



De las métricas/ metrología a la metrolatría



José de la Peña Sánchez

Mi propósito inicial en esta entrega tenía como objetivo el cuadro de mando de la seguridad del sistema de información, esto es, qué puede entenderse por cuadro de mando en este contexto y lo que a todo ello subyace, incluyendo su conexión con el cuadro de mando corporativo (por cierto, no uso el término integral) en estos tiempos marcados por la tendencia al *continuous* (*monitoring, assurance, reporting & auditing*), la cual, obviamente, tiene sus repercusiones métricas y/o metrológicas.

Pero me voy a permitir una ligera desviación del asunto, motivada por el interés que he detectado en el último trimestre de 2003 en los mundillos profesionales de la gestión de la seguridad de la información y aledaños, en el asunto de la cuantificación, entendida como medio de comprensión de la realidad, ya sea cuantitativa como cualitativamente (para todo hay métodos creativos). Existe una gran confusión terminológica entre los distintos profesionales, y no es aconsejable que la misma crezca en estos primeros envites de la gestión de la seguridad de la información con el inevitable universo de la medida para las finalidades que usted y yo estamos pensando.

La cuantificación nos lleva inevitablemente a los ámbitos de los sistemas de medida, esto es, al término Metrología ("metro": medida o medición, y "logía", tratado, estudio, ciencia), que queda algo obsoleto, y Métrica/métricas (del inglés *metrics*), que hoy nos suena mejor.

Antes de entrarle al asunto, recordemos que la unidad de medida en la empresa española es el euro, lo que está propiciando la aparición de la eurometría, un frente más de la ya citada obsesión por la cuantificación. Al final, señores, mal o bien, todo hay que medirlo en euros: riesgos de información, casos de *phishing*, irregularidades en el cumplimiento de normas, multas, debilidades materiales en las prácticas y controles internos de la seguridad

de sistemas, ROI-ROSI, gastos en protección, auditorías...

Calidad y definiciones

Pero avancemos. En opinión de un servidor, y en el epígrafe de métrica/medición/metrología, se puede iniciar la descubierta al respecto de la seguridad desde la óptica paralela de la gestión de la calidad y de su entorno. Evitaremos así no volver a descubrir la rueda y, de paso, también evitaremos caer en los ya conocidos problemas de sinonimia/poli-semia.

Al respecto, y además de la serie ISO 9000:2000, es apropiado utilizar las siguientes normas inicia-

se define como "datos o conjunto de datos que ayudan a medir objetivamente la evolución de un proceso o de una actividad". Calibración es la "comparación técnica del equipo de medición con un patrón de medida".

En lo referente a las TIC, hemos analizado las conocidas normas sobre la gestión de la seguridad de la información: UNE-ISO/IEC 17799:2002 "Código de buenas prácticas...", y UNE 71501-(1-2-3) IN:2001 "Guías: conceptos y modelos, Gestión y planificación, y Técnicas". También hemos ojeado el hasta este momento proyecto de norma UNE PNE 71502 "Especificaciones para los sistemas de gestión de la seguridad de la información.

Se detecta un creciente interés en el mundillo profesional de la gestión de la seguridad de la información por la cuantificación como medio de comprensión de la realidad

ticas: UNE 66175:2003 "Guía para la implantación del sistema de indicadores", y UNE EN ISO 10012:2003 "Sistemas de gestión de mediciones: requisitos para los procesos y equipos".

En consecuencia es importante concretar algunos términos, tales como métrica, cuadro de mando, indicador, parámetro, criterio, medida, medición y calibración.

Métrica se entiende como "criterio de medición", siendo criterio "norma para conocer la verdad..." y medición "acción y efecto de medir" -no obstante, la norma TL 9000 emplea el término medición para reemplazar al término métrica, como término afín está metrología, ya reseñado-; medida es el resultado de una medición.

Por su parte, cuadro de mando se entiende como "herramienta de gestión que facilita la toma de decisiones, y que recoge un conjunto coherente de indicadores,..."; parámetro es el "dato o factor que se toma como necesario para analizar y valorar una situación", e indicador

pos de medición y registro) o no automáticas (riesgo de apreciación).

- Se plantea ya la necesidad de homogeneización/agregación de indicadores, así como de ponderación/consolidación, para conseguir visión de conjunto (con pérdida de detalle), todo ello en función de las necesidades de cada usuario (competencias/responsabilidades; urgencia: inmediata/diferida...).

- La valoración de activos, prevista en el Anexo B de la Norma UNE 71501-3 IN:2001 necesita un desarrollo de acuerdo con las reglas de valoración de algunas NIC (normas internacionales de contabilidad)/NIIF (normas internacionales de información financiera), tema complejo, ya que conceptos como valor razonable, activos intangibles, etc., podrán ser volátiles desde una óptica conservadora.

- Mi experiencia en los cuadros de mando señala que su utilidad para necesidades preponderantemente *Flash* se incrementa con la reducción -en lo posible- de la parte narrativa; el aumento de las partes gráfica y numérica le confieren mayor inteligibilidad, siendo los indicadores de evolución o posición, absolutos o relativos,... pero específicos.

Antes de terminar esta entrega, no me resisto a reseñar tres aspectos que adornan nuestro actual panorama, y que van a tener una gran importancia futura: 1) la aparición en nuestro país -procedentes de USA- de sociedades *proxy*, cuya función es la comunicación entre las sociedades y sus accionistas; es un caso de permeabilidad conceptual TIC/ Derecho mercantil. 2) La pérdida de puestos de trabajo de personal muy cualificado en USA vía el *offshoring*, puestos que se han trasladado a determinados países con salarios muy inferiores, atención, aprovechando la banda ancha de Internet. 3) Se constata nuevamente que la actuación de la RAE con la ampliación del lenguaje técnico-científico es manifiestamente mejorable, y que deberíamos acostumbrarnos al sistema UNE-EN-ISO de publicaciones, donde siempre aparece el epígrafe "Términos y definiciones" en cada norma. ■

JOSÉ DE LA PEÑA SÁNCHEZ

Auditor de Cuentas Censor Jurado
y Licenciado en Informática
info@codasic.com