Auditoría: o todo, o nada

José de la Peña Sánchez

La 'alarma social' que están provocando los episodios de AVA y Gescartera en España, y de ENRON en USA, está incrementando hasta límites desconocidos el *gap expectations* en usuarios y público en general.

A tenor de ello, la actividad de auditoría, en su sentido más amplio y multidisciplinar, en tanto que sustanciada en informes cuyo contenido hay que entender como documentos en los que se expresan opiniones profesionales independientes acerca de una parte o del todo de la realidad del auditado en periodos de tiempo concretos (dejémoslo así), y no como certificados de buena o mala conducta, se está reorientando en el 'medio' a la detección de fallos (errores, irregularidades, incumplimientos de normativa...).

Por 'medio' vamos a entender aquí –si me lo permiten– un mundo de naciones-estado en el que pululan corporaciones transnacionales de tamaño y versatilidad crecientes. En fin, nada que no sepamos.

En buena lógica podemos aquí hacer un apunte, en el sentido de que tales corporaciones tienen sistemas de información muy complejos y parece ser que en «algunos» casos presentan disfunciones (socorrido vocablo) significativas, sobre todo en lo que atañe a opacidad y vulnerabilidad.

Dichos S.I., soportados en líneas generales por TIC, están empezando a requerir la creación e implantación de unos controles de seguridad sobre la información propia y de terceros que tratan (el descomponer en sus partes significativas el concepto de seguridad de la información en un mundo en el que la 'externalización externalizada' parece que se impone, es algo que dejaremos para otra entrega), que más tienen que ver, en su creación, implantación y auditoría con áreas distintas a las de S.I. y aledaños.

La visión exclusivamente tecnológica de la seguridad de la información no sirve hoy para justificar la necesidad de seguridad de la información ante los ejecutivos de las organizaciones encargados de dar el visto bueno a las inversiones en seguridad de la información (pido disculpas por la repetición).

El concepto de control se impone. Y tengo bien aprendido, que crear buenos controles, en este caso de seguridad de la información –no digo ya poder implantarlos, mantenerlos, dejarlos listos para que alguien cualificado e independiente los audite y, después, perfeccionarlos– es una de los retos más formidables de cuantos pueda o deba acometer un profesional de la seguridad de la información en una entidad.

AUDITORÍA INTEGRAL

Pero no quisiera desviarme de la temática que nos interesa desarrollar aquí –con ser la del párrafo anterior apasionante–, que no es otra que la que se vislumbra tras la fina interpretación del contenido de la Norma Técnica de Auditoría sobre «Cumplimiento de la normativa aplicable a la entidad auditada» (BOICAC, 47: 9-2001), unida a la dedicada a errores e irregularidades (BOICAC, 42: 6-2000), ambas basadas en Normas Internacionales IFAC según decisión de la UE.

La primera norma mencionada –todo un hito en España– contempla a la entidad desde un punto de vista de totalidad (funcional, territorial, organizativo...); la considera, en suma, como un sistema. El asunto tiene tomate. Y para que se evidencie lo dicho, nada como precisar algunos conceptos.

En el contexto, se entiende por **incumplimiento** los «*actos, por acción u omisión contrarios a la normativa aplicable, tanto si se aprecia intencionalidad como si no se advierte*». Por **normativa** se entiende aquel «*... Conjunto de disposiciones, cualquiera que sea su rango, a las que se halle sujeta la entidad auditada, ya sea con carácter general, específico o sectorial*»; y, en consecuencia, «*Incluye normativa de toda clase y de todo tipo: comunitaria, nacional, autonómica, provincial, municipal..., civil, mercantil, penal, fiscal, contable, laboral,...*». ¿Alguien da más? La verdad es que a la vista de esto se inicia en serio la etapa de la auditoría integral.

> ***La normativa «blanda», tipo Informe Olivencia, ha sido ineficaz, por lo que se ha considerado oportuno que lo que procede es la aplicación de la normativa «dura», es decir, aquella de obligado cumplimiento.***

En la norma también aparece el correspondiente epígrafe, en relación con determinado tipo de entidades por su dimensión, dedicado a la asignación de responsabilidades adecuadas (función de auditoría interna, comité de auditoría y director de cumplimiento de normas).

Por lo señalado hasta aquí, casi estaríamos dispuestos a afirmar que la normativa «blanda», tipo Informe Olivencia, ha sido ineficaz, por lo que se ha considerado oportuno que lo que procede es la aplicación de la normativa «dura», es decir, aquella de obligado cumplimiento.

La nueva orientación de la función auditora externa requiere equipos multidisciplinares de auditoría (o servicios profesionales surtidos...) de composición variable en el tiempo y en el espacio, que cubran el ámbito de la entidad auditada a partir de una determinada dimensión. Todo ello con «actitud de excepticismo profesional», «razonable» y «significativo», sin olvidar el «código de conducta» y todas aquellas normas sobre el uso del trabajo de terceros: otro auditor, auditor interno y experto independiente.

Queda para más adelante el conflictivo asunto –ya tratado en SIC– de la independencia del auditor y de la asesoría y la consultoría como actividades mercantiles colindantes. El que los equipos multidisciplinares de auditoría puedan hacer consultoría o asesoría, es asunto que veo hoy poco claro. La UE dirá.

Para terminar esta primera entrega de 2002 de una forma más directamente entroncada con las áreas de TIC y aledaños, incluida la de seguridad (no olvidar el 11-S ni el principio de empresa en funcionamiento), bien merece la pena repetir la saga de repercusiones en los sistemas de información de las entidades de ciertos acontecimientos (Y2K y efecto €), recordar algunos venideros (datos personales: se acerca la fecha límite establecida para la auditoría obligatoria del nivel medio, y, obvio es apuntar –por ser verdad de perogrullo– que no se pueden cumplir las medidas de nivel medio sin cumplir las de nivel bajo).

Otros asuntos por venir, y sus repercusiones en el mundo de los S.I.: medidas de nivel alto..., propuesta de directiva sobre el tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas..., futura ley de firma electrónica..., empresas cotizadas: cambios sustantivos por aplicación de las Normas Internacionales IASC en el Plan General de Contabilidad (UE 2005 *Regulation*), todavía en estudio... los dejaremos para otro momento. n

José de la Peña Sánchez
Auditor Censor Jurado de Cuentas
y Licenciado en Informática
info@codasic.com