• El *ransomware* tiene un precio. Este es el título principal de la próxima edición de Espacio TiSEC, que tendrá lugar en Madrid los días 19 y 20 de este mes. Esta cita hay que entenderla como la continuidad de la serie temática sobre riesgos cibernéticos y ciber seguros que SIC inició en el año 2014 y en la que se proponía empezar a contestar a la siguiente pregunta: ¿Qué daños causados por ciberataques se atreve a cubrir el sector asegurador? Una década después esta cuestión sigue criando nuevas aristas, principalmente a raíz de la irrupción de la extorsión -en múltiples escalas y variantes- en los planes de negocio de la delincuencia.

El flujo de los ciberataques (también de los exitosos) forma parte del panorama del estado actual del arte de la digitalización y de gestión de riesgos de ciberseguridad (tecnología, implementaciones, servicios…). Bien puede decirse que, si no te toca hoy, te tocará mañana.

Por tanto, ese conceptual "riesgo residual" que se nos queda enquistado después de proteger y proteger, es como un "Pepito grillo" que nos recuerda que lograr la supresión de todos los riesgos es un objetivo inalcanzable. Y que mientras seguimos intentándolo, hay que estudiar por lo menudo la otra parte del asunto, aquella en la que debemos de tratar de que el impacto de un ciberataque exitoso sea, a todos los efectos, el menor posible.

En ambos terrenos el CISO tiene un papel estelar. Pero históricamente –y por razones obvias– las generaciones iniciales de CISOs tuvieron que hacer hincapié en la primera. Desde hace ya tiempo, y con la elevación en el ranking de importancia de los riesgos asociados con la ciberseguridad en el sistema de gestión de riesgos de las corporaciones (especialmente de las multirreguladas) al Responsable de seguridad de la información, los daños causados por ciberataques a propios y terceros, que se miden en dólares y euros, le han llevado a potenciar la suscripción de pólizas de seguros. Y aquí el CISO tiene un gran papel. Y también lo tienen la cadena de valor del seguro, la industria de ciberseguridad, los proveedores de servicios, la legislación en general y, a la postre, el mundo de los negocios y actividades.

En este Espacio TiSEC, la revista SIC, fiel a su ideario, volverá a tratar este asunto de la mano de los principales implicados: usuarios corporativos/CISOs, aseguradoras, mediadores, consultores, proveedores de servicios y de tecnologías y, como no puede ser de otra manera, los CSIRTs de referencia principalmente concernidos en España y los investigadores policiales. (Programa e inscripciones en https://revistasic.es/espacio-tisec/propuesta-el-ransomware-tiene-un-precio).

• Legislación y caos. Quizá haya alguien que sepa si vamos a trasponer la NIS2 a fecha. Aunque con la que tenemos encima, ni siquiera está claro si la pieza que se prepare finalmente va a responder solo a la trasposición o, además, va a incorporar deliciosos peteretes rellenos de ciber resiliencia y bañados por fuera con la esencia de lo integral, que tanto gusta en algunos ambientes gubernativos.

Recordará el lector avispado que aprovechando la necesidad de ajustar la legislación española al RGPD, hicimos la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos, en la que se coló la "garantía de los derechos digitales" so pretexto de cumplir con el artículo 18.4 de la Constitución. Desde luego, mal pensado no estaba.

Vista la gran discrecionalidad que cada Estado miembro de la UE tiene para trasponer directivas, habrá que esperar cualquier cosa, incluso la creación de una Agencia Nacional de Ciberseguridad que dependa del Ministerio de Juventud e Infancia. Por aquello de trabajar a largo plazo.

• Agencia de Ciberseguridad de la Comunidad de Madrid. Ya está en marcha la entidad, cuyo responsable es Alejandro Las Heras en calidad de consejero delegado.

En el momento actual se está creando la estructura de la Agencia, su Comité de Seguridad de la Información, la estrategia de ciberseguridad y la política global de seguridad de la información de la Comunidad de Madrid que dará lugar en 2025 a un Plan Estratégico de Ciberseguridad en el que se definirá la arquitectura de ciberprotección de esta Comunidad Autónoma y se determinará el presupuesto de la Agencia y el equipo humano necesario para su implantación y operación.

El lector puede leer en páginas interiores una entrevista de alcance, amablemente concedida por Alejandro Las Heras a SIC, en la que avanza los primeros pasos de la organización.

Edita: Ediciones CODA, S.L. Goya, 39. 28001 Madrid (España) Tels.: 91 575 83 24 / 25 Fax: 91 577 70 47 **Correo-e:** info@revistasic.com www.revistasic.com **Editor:** Luis Fernández Delgado **Director:** José de la Peña Muñoz **Redacción:** Ana Adeva, José Manuel Vera **Colaboran en este número:** Miller Auker, Nacho Barco, Marina Barroso, Ayla Chabouk, Jorge Dávila, Miguel F., Vanesa Gil, Gonzalo Gómez-Abad, Luis Fisas, John heldreth, Estefanía L., Guillermo Lorenzo, Juan López-Rubio, Andrés Romero, Julio San José, Mar Sánchez, Manuel Sanz, Manuel Serrano, Juan Miguel Velasco **Departamento de Marketing/Publicidad:** Rafael Armisén Gil, Fernando Revilla Guijarro **Administración y suscripciones:** Susana Montero, Maite Montero, Mercedes Casares **Fotografía:** Jesús A. de Lucas **Ilustración:** Fernando Halcón **Diseño y producción:** MSGráfica | Miguel Salgueiro **Imprime:** Monterreina **ISSN:** 1136-0623