

# Convergencia entre ISMS y requerimientos legislativos

**Alex Quintieri Fernández**

alex@quintieri.com

## Resumen

La presente ponencia expone, como Best Practices en Gestión en Seguridad en Sistemas de la Información (ISMS), convergen con nuevos requerimientos legislativos.

Se introducen algunos de los aspectos críticos de la ISO 17799, usando esta como punto de partida para exponer su relación con los requerimientos de Sarbanes & Oxley Act (EEUU). Se describe el objetivo de Sarbanes & Oxley Act (en adelante SOX), y su implicación directa e indirecta en el área de Tecnologías de la Información. Finalmente se hace mención a Basel II, como nueva regulación Europea, la cual tiene múltiples puntos en común con SOX, en lo que a requerimientos IT se refiere.

**Palabras clave:** ISMS, ISO17799, Sarbanes & Oxley, Basel II

## 1. Descripción de la ponencia

La siguiente descripción pretende esquematizar los puntos a tratar en la ponencia, sin desarrollar, en el presente paper, el detalle de cada uno de ellos.

### 1.1. IT Security Governance

Best Practices en Gestión en Seguridad en Sistemas de la Información

- Objetivo de un ISMS (Information Security Governance)
  - o Definir los Objetivos del ISMS (dependiente de cada entidad y contexto)
  - o Asegurar la Gestión del Riesgo
- Descripción del Circuito en Gestión del Riesgo
  - o Documentación de los Activos
  - o Análisis de Riesgos de los activos
  - o Establecer Salvaguardas
  - o Realizar Gestión del Riesgo
  - o Establecer Controles
  - o Monitorizar entorno
  - o Gestión del Cambio

- ISO 17799

Breve descripción del catalogo de controles establecidos en la ISO17799

### 1.2. Sarbanes & Oxley Act

Como resultado de grandes fraudes financieros como Enron o WorldCom, se aprobó la Ley "Sarbanes & Oxley Act of 2002" (en adelante SOX). La ley tiene como objetivo asegurar la correcta gestión contable, mediante políticas y procedimientos financieros documentados, de forma que se devuelva la confianza al inversor.

Las grandes implicaciones de SOX en Tecnologías de la Información quedan definidas en la sección 404 (Management Assessment of Internal Controls), la cual especifica deben existir procedimientos y políticas los cuales aseguren la integridad de la información, así como la disponibilidad de la misma (req. anual). Asimismo, la sección 303 requiere el CEO y el CFO confirmen la fiabilidad de los reportes financieros, teniendo esta sección también sus implicaciones a nivel IT (req. trimestral).

Las principales áreas IT implicadas en el cumplimiento de Sarbanes-Oxley, se pueden resumir en:

- Seguridad en Sistemas y Gestión de

#### Incidencias

- Gestión de Rendimiento y Capacidad
- Continuidad de Servicio (BCP)
- Gestión de la Información
- Gestión de Procesos y Operaciones
- Gestión del Desarrollo y el Cambio
- Gestión de Instalaciones
- Terceras Partes Implicadas

Estas áreas deben poseer los controles necesarios en cada una de ellas, según las características propias de cada entidad. Cada control debe llevar anexo la documentación requerida, así como asegurar se hayan realizado los Tests periódicos, los cuales aseveren los controles son vigentes y activos. Finalmente, es importante asegurar la monitorización de los controles, así como la recopilación y registro de las trazas requeridas.

Finalmente, es importante asegurar el mantenimiento del cumplimiento de Sarbanes-Oxley.

### 1.3. Basel II

En 1988 el Comité de Supervisión Bancaria de Basilea aprobó el Marco por el que se rigen gran parte de entidades financieras, el Acuerdo de Basilea, denominado Basilea I.

Este acuerdo de amplio uso quedó obsoleto con el paso del tiempo, planteandose carencias del mismo a ser cubiertas y reconducidas.

Las principales deficiencias de Basel I, respecto a Seguridad IT son la carencia de contemplar los Riesgos Operacionales (control interno) en el acuerdo. Este punto en concreto ha sido reconsiderado en el nuevo marco denominado Basel II (de cumplimiento obligado en EU).

Como describe Basel II los Riesgos Operativos: El riesgo de pérdida como resultado de procesos, sistemas, fallos humanos o eventos externos.

Algunos aspectos contemplados desde la perspectiva IT:

- Gestión y Ejecución de Procesos de Negocio
- Fraude Interno / Externo
- Empleados y Entorno de Trabajo
- Plan de Continuidad de Negocio (BCP)

## Referencias

British Standard 17799:2

- <http://www.iso-standards-international.com/bs-7799.htm>

What is Sarbanes-Oxley

- Guy P.Lander
- Ed. McGraw Hill

The Sarbanes Oxley Guide for finance and IT Professionals

- Sanjay Anand
- Ed. Sarbanes Oxley Group LLC

<http://www.sarbanes-oxley.com>

Information Technology Control and Audit

- Ed. Auerbach

Information Security Foundation Good Practice for Information Security (ISF)

- <http://www.isfsecuritystandard.com>

International Convergence in Capital Measurement and Capital Standards

- Basel Committee on Banking Supervision
- <http://www.bis.org/publ/bcbs107.pdf>

Evaluating Internal Controls – EY

- [http://www.ey.com/global/download.nsf/Venezuela/Evaluation\\_Internal\\_Controls/\\$file/Evaluation\\_Internal\\_Controls.pdf](http://www.ey.com/global/download.nsf/Venezuela/Evaluation_Internal_Controls/$file/Evaluation_Internal_Controls.pdf)

Integrity Driven Performance - PWC

- [http://www.pwc.com/images/gx/eng/about/svcs/grms/PwC\\_GRC\\_WP.pdf](http://www.pwc.com/images/gx/eng/about/svcs/grms/PwC_GRC_WP.pdf)

<http://www.sarbanes-oxley-forum.com/>