

SINERGIAS CRÍTICAS

Como en su momento propugnó ESRAB, una iniciativa europea nacida hace un par de años para asesorar al venerable continente en materia de innovación en seguridad, el epígrafe de las infraestructuras críticas conforma, junto a los de protección frente al terrorismo, la seguridad de fronteras y la gestión de crisis, las cuatro misiones tecnológicas prioritarias identificadas por el citado organismo asesor, hoy reconvertido en ESRIF.

Sobre este asunto, tan típicamente asociado a la frágil 'pata' de la disponibilidad, ha habido una buena noticia: haciéndose eco de las instancias europeas de unificar la política de seguridad común de la UE, el Consejo de Ministros aprobó el pasado 2 de noviembre la creación de un Centro Nacional de Protección de Infraestructuras, cuya misión nuclear es la de custodiar y actualizar el denominado Plan de Seguridad de Infraestructuras Críticas.

El Centro, dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior, tiene encomendado conformar un Catálogo Nacional de Infraestructuras Críticas. Según ha trascendido, parece que, inicialmente, ya han sido inventariadas más de 3.500 instalaciones clave.

No es difícil imaginar –y sólo eso, pues es de carácter secreto–, que el tuétano del listado habrá recopilado las principales instalaciones estratégicas de nuestro país, entendidas desde un prisma valorativo digamos clásico: centrales nucleares, térmicas y eléctricas, de comunicaciones, redes de abastecimiento, de transporte... Todas ellas son sin duda posibles objetivos de acciones terroristas convencionales pero, ¿y las que no lo son? Imaginemos, por ejemplo, las que pudieran cometerse contra escenarios TI críticos (verbigracia: por si las moscas, la Comisión Reguladora de la Energía de EE.UU. aprobó en enero 8 estándares de reforzamiento de la seguridad y la fiabilidad para estas infraestructuras).

Aunque hay consenso general en atribuir todo su valor a las infraestructuras críticas en su sentido primario, no es menos cierto que el tema, por incipiente, no ha sido tan bien entendido –y subsiguientemente valorado–, al referirse a esas otras, menos evidentes pero igualmente 'tangibles,' como son las que descansan en bits, cuyo valor ya radica en ser en sí mismas información crítica.

Sin menoscabo de la tarea realizada, quizá convendría enriquecer esta noble encomienda con la incorporación de experiencias adicionales de profesionales probadamente desenvueltos en materia de protección TI. Seguro que con las aportaciones plurales de estos expertos, tanto de procedencia privada como pública, podría obtenerse un más exhaustivo chequeo.

A fin de cuentas, la pretensión de conformar un catálogo de activos críticos no puede desligarse de una visión moderna de la sociedad, sustentada inevitablemente en sistemas de información y comunicaciones. La invitación al maridaje, pues, está servida. ¿Quién se apunta?

Por cierto, y para hacer las cosas bien, las entidades que formen parte del catálogo de infraestructuras críticas deberían estar obligadas a disponer de un Sistema de Gestión de Continuidad de Negocio certificable. ●



LUIS G. FERNÁNDEZ
Editor
lfernandez@codasic.com