



COSO II, veinte años después



José de la Peña Sánchez

Las olas procedentes del "tsunami" Treadway Commission, afortunadamente no cesan. Recuerdo que su denominación oficial en USA es National Commission on Fraudulent Financial Reporting, que inició su marcha en 1985 y emitió su informe en 1987, entregando el testigo a su Committee of Sponsoring Organizations, que publicó en 1992 el famoso Informe COSO sobre Control Interno-Marco Integrado, que desarrolló nuevos conceptos de control interno, traducido en 1997 para España.

Con algún retraso respecto a la saga Enron, reanudó su funcionamiento el precitado Comité y en 2004 apareció otro informe, el llamado COSO II sobre Gestión de Riesgos Corporativos-Marco Integrado –que de hecho comprende el COSO I– cuya versión española, utilizada como fuente en esta entrega, ha sido editada este año por **PricewaterhouseCoopers**, constituye una gran aportación a la cultura de la seguridad TIC desde mi personal punto de vista, dicho sea sin olvidar a otros grupos de interés, tanto públicos como privados, que se citan reiteradamente en el texto.

Por comparar, se observa que la versión española del COSO II se ha acelerado a la del COSO I –de USA 2004 a 2005 respecto a USA 1992 a 1997–, lo que motiva felicitación.

La versión escrita en español del COSO II tiene 151 páginas y 420 de la del COSO I, detalle que dice mucho y bueno, puesto que denota una sensibilidad hacia las limitaciones de tiempo, casi "ostentóreas", de los lectores de *estatus* elevado de determinados sectores.

En mi opinión es importante reseñar que la idea fuerza que alienta el COSO II es una especie de tratado de ciencia actuarial + Seguridad TIC + Código de Buenas Prácticas de Gobierno Corporativo, dicho sea en el mejor sentido.

Esto queda reflejado en algunos párrafos: "... La gestión de los riesgos corporativos es que las entidades existen con el fin último de generar

Gestión de Riesgos Corporativos - Marco Integrado Técnicas de Aplicación septiembre 2004

valor para sus grupos de interés" pero "La búsqueda de equilibrio entre intereses, a menudo contrarios, puede resultar complicada y frustrante". Grupo de interés se define como un "Conjunto de personas físicas o jurídicas que colaboran con una entidad o están afectadas por ella, tales como accionistas, comunidad en que opera,..." . Casi, casi, llegamos a la denominada responsabilidad social corporativa (RSC para los amigos).

La idea que alienta el COSO II es una especie de tratado de ciencia actuarial + Seguridad TIC + Código de Buenas Prácticas de Gobierno Corporativo.

El texto es comprensivo de los habituales Índice, Prólogo e Introducción, y por supuesto, la parte expositiva, que contiene el Resumen Ejecutivo, el Marco con doce capítulos –cada uno con un Resumen inicial– y los siete Anexos, que incluyen un Glosario; indudablemente permite, tanto la lectura íntegra y sistemática como la selectiva.

Por concretar: el COSO II se presenta gráficamente en formato de matriz tridimensional, que relaciona:

• **Las categorías de objetivos:** Estrategia – Operaciones – Información – Cumplimiento.

• **La entidad y sus unidades.**

• **Los componentes:** Ambiente interno – Establecimiento de objetivos – Identificación de eventos – Evaluación de riesgos – Respuesta a los riesgos – Actividades de control – Información y comunicación – Supervisión.

Pero antes de seguir, y por su interés para la seguridad TIC, volvamos a echar mano de definiciones, en este caso algunas reseñadas en el Glosario del Informe; las siguientes:

• **Riesgo inherente:** el riesgo a que se somete una entidad en ausencia de acciones de la dirección para alterar o reducir su probabilidad de ocurrencia e impacto.

• **Riesgo aceptado:** la cuantía en sentido amplio del riesgo, que una

entidad está dispuesta a asumir para realizar su misión (o visión).

