?
4. ¿Qué implica la segregación de funciones en el contexto de SOX?
5. ¿Qué exige SOX en materia de gestión de cambios en los sistemas?
6. ¿Qué planes de continuidad requiere SOX para los sistemas críticos?
7. ¿Cómo impacta la Sección 404 en el área de TI?
8. ¿Qué marcos de referencia complementan a SOX en la implementación de controles?
9. ¿Qué riesgos organizacionales surgen si los sistemas financieros no están adecuadamente controlados?
10. ¿Por qué SOX transforma a TI de área operativa a actor del gobierno corporativo?