



SAO: efecto colateral



José de la Peña Sánchez

Los acontecimientos Enron-11S como casos cero han desencadenado la alarma social en USA y provocado una rápida reacción causa-efecto, que se traduce en la aprobación de la Sarbanes-Oxley Act 2002 (SAO, según el acrónimo profesional).

Pero semejante pieza plantea un problema inicial de soberanía territorial en lo referente a sociedades extranjeras que cotizan en bolsas norteamericanas, asunto que se encuentra en negociación entre EEUU y UE respecto a la extraterritorialidad del Comité de Supervisión de Auditores de Compañías Cotizadas (PCAOB-USA).

Para ponerle la guinda al asunto, es decir, para provocar una escalada de desconfianza en USA sobre la supervisión en la UE, vino el caso Parmalat, inacabado e inacabable, una joya de la globalización de la criminalidad económica.

Entresacando aspectos básicos de esta ley, merece destacarse lo referente al control interno (Regla 404), tanto en lo que atañe a sus procedimientos como a su evaluación, sin olvidar los comités de auditoría externa e interna o de la seguridad TIC; por supuesto, existen más epígrafes reseñables.

Sobre esto del control interno, función esencial en una organización, aunque de difícil comprensión en grano fino, y a pesar de que el lector pueda considerar presuntuoso por parte del autor citarse a sí mismo, creo que merece la pena recordar lo escrito alrededor del Informe COSO (revistas SIC nº 26 / 9-1997 y nº 54/4-2003) sobre infraes-

estructuras TIC, y que reitero.

La publicación de «Los nuevos conceptos del control interno» o sea, el Informe COSO, se editó en 1992 en EEUU y la traducción española vio la luz en 1997; COSO es el acrónimo de Committee Of Sponsoring Of the Treadway Commission, o sea la National Commission On Fraudulent Financial Reporting creada en 1985; ya se sabe, lo urgente (punto com+E 2000), desplazó lo importante.

La dinámica que establece la SAO entre el primer ejecutivo de una cotizada y el director financiero en la certificación de los informes periódicos de información financiera, se debería materializar en un incremento de recursos para favorecer la seguridad TIC

Entrando en materia SAO y en lo referente al control interno, conviene decir que los procedimientos y la evaluación serán certificados tanto por el CEO (ejecutivo máximo) como por el CFO (director financiero) en los Informes periódicos de la Información Financiera.

Desde luego, el cumplimiento de los objetivos SAO, especialmente su Regla 404, requiere una infraestructura TIC de alto nivel como *conditio sine qua non* para posibilitar el control interno prescrito, lo que va a traer como consecuencia un incremento de los presupuestos de inversión y gastos, que necesitará un incremento de los ingresos o una redistribución de inversiones y gastos.

Continuando con la Regla 404 de la SAO, los informes

periódicos (trimestrales, ..., atención al «síndrome del *quarterly*») de evaluación, incluso procedimientos, del control interno, insisto, certificados por CEO/CFO, exigen razonablemente una acción continua/continuada de aseguramiento, monitorización, información y auditoría, atendiendo al análisis coste/beneficio según SAO 404-9. Este análisis coste/beneficio puede ser un condicionante limitativo del cumplimiento.

No es de dudar que tanto

el Comité de Auditoría como la Auditoría Interna tendrán un papel destacado, máxime si tenemos en cuenta que la Auditoría Externa estará vigilada por el PCAOB.

Otro aspecto del tema es el de la información privilegiada (*inside and restricted information*), o sea, la utilización ventajosa de información de acceso interno y restringido en beneficio propio o de terceros, por acción o por omisión. Este aspecto estará sujeto a riesgo por las previsibles vulnerabilidades/amenazas.

En lo referente a la doctrina jurídica del levantamiento del velo y el incremento lógico del perímetro de consolidación en las corporaciones, realmente significa la evidencia del poder de hecho y no el ropaje jurídico de co-

bertura operativa.

Es indudable que la aparición de hipercorporaciones transnacionales, junto a la separación de la propiedad (el capital) mayoritaria y dispersa, de la gestión (el poder), con sus correspondientes información asimétrica y opacidad, ha llevado a una situación de habitualidad de heterodoxas prácticas de gobierno corporativo, por decirlo suavemente. Y esto no resulta deseable.

Creo que la dinámica que establece la SAO entre el primer ejecutivo de una cotizada y su director financiero se debería materializar en un incremento de recursos para favorecer la seguridad TIC; pero no debería olvidarse un hecho: que los delitos los cometen las personas —«amenazas endógenas y exógenas»—, y que las exigencias éticas no son sólo un tema académico, sino realmente un asunto corporativo prioritario.

Desde luego, el equipo CEO/CFO tendría que considerar que el responsable de seguridad TIC (dependa de quien dependa) será uno de sus mejores garantes a la hora de certificar el informe de control interno, ya que les podrá proteger con un robusto nivel de protección de la información. Ahora bien, para poder cumplir con esta función, este responsable necesitará recursos.

Pues bien, a la hora de la presupuestación de inversiones y gastos, la evaluación del ROSI tendrá un componente destacado dentro del negocio. Y es de esperar que el equipo CEO/CFO sepa valorar la importancia de la función de seguridad de la información/seguridad TIC en todos sus aspectos. ■

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