• **Riesgo residual:** el riesgo remanente después de que la dirección haya llevado a cabo una acción para modificar la probabilidad o impacto a un riesgo.

• **Tolerancia al riesgo:** la variación aceptable en la consecución de un objetivo.

Efectivamente, el COSO II demuestra una sutil sensibilidad hacia la seguridad en forma de preocupación por los sistemas de información, otras veces como sistemas informáticos o

tecnología de la información o, escuetamente, tecnología, considerando su importancia en profundidad. Incluso concreta que el "... Concepto de 'seguridad razonable' refleja la idea de que la incertidumbre y el riesgo están relacionados con el futuro, que nadie puede predecir con precisión, y no implica que la gestión de riesgos corporativos fracase con mucha frecuencia".

Continuando el análisis del COSO II, merece completar los capítulos de MARCO, además de los componentes; me refiero a la Definición y a los finales: Roles y responsabilidad, ya que reseña, además de los habituales Consejo de Administración, Dirección, Director, Directores Financieros y Auditores Externos, también a Auditores Internos, Otro personal de la Entidad, Terceros, Legisladores y Reguladores, Terceros en Interacción con la Entidad, Proveedores de Servicios Externos, Analistas Financieros, Agencias Certificadoras de Solvencia Financiera y Medios de Comunicación; así como los capítulos sobre Limitaciones de gestión de riesgos corporativos y el referente a Qué hacer, que personaliza algunos roles y responsabilidades, llegando incluso a las Asociaciones Profesionales y a los Educadores, pero insistiendo en los miembros del Consejo de Administración, Alta Dirección, Reguladores y Otro personal de la Entidad.

Deberá aceptarse que el complejo legisladores/reguladores/supervisores USA ha reaccionado con significativa rapidez ante el evento Enron *et alii*, ya que alumbró la Sarbanes Oxley Act en 2002, potenció la SEC (*Securities and Exchange Commission*), creó la PCAOB (*Public Company Accounting Oversight Board*), y aceleró la publicación del COSO II, facilitando un marco teórico-práctico ante la avalancha normativa.

También ha tenido en cuenta Basilea II (y sus pilares), muy importante para el macrosector bancario y financiero, así como otras aportaciones de área anglosajona.

En UE y en España, la migración normativa de USA es lenta y asintótica; por ejemplo, se espera para 2006 el POB (*Public Oversight Board*) paneuropeo, que coordinará en dos direcciones, con USA/PCAOB (*Public Company Accounting Oversight Board*) y con los 25 POB nacionales, por ahora. A ello se suma la actual movida de I+D+i, la productividad, la RSC (Responsabilidad Social Corporativa), los Códigos de Buenas Prácticas de Gobierno Corporativo Olivencia y Aldama, y el próximo Código Conthe impulsado por la CNMV, teniendo en cuenta, el Informe Winter UE/2003.

En fin, que todo llegará; eso sí, con arranques de caballo y paradas de burro.

Para rematar esta entrega, quizás convenga evidenciar dos textos convenientemente entrecuillados, a fin de que algunos profesionales afectados por el análisis y la gestión de los riesgos se reencuentren con la pura verdad. Así me pareció a mí al leer que "El riesgo corresponde al futuro, que es inherentemente incierto. La gestión de riesgos corporativos no puede facilitar una seguridad absoluta", algo que por conocido no es menor cierto.

La segunda cita es todavía más balsámica, al indicar que "La primera limitación recuerda que nadie puede predecir el futuro con certeza. La segunda reconoce que ciertos eventos están sencillamente fuera del control de la dirección. La tercera tiene que ver con el hecho de que ningún proceso hará siempre todo aquello para lo que ha sido diseñado".

En otras palabras, que la seguridad TIC tiene su óptimo si es razonable. Claro está que lo difícil es ir midiendo lo razonable. ■

JOSÉ DE LA PEÑA SÁNCHEZ
Auditor de Cuentas Censor Jurado
y Licenciado en Informática
info@codasic.com