CISO: se hace camino al legislar

José de la Peña Muñoz
Director
jpm@codasic.com

Cuando se publique en el BOE el Real Decreto de desarrollo del Real Decreto-Ley NIS, cuyo proyecto puso el Gobierno en funciones, a través del centro directivo competente, en este caso la Secretaría de Estado para el Avance Digital, en trámite de audiencia e información pública, veremos si hay algún cambio relevante de contenido.

El documento, en su fase de tramitación a fecha de cierre de esta edición, trae buenas noticias para los concernidos por el ámbito NIS (directamente los operadores de servicios esenciales y proveedores de servicios digitales): concreta el marco estratégico e institucional, fija requisitos de seguridad, dedica un capítulo a la gestión de incidentes (notificación, procedimiento y Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes), fija criterios para la supervisión y aporta en anexo la Instrucción Nacional de Notificación y de Gestión de Incidentes.

> "Algunos responsables de seguridad de la información, aun aplaudiendo el contenido del artículo 7 del proyecto de Real Decreto de desarrollo del RD-L NIS, manifiestan que se ha perdido la oportunidad de definir la relación entre el RSI y el Responsable de Seguridad y Enlace (RSE), o ser más explícitos en el nivel de capacitación de los RSI".

La verdad es que si alguna persona del mundillo de la ciberseguridad no lo ha leído, debería hacerlo urgentemente, porque envueltos en los puntos generales antedichos, hay peteretes, piezas falsamente insípidas y alguna especia que amarga.

La especia que amarga es el uso de la expresión "seguridad integral" en un documento NIS. (Tampoco debería usarse en el ámbito PIC). La seguridad integral, una apropiación del mundillo de la seguridad física y de las personas e instalaciones ante ciertas situaciones y circunstancias, es producto del ombliguismo anacrónico que impera en ciertos predios corporativistas, que la usan para dar fundamento a lo que no lo tiene. Hay decenas de seguridades en base a la disciplina y el escenario: médica, farmacéutica, industrial, alimentaria, hospitalaria, nuclear, vial, arquitectónica, aérea, naval, tecnológica, jurídica… Habría que hacer un esfuerzo por dejar claro esto. La buena noticia es que en el proyecto del que hablamos, solo se usa la citada expresión en una ocasión.

Vayamos ahora con las piezas que he llamado antes falsamente insípidas. No son otras que aquellas en las que se empieza a dar el pistoletazo de salida a la apertura del melón normativo sectorial NIS (léase el Artículo 3. Autoridades competentes). Resulta necesario abrirlo, pero de un modo especialmente multicooperativo.

La bomba

Y llegamos a los peteretes, es decir, al Capítulo III (Requisitos de Seguridad) del proyecto, y muy especialmente su Artículo 7, titulado "Responsable de Seguridad de la Información". Para empezar lo que allí pone está más que bien. ¿Se puede mejorar? Por supuesto. Pero ante todo hay que felicitarse por el logro, que esperemos no se modifique a mal en el BOE.

Algunos responsables de seguridad de la información (RSI), aun aplaudiendo el contenido de este artículo, insisten en que hubiera sido necesario definir la relación entre el RSI y el Responsable de Seguridad y Enlace (RSE), o ser más explícitos en el nivel de capacitación de los RSI, por ejemplo.

Cierto es que se podrían hacer muchas cosas pero, si el asunto va por donde va, la figura del Responsable de Seguridad de la Información ha iniciado el camino de la regularización. Eso sí, exclusivamente en el ámbito NIS.

Mmm… me da que en algún momento la UE tendrá que abordar la unificación NIS y PIC, porque los modelos conceptualmente no se sostienen. Y en el caso español, además, la complejidad del sistema (incluida la dimensión RGPD) hace empalidecer la de las Teorías físicas del Todo.

Por tanto, arremanguémonos, colaboremos, esperemos a que se articule el Foro Nacional de Ciberseguridad, y seamos conscientes de que posiblemente tengamos RSI NIS en PSE y PSD, RSI no NIS en PIC, RSI ni NIS ni PIC, RSI NIS en PIC, RS por el ENS, DPDs y responsables de todo junto. (Seguro que alguno se me pasa).

Y un apunte final: según el proyecto, el RSI NIS "podrá apoyarse en servicios prestados por terceros" para desarrollar sus funciones. Y me pregunto: ¿tendrá alguien pensado regular a estos terceros proveedores de servicios? ●