Sin dinero no hay ciberseguridad

José de la Peña Muñoz
Director
jpm@codasic.com

En marzo de 2019 el Tribunal de Cuentas de la Unión Europea emitió un muy oportuno documento informativo, intitulado "Desafíos de una política eficaz de ciberseguridad en la UE". El trabajo de campo se realizó entre abril y diciembre del año pasado. Y los resultados no pueden ser más desalentadores, porque de ellos se deduce que la UE y sus Estados miembros están construyendo su ciberseguridad sin tener una idea mensurable de en qué consiste y en qué debiera consistir, algo que, por otra parte, a nadie extraña, porque las decisiones de alto nivel en esta y otras materias las toman los políticos. ¡Ah, qué sería si la ciberinseguridad diera y quitara votos! (No piense el lector que estoy dándole ideas al CIS; aunque todo se andará).

> "No se trata solo de saber si se está invirtiendo y gastando mucho o poco, sino de cuánto. El Estado lo desconoce. Si quiere saberlo tiene que fijar partidas contables exhaustivas para la ciberseguridad y reflejarlas en los próximos Presupuestos. Así todos veremos cuánto cae, a quiénes y para qué"

Pero volvamos al Tribunal de Cuentas de la UE. Entre las deficiencias encontradas (a las que se refiere educadamente como desafíos), hay varias que no tienen desperdicio: la primera, enmarcada en el objetivo de la construcción de un marco político y legislativo, no es otra que disponer de una evaluación y rendición de cuentas verdaderamente significativas. Vamos, que se han hecho las cosas a ojo de buen cubero, cada uno a su leal saber y entender, sin objetivo definido, sin supervisión y sin medición de resultados.

Hasta aquí pareciera que toda la Europa comunitaria se ha contagiado del tópico modo de proceder mediterráneo. Pero al avanzar en la lectura del documento, la sospecha se desvanece, convirtiéndose en… ¡certeza!

Y es que en el epígrafe dedicado a financiación y gasto, el Tribunal ha identificado los siguientes desafíos: primero, adecuar los niveles de inversión a los objetivos (aumentar la inversión, incrementar su impacto); segundo, tener una visión clara del gasto presupuestario de la UE (gasto identificable en ciberseguridad; otros gastos en ciberseguridad no identificables como específicos, perspectivas de futuro); y tercero, dotar de recursos suficientes a las agencias de la UE (en esencia ENISA, EC3 de Europol y CERT-UE).

Sin duda, es en este último punto, el de financiación y gasto, en el que juraría que los expertos del Tribunal de Cuentas han tenido que contenerse y no lanzar un exabrupto. Resulta que no han podido conocer la inversión y gasto en los países, que algunas iniciativas de cofinanciación comunitaria no se han ejecutado, que otras, por ejemplo de ENISA, estuvieron infradotadas, y que se desconoce si algunos proyectos ejecutados han tenido retorno.

España

Aquí no hay quien sepa lo que se invierte en ciberseguridad (a efectos globales y en detalle) ni en la AGE, ni en las Comunidades Autónomas ni en los Ayuntamientos. Tampoco en el sector privado. (La revista SIC lleva haciendo estimaciones indicativas desde hace años, pero sometidas a una no despreciable incertidumbre). Hay confusión, además, en lo que se debe entender a efectos contables por ciberseguridad. Y, en ocasiones, el gasto en medidas técnicas de protección se embebe en el entorno operativo, desvaneciéndose la posibilidad de contabilizarlo de modo específico.

Ya no se trata de saber si se está invirtiendo y gastando mucho o poco, sino de cuánto. El Estado no lo sabe. Si quiere saberlo, urge fijar partidas contables exhaustivas para la ciberseguridad, a fin de que tengan reflejo en los próximos Presupuestos. Y así todos veremos cuánto cae, a quiénes y para qué. ●