La senda olvidada entre lo crítico y lo esencial

José de la Peña Muñoz
Director
jpm@codasic.com

Ya que el sector TIC continúa divulgando sus predicciones para este año, incluso entrado febrero, y que además en la revista SIC hemos tenido la osadía de preguntar a 161 entidades especializadas sobre qué técnicas novedosas se espera que pongan en práctica los ciberdelincuentes (y ellas la amabilidad de contestar), justo es que un servidor se atreva a mencionar (que no vaticinar, predecir, adivinar o pronosticar, y menos, pontificar) algunos asuntos concretos que convendría aclarar, encauzar o emprender de aquí al 31 de diciembre, convoque o no elecciones el presidente del Gobierno. Ahí van:

– El reconocimiento legal y armonizado de la figura del CISO (o como a la postre se le denomine) y la función en los ámbitos regulados NIS y PIC. A fecha de cierre de esta edición no se ha publicado en el BOE el desarrollo reglamentario del Real Decreto-ley 12/2018. Sería la primera pieza en la que esto quedara consagrado. Pero no la única.

> "Conviene tomarse en serio si las particularidades de algunos sectores críticos y esenciales, como por ejemplo el Eléctrico, hacen conveniente la creación de CERTs específicos".

– Tras la elaboración de la Guía nacional de notificación y gestión de ciberincidentes, urge poner en servicio la Plataforma Común de Notificación, la famosa "Ventanilla única de notificación".

– Dotar con los medios necesarios a la Fiscalía, a las FCSE y a las policías autonómicas para que no se vean desbordadas por un incremento de denuncias y por la expansión de la ciberdelincuencia.

– Aclarar muy por lo menudo cómo se va a regular la "actividad compatible" de la seguridad informática en el ya largamente esperado reglamento de desarrollo de la Ley de Seguridad Privada. Lo que se haga, si se hace, habrá que armonizarlo con lo que ya hay.

– Poner en marcha la primera fase del SOC de la AGE con visión de futuro a medio y largo sobre la transformación que afecta a productos, sistemas y servicios.

– Que los compradores empresariales, principalmente los grandes grupos y las compañías grandes y medianas, consignen la adquisición de productos y sistemas de ciberseguridad y la contratación de servicios en partidas presupuestarias específicas.

– Que por higiene algunas asociaciones de empresas y personas, en feliz revoltijo, cambien de presidente y vicepresidente al menos una vez cada década. La supuesta falta de tiempo de otros posibles candidatos es una razón manida y desacreditada para justificar la continuidad en la poltrona. Hay que estimular el cambio.

– Que los Consejos de Administración, Administradores y Alta dirección de empresas que aducen no entender, aprendan a interpretar si la información que se les facilita sobre el estado de la ciberseguridad de sus sociedades es o no aceptable para actuar en consecuencia incorporando en sus planes acciones de inversión y gasto si el nivel de exposición resulta inaceptable. No hay que olvidar que en el Barómetro de Riesgos de Allianz 2019, el cibernético se suma, por primera vez, a la pérdida de beneficios como el principal riesgo para las empresas.

– Todos estamos de acuerdo en que faltan expertos en ciberseguridad y hay que formarlos. Pero decir tal cosa sin más es una simpleza, porque esta disciplina y práctica se ha complicado. Conviene estudiar con urgencia qué perfiles y cantidades se van a necesitar a medio y largo plazo. En esto no podemos ir de Q en Q.

– Conviene tomarse en serio si las peculiaridades de algunos sectores esenciales y críticos hacen recomendable crear CERTs específicos.

– Los estados, las organizaciones internacionales y supranacionales deben obligar a los fabricantes de sistemas electrónicos con IT embebida y conectividad (estoy pensando en Medicina y Sanidad, por ejemplo) a que incorporen con urgencia la ciberseguridad por diseño en sus equipos. Quizá pueda incentivarse este particular diseñando planes de inversión públicos y privados para renovación y modernización. Hay que evitar desgracias.

– Las técnicas y métodos de Inteligencia Artificial y los sistemas basados en IA los aplican los buenos y los malos. Sucede, sin embargo, que bueno y malo son calificativos humanos.

– Continuará…