



JOSÉ DE LA PEÑA MUÑOZ  
Director  
jpm@codasic.com

## RNS: mercado y patriotismo

**A** las estructuras verdaderas de la ciberseguridad nacional de España no parece que les guste depender de compañías especializadas proveedoras de tecnología y servicios con un alto riesgo de ser adquiridas por capital extranjero o de las que se pueda sospechar que sus socios o propietarios estuvieran deseando que entre capital extranjero en sucesivas rondas de financiación.

Por otra parte, el sector de la defensa y la seguridad patrio, ha estado desde hace muchos años sin interés por invertir también en el futuro (salvo escasas y muy significadas excepciones), mientras sus ejecutivos (que se pensaban que ellos eran el Estado) se mantenían dulcemente

mente asociados al mundo TIC: enfoque exclusivo a resultados, beneficios rápidos, rondas galácticas de financiación/inversión, caza y captura de ideas con futuro inmediato en modo churrera acelerada e incorporación eficiente en el proceso especulativo de muerte súbita y nacimientos múltiples.

Para poder empezar a construir el esqueleto de la ciberseguridad nacional, los responsables de la misma se vieron en su momento obligados a tirar de expertos y de las empresas que creyeron en la idea e invirtieron en un futuro lleno de riesgo. Y esas son las que, más o menos, configuran en el presente el ramo de la ciberseguridad nacional.

Pero los tiempos están cambiando: ahora sí interesa la ciberseguridad nacional (que es la de todos), suena la pasta y está en ejecución un primer piloto de la Red Nacional de SOC-RNS, una buena iniciativa no exenta de provocar desajustes sectoriales hasta ahora no vividos, porque al requerir para algunos procesos el uso de herramientas comunes, algunos prestadores privados que aspiran a estar en dicha Red, sienten cierta curiosidad por saber las condiciones de su uso.

El segundo punto de fricción tiene que ver con

la compartición y los tipos de actores de la RNS, en la que junto a los centros públicos hay prestadores especializados privados. Y esto ha despertado susceptibilidades entre algunos responsables de MSSPs. ¿Por qué? Pues dicho en román paladino: porque el prestador comparte en la Red lo que su cliente de la Red le diga, en función del contrato de prestación al que los dos se obligan. Si ser miembro de la Red le obliga a más, podría ver en peligro su *know-how* y generar en clientes suaves quebras de confianza.

Nos vamos haciendo mayores, el gremio va creciendo y la importancia de la ciberseguridad, también. Y lo que antaño empezó como una magnífica colaboración entre leales, ahora más que nunca debe fortalecerse. Al fin y al cabo, los de este lado somos los buenos. ●

**Ahora sí interesa la ciberseguridad nacional (que es la de todos), suena la pasta y está en ejecución un primer piloto de la Red Nacional de SOC-RNS, una buena iniciativa no exenta de provocar desajustes sectoriales hasta ahora no vividos en el gremio.**

anestesiados por la suave cadencia de los millonarios pedidos clásicos del 'cliente', que no invertía un duro en seguridad de la información. Mientras eso sucedía, el ramo de la ciberseguridad de muchos otros países se abría camino a su alrededor al ritmo de *speed metal* propio de las transformaciones 'digitales' (la de antes y la de ahora). Y así tenemos en nuestra historia casos extremos: el del temprano emprendedor al que le compró la compañía una multinacional de copete, y empresas de las que España como estado no puede prescindir, al tiempo que económicamente raquíticas, como Epicom.

El hecho es que aquí, y hasta hoy, la ciberseguridad ha crecido ligada preponderantemente al comprador privado. Es muy anglosajona y, por tanto, sus cromosomas incorporan genes típica-