Qué hacer con la seguridad TIC

José de la Peña Sánchez

Antes de centrarme en el asunto principal de esta entrega, que no es otro que sacarle un cierto colorido a la razón de ser de la seguridad TIC (como componente principal hoy de la seguridad de la información) en su lectura corporativa, realicemos una aproximación por zonas afines.

Y nada mejor para ello que remarcar un hecho poco cuestionable: que el entorno TIC ya ha sido metabolizado dentro de las estructuras organizativas corporativas, y ha pasado de considerarse una importante función de apoyo a admitirse como una función principal, ya que su actividad y repercusión son críticas. En este sentido, la experiencia traumática de la burbuja utópica punto.com ha sido catártica y eficiente al respecto.

Por otra parte, la actual situación de inseguridad en esta época de globalización y de deslocalización generalizada, teniendo en cuenta la sucesión de megaescándalos y de terrorismo ubicuo, alumbra un mundo complejo y caótico.

También merece recordarse el etiquetado "buen gobierno corporativo", esa insistente tendencia normativa, uno de cuyos fines principales es modificar el funcionamiento de las cúpulas empresariales. Conviene recordar aquí términos tales como la separación de funciones, los conflictos de intereses, la transparencia informativa, los códigos éticos (la ética no se regula, se practica. Banco Popular *dixit*), las «murallas chinas», el desarrollo sostenible, la responsabilidad social, la reputación, ..., o sea, del *Corporate Governance* al *IT Governance*, y después al *Information Security (IS) Governance*. Fácil de entender, aunque no tanto de implantar, controlar y medir.

Seguridad

Acercándose al tema de la Seguridad TIC, viene al caso en estos tiempos pensar que el incremento de la posibilidad de que algunas corporaciones acaben en los tribunales de justicia ha llegado a ser desgraciadamente un horizonte previsible.

Ya es frecuente detectar en la prensa profesional la aparición de trabajos sobre *Computer Forensics*, o *Forensic*, informática forense en versión española. La finalidad de la misma para las organizaciones (empresas, por ejemplo) es un asunto que requiere una entrega específica, ya que tiene implicaciones internas profundas que superan en varios órdenes de magnitud a la clásica y socorrida de poder probar las maldades que pueda haber realizado o estar realizando un intruso (de fuera) en un sistema de una persona física o jurídica.

Considero necesario, siguiendo usos UNE EN ISO, precisar algunas definiciones, lo que siempre es bueno en tiempos de cambio como los actuales:

– Forensics: si se sigue la analogía con *Economics*, *Mathematics*, *Statistics*, ..., se podría considerar como ciencia forense. Creo que la apropiación de términos de otras disciplinas es útil y clarificador en principio, pero debería precisarse lo suficiente para evitar equívocos, so pena de llegar al "informatiqués" o al *spanglish*.

Resulta adecuado citar al RAE/ 2001 para puntualizar los posibles usos en español: forense, del latín *forensis*: perteneciente o relativo al foro. Foro, del latín *forum*: sitio en que los tribunales oyen y determinan causas, y 2: curia y cuanto concierne al ejercicio de la abogacía y a la práctica de los tribunales. Médico forense: médico encargado por la justicia para dictaminar los problemas de la medicina legal. Medicina legal: aplicación de la medicina al asesoramiento pericial de los tribunales. Legal: prescrito por la ley y conforme a ella.

Además, he detectado *Forensic Audit* y *Forensic Accounting*, sólo comprensible el primero como auditoría forense.

En esta época de competitividad debería desarrollarse, en paralelo a la gestión de costes de calidad/no calidad, la gestión de costes de seguridad/no seguridad TIC, en el supuesto de que sean diferentes.

Regresando al *leit motiv* de este trabajo, esto es, la seguridad TIC, debería considerarse que, tanto desde el Consejo de Administración, como desde el Equipo Directivo, se está creando alrededor del entorno TIC un núcleo *ad hoc* que conviene estudiar a fondo, núcleo tan extremadamente "tecnologizado", que de presentar disfunciones en casos límite podrían llevar al desastre corporativo.

Además, dicho núcleo *ad hoc* podría entrar en colisión con otras unidades de control y/o supervisión, por lo que es conveniente eliminar tanto duplicidades como vacíos de competencias.

A fortiori, la seguridad TIC tiene acceso a la información, y por tanto, dispone de poder, luego su ubicación estructural no es tema baladí. Ojo con esto.

Desde luego, se tendría que evitar que la seguridad TIC fuera uno de los malos de la película, más que nada para evitar ineficiencia funcional, pero sólo por eso.

En mi opinión y en principio, existen dos posibles series de problemas, bien respecto al entorno TIC, bien respecto a la Auditoría Interna, comprensiva de la Auditoría del entorno TIC o como se pueda denominar; por lo tanto, las reglas de juego deberán ser muy claras, si se pretende que el «artefacto» funcione eficientemente.

Piensa S. Covey que «*Las compañías contabilizan a las personas como gastos y a las cosas como inversión*», «*...usando métodos de la época industrial, sin asumir que están en la era del conocimiento*». Indudablemente, estamos en tiempos del «valor razonable» y de los «intangibles», términos propicios a la creatividad.

No obstante, no se debe olvidar que, además de la Comisión de Auditoría, como «última ratio» aparece la Auditoría Externa.

En esta época de competitividad y su correspondiente necesidad de reducción de coste, debería desarrollarse en paralelo a la gestión de costes de calidad/no calidad, la gestión de costes de seguridad/no seguridad TIC, en el supuesto de que sean diferentes.

Otrosí: creo que sería útil ampliar el estudio de la seguridad TIC desde el punto de vista de un autoseguro; enriquecería el conocimiento del tema con una óptica no tecnológica. Como ilustración cito algunos términos interesantes: comunidad y dispersión de riesgos, coaseguro/reaseguro, reservas técnicas, lucro cesante, daños cantidad/daños calidad. Hay que hacerse mayores en esto de la protección de la información con especial intensidad en la seguridad TIC.

Para finalizar, merece la pena recalcar que la deslocalización está acelerando las prácticas de *outsourcing* y *offshoring* en aras de una reducción de costes, pero ante estas tendencias desaforadas y no del todo coyunturales, podrían aparecer riesgos de inseguridad jurídica y riesgo país cuyo estudio requiere la máxima atención. ■

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