



Independencia vs 'murallas chinas'

José de la Peña Sánchez



El ámbito en el que se desarrolla la protección de la información en la empresa y, especialmente el de la seguridad de los sistemas y tecnologías de información y comunicaciones, es permanente, y su gestión, continua y sin interrupción. Así hay que entenderlo desde la óptica del principio de empresa en funcionamiento.

En la actualidad, la sociedad se encuentra inmersa en una "cultura de la desconfianza", por lo que la seguridad debería de ser un bien muy apreciado por los gestores que realmente consideran prioritario trabajar e invertir económicamente para garantizar la supervivencia de su organización, incluso en hipotéticos escenarios de contingencia tecnológica inverosímiles. Ya saben: si algo es posible, pasará.

Una vez disparado este proceso (trabajar e invertir en seguridad TIC, o como dicen algunos SI/TIC), y alcanzada una fase de equilibrio suficientemente estable, o sea, una vez funcionando el tinglado (hoy se destina más presupuesto a proteger los sistemas que hace por ejemplo dos años, aunque eso no significa necesariamente que estén más seguros, que también), puede prestarse la debida atención a idear proyectos con/de seguridad cuyo emprendimiento esté justificado por aportar valores añadidos medibles al negocio o actividad.

Dicho esto, conviene remarcar que las reglas del juego en ciertos ámbitos están cambiando: nos referimos al principio de separación de funciones (de obligado cumplimiento) en la prestación simultánea de servicios de auditoría y consultoría por parte de una empresa a un

mismo cliente.

La función de seguridad de una empresa se va a ver afectada en este contexto en lo referente al diseño y puesta en explotación de sus sistemas de tecnología de la información, así como el servicio de auditoría interna.

Tiempo al tiempo: la actuación, por separado, con independencia y sin "murallas

chinas", de las actividades auditora y consultora, razonablemente, será algo diferente a la situación presente, lo que no acertamos aquí es a vaticinar cómo será, aunque sí podemos aventurar que acarreará tanto tensiones como nuevas oportunidades, como corresponde a un nuevo escenario cuyo punto inicial de pro-

En este marasmo de presente y de futuro se encuentra hoy inmersa la gestión de la seguridad TIC, intentando encontrar una ubicación estable que –se me ocurre pensar– no es compatible con los viejos usos y costumbres propios de la informática trasnochada

pios de la informática trasnochada. Y es de esperar que los decisores corporativos hábiles consideren indispensable una elevación del nivel de profesionalización de la seguridad de las TIC, ya que algunos expertos –buenos expertos– están pidiendo guerra. Y hay que dársela. (En el mejor de los sentidos).

CONTINUIDAD

Cambiando un poco de tercio, pero sin perder de vista el contexto de la protección de la información y colindantes, quizás convenga insistir en un tema ya tocado en mi anterior entrega (SIC 54: abril de 2003); me refiero a cierto desarrollo del criterio de continuidad (sin

Es de esperar que los decisores corporativos hábiles consideren indispensable una elevación del nivel de profesionalización de la seguridad de las TIC, ya que algunos expertos –buenos expertos– están pidiendo guerra; y hay que dársela (en el mejor de los sentidos).

interrupción). Me refería a las actividades continuas (*continuous*) de la monitorización (*monitoring*), del aseguramiento (*assurance*), de la información (*reporting*) y de la auditoría (*auditing*)...

Sin olvidar el dicho "traduttore, traditore", he realizado un periplo investigador teniendo en cuenta los diversos orígenes de los precitados vocablos, desde los clínicos hasta los actuariales, pasando por los de calidad y tecnológicos.

Y sin atreverme a citar las similitudes y diferencias entre todos ellos, he llegado a la conclusión de que los objetivos de trazabilidad y de evidencia básicos en la gestión de la seguridad de las TIC y de su auditoría, podrán ser cubiertos en su más amplio aspecto.

Ahora bien, para ello, es decir para que sea viable disparar el proceso de auditoría continua en una empresa, resulta necesario el cumplimiento de ciertos requisitos previos; a saber:

- Un sistema de características suficientes
- Un sistema de información fiable con controles primarios en la toma de datos
- Una auditoría o control secundario muy automatizado
- Un auditor experto en tecnologías de la información y en el sistema
- Control del proceso de información de la auditoría.

Indudablemente los prerequisites citados son difíciles de cumplir de forma generalizada en cada empresa, posiblemente de forma parcial en algunos casos. Además, es un hecho que, en la mayoría de ocasiones, no se contempla la vulnerabilidad con su correspondiente análisis de riesgos, algo básico.

Pero, claro, es que la tarea de gestionar la seguridad de la información es una función empresarial muy joven aún en los contextos ejecutivo y tecnológico cambiantes propios de nuestro tiempo, y es ahora cuando se están poniendo los cimientos para el futuro. En su momento, y si las cosas no se tuercen, se llegará a poner en marcha la auditoría continua de la seguridad, el control y su gestión. Falta maduración, experiencia, práctica y no sólo presupuesto. ■

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