



JOSÉ DE LA PEÑA MUÑOZ
Director
jpm@codasic.com

Ciberseguridad por diseño: ahí te quiero ver, Gobierno

Despues de que las escuelas de negocios lleven décadas criando monstruos; despues de que se haya dejado el menudeo inversor de *start-ups* en manos de zangolotinos con un algoritmo implantado en los lomos; despues de que algunos predicadores lleven más tiempo del necesario castigándonos las entendederas con el neomantra del emprendimiento innovador... Despues de todo, lector, en tiempos duros las personas físicas seguimos apegadas a las cosas del comer y las jurídicas a las de intentar seguir en funcionamiento, procesos ambos complejos e interrelacionados en los que, al final, tienen un papel estelar los euros.

Entre PERTES, manifestaciones de interés, planes de digitalización, medios propios, encargos a medios propios, proyectos tractores, instrumentos de colaboración público-privada, no se nos puede pasar que de lo que el Gobierno de España haga para ayudar a salir de la crisis a través de los Presupuestos y del ya convalidado Real Decreto-ley de medidas urgentes para la modernización de la Administra-

es debido. Y un indicador para saberlo es la expresión concreta de partidas presupuestarias para hacer visible la ciberseguridad también en las licitaciones que no sean exclusivas de ciberseguridad, pero que deben incorporarla.

Desarrollo reglamentario

El BOE nos ha traído, entre otros peteretes, el RD 43/2021, en el que se ha realizado el desarrollo reglamentario del Real Decreto-ley por el que se incorporó a la legislación española la Directiva NIS. Nos guste o no es una buena noticia, porque permite empezar a completar el siempre delicado proceso que va de lo estratégico a lo operativo.

En el texto hay mención a los Responsables de Seguridad de la Información, se dibuja en grano más fino la estructura e interrelaciones de los actores de la ciberseguridad nacional, se establecen obligaciones para los regulados, se nos aclara a algunos el papel de la Oficina de Coordinación de Ciberseguridad (OCC) y se aporta una Clasificación/Taxonomía de los ciberincidentes en la que, por cierto, se ha incorporado el vocablo "Troyano" en vez de haber incluido el correcto, caballo de Troya. (La verdad: me encantaría escuchar cómo le explica un experto a un político que un "Troyano" es un caballo de Troya...).

Un apunte más para terminar.

La Secretaría de Estado de Seguridad, a través de su Gabinete de Coordinación y Estudios, quiere contratar en el mercado apoyo técnico para tareas realmente sensibles relacionadas con CNPIC y OCC. Me atrevo a dar opinión: no tengo claro que un país como España deba hacer tal cosa. Las capacidades completas las debe tener el Ministerio correspondiente. Y leyendo los documentos disponibles, no da esa sensación. Pero este es un mal menor, porque seguramente tenemos que cubrir deficiencias históricas heredadas. Y eso es lo importante.

Y ya que mencionamos al CNPIC, le diré, lector, que sigue desde este verano (y a fecha de cierre de esta edición, el 29 de enero del presente) en obras www.cnpic.es, con el certificado caducado y el nombre antiguo, que no es el que se le puso en el Real Decreto 734/2020 por el que se desarrolló la estructura orgánica básica del Ministerio del Interior. Edificante. ●

“Los planes de digitalización tienen que venir con la ciberseguridad por diseño. Y las instancias gubernamentales deberían de arbitrar controles estrictos por sí con las prisas, la presencia de la ciberseguridad en las acciones públicas y las reguladas no atienden este particular como corresponde”

ción Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia (el de los 140.000 millones de euros en fondos europeos), depende que nuestro país no se convierta en el mayor secadero de *clusters*, *hubs*, polos, observatorios y parques tecnológicos de toda Europa.

Y, ¿qué tiene que ver con esto la ciberseguridad, con las consultoras, integradores, fabricantes, mayoristas, investigadores, compradores y resto de integrantes de la cadena de valor? Pues todo, porque es horizontal y vertical a todas las iniciativas que se lleven a cabo en el proceso de digitalización y modernización de todos los sectores, que, por cierto, es algo más complejo que el 5G.

Los planes de digitalización tienen que venir con la ciberseguridad por diseño. Y las instancias gubernamentales deberían de arbitrar controles estrictos por sí con las prisas, la presencia de la ciberseguridad en las acciones públicas y las reguladas no atienden este particular como