



El reflejo de la seguridad en el cuadro de mando: hipótesis y perversiones



José de la Peña Sánchez

Por lo que está sucediendo al otro lado del charco y que en alguna medida ha llegado a la UE, la responsabilidad máxima empresarial corresponde al binomio CEO/CFO; en consecuencia, y dicho en primera aproximación y de forma muy esquemática, son la Cuenta de Resultados, el Balance y el Presupuesto los que condicionan tanto el esperable beneficio como el deseable incremento patrimonial. Estos son los ejes principales del cuadro de mando.

Pero entrémosle a la cosa, es decir, al cuadro de mando (Tableau de Bord en los 60/70), y definamos lo que podría entenderse como tal. Hay bastantes definiciones, pero aquí citaremos pocas.

Según Andersen (1998) es un "Informe ejecutivo que contiene las diferentes variables que permiten a los directivos de una empresa observar el funcionamiento de ésta, mediante el examen del grado de cumplimiento de los objetivos y de las desviaciones producidas".

Desde el punto de vista de la UNE 66175: 2003 "Guía para la implantación de sistemas de indicadores" 3.3, se entiende como una "Herramienta de gestión que facilita la toma de decisiones, y que recoge un conjunto coherente de indicadores que proporcionan a la alta dirección y a las funciones responsables una visión comprensible del negocio o de su área de responsabilidad. La información aportada por el cuadro de mando, permite enfocar y alinear los equipos directivos, las unidades de negocio, los recursos y los procesos con las estrategias de la organización".

Todo ello está en relación con la UNE-EN ISO 10012:2003 "Sistemas de gestión de las mediciones: requisitos para procesos y equipos", así como la UNE 66172 IN: 2003 "Directrices para la justificación y desarrollo de normas de sistemas de gestión".

Para mayor finura, AECA: 2000 establece una diferenciación entre el sistema de indicadores y el cuadro de

mando, ya que el segundo comprende al primero, y, además, otros tipos de información que los indicadores no ofrecen, básicamente cualitativa, sobre competidores, mercado,...

Imagen fiel

Resulta muy procedente señalar un aspecto crucial del cuadro de mando: que debería ser una "imagen fiel" (*true and fair view*) de la empresa, al tiempo que hacer algunas consideraciones no baladíes, como, por ejemplo, que el exceso de información podría provocar desin-

¿Qué cantidad/calidad de información sobre seguridad TIC debería incluir el cuadro de mando destinado a la cúpula de la empresa?

formación, ya que a medida que se asciende de nivel, la ampliación de ámbito requerirá concentración, o sea, filtrado, riesgo no desdeñable pero inevitable. Y es aquí donde el arte y la ciencia se juntan.

Hipótesis

Entre los aspectos a considerar al respecto de nuestro protagonista, está el de su posible auditabilidad, ya que se encuentra en el entorno de la Toma de Decisiones y del Control Interno, incluso del Informe de Gestión, si la empresa estuviera sujeta a Auditoría obligatoria.

Desde la óptica de la seguridad TIC, los indicadores deberían cumplir determinados requisitos, observar determinadas hipótesis (antes principios) de buen gobierno; a ser posible, generalmente aceptadas, como existen en otras disciplinas.

Cito las que considero más adecuadas: empresa en funcionamiento, uniformidad, importancia relativa, registro, no compensación y periodificación.

La hipótesis de "empresa en funcionamiento" (*going concern*) señala "que se considerará que la gestión de la empresa tiene prácticamente una duración ilimitada". Es

muy importante desde el punto de vista de la seguridad TIC, ya que "en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos" TIC, debería existir un Plan de Contingencia o de Continuidad del Negocio, que garantice su supervivencia.

La hipótesis de "uniformidad" (*consistency*), señala la necesidad de mantener en el tiempo los criterios adoptados en la elaboración de indicadores a efectos de comparabilidad; de alterarse de forma motivada, deberá reseñarse en el cuadro de mando. También es básico desde

el entorno de la seguridad TIC mantener los aspectos metrológicos de los indicadores respecto de la función, característica y confirmación.

La hipótesis de "importancia relativa" (*materiality*) determina que podrá admitirse la no aplicación estricta de los criterios, siempre y cuando la importancia en términos cuantitativos de la variación que tal hecho produzca sea escasamente significativa. Puntualizando, el juego de las siete y media de la importancia relativa estriba en que el riesgo está en sobreestimar (pasarse) o subestimar (quedarse corto).

La hipótesis de "registro" (*recording*) señala que los hechos deben registrarse cuando se produzcan. Resulta terrible desde la perspectiva de la seguridad TIC, la omisión transitoria o definitiva de hechos. Esto es de todo punto inaceptable, sobre todo si dichos hechos son relevantes o significativos (recordemos el principio de empresa en funcionamiento).

La hipótesis de "no compensación" (*no off setting*), señala que en ningún caso podrán compensarse hechos de distinto signo. Desde el ámbito de la seguridad TIC y típico de los indicadores no automáticos, podría disimular tendencias críticas vía

enmascaramiento de la realidad.

La hipótesis de "periodificación" (*accrual*) matiza que la imputación de hechos debería realizarse cuando se produzcan con independencia del momento en que se confirmen sus consecuencias. Desde el punto de vista de la seguridad TIC, está claro que son dos aspectos diferentes, de acuerdo con el principio de registro.

Ya se sabe que cada toro tiene su lidia, por tanto el cuadro de mando deberá presentar la imagen fiel de la empresa en el contexto de buen gobierno; sobre todo evitar su patología representada por la "creatividad" de su preparación, incluso la "alquimia" con los datos, letal en lo referente a seguridad TIC.

Insisto en estos aspectos no deseables por causa de la utilización habitual en este tema de métodos estadísticos, bien descriptivos o exhaustivos (además de la media, existen otras medidas de concentración / dispersión), bien no exhaustivos o por muestreo (atención a los tamaños muestrales, niveles de confianza o fiabilidad,...), bien por muestreos "opináticos", que son típicos de los indicadores no automáticos.

No parece descabellado aquí recurrir a la clasificación de Disraeli, quien sostenía que "Existen tres clases de mentiras: mentiras, grandes mentiras y estadísticas".

Y para finalizar esta entrega, dejaremos apuntadas un par de respuestas a una pregunta sabrosa acerca del Sistema de Indicadores de Seguridad TIC; la siguiente: ¿qué deberían contener los cuadros de mando de la Dirección de Sistemas, la Dirección de Seguridad TIC y Auditoría Interna (Comisión de Auditoría y Dirección de Auditoría)?

Daremos únicamente dos opciones:

1. Los mismos indicadores para las tres áreas.

2. Los mismos indicadores Sistemas y Seguridad TIC, y Auditoría Interna sólo lo significativo.

Se me ocurre que la segunda opción parece arriesgada, ya que existen términos bastante imprecisos, tales como: relevante (recuerdo que no existe el "relevatómetro"), significativo, relativo, razonable, volátil... ¿O no? ■

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