

• **Riesgos asociados con terceros.** Las organizaciones con mayor cultura llevan años intentando gestionar del modo más eficiente posible los riesgos empresariales originados por vulneraciones o explotación de agujeros en la ciberseguridad de terceros proveedores integrantes de sus redes de suministro, que a su vez provocan riesgos de distinta naturaleza y en cascada en clientes y en organizaciones de las que también el cabeza de cadena de provisión puede ser proveedor.

Este tipo de macro riesgo, de materializarse los ciberataques y ser exitosos, tiene impactos múltiples en el espacio y en el tiempo, sobre la economía y la sociedad. Su carácter sistémico hace que, en el contexto, las amenazas (cibernéticas, ciber físicas y físicas) se enmarañen y den como resultado un escenario muy difícil de controlar.

A este hecho se une la mala posición de ciberseguridad de la mayoría de las pymes en las economías de los países, no ya solo por cultura y medios económicos y materiales, sino también por estar mal atendidas por la oferta de servicios, prestados por fabricantes y por proveedores, que presionados por los requisitos de resultados (la ciberseguridad se vende) no han tenido la necesidad de diseñar ni comercializar servicios gestionados de calidad y precio a medida de los distintos tipos y tamaños de pymes.

Es ahora, con motivo de la presión regulatoria y la obligación de prestar atención a la ciberseguridad de las cadenas de suministro, tras notables ejemplos de ciberataques, cuando los proveedores empiezan a ponerse las pilas. Y los estados y gobiernos también, tras años de dedicar dinero de los contribuyentes a acciones de la más variada índole y de resultados inmedibles.

Así pues, instauradas ya las ciberamenazas a las cadenas de suministro y a terceros de todo tipo, ejecutados algunos ciberataques para la galería y con distintas legislaciones de ciberseguridad, seguridad y resiliencia operativa del sector financiero (sin trasponer o sin estar en disposición todavía de ser aplicadas en plenitud), nos encontramos hoy un RGPD plenamente vigente y la dificultad añadida para las compañías aseguradoras, de poder valorar riesgos y empujar un mercado de ciberpólizas en el que los que ofrecen y los que contratan sepan realmente lo que están haciendo.

Precisamente en esta edición de SIC se dedican unas páginas especiales a la ciberseguridad en las redes de suministro. Y se hace con un enfoque multidisciplinar, en el que tienen cabida todos los actores involucrados, excepción hecha de los atacantes, a quienes desgraciadamente hay que tener muy en cuenta.

• **Espacio TiSEC: seguridad digital en ecosistemas de subcontratación.** El carácter sistémico de los riesgos a los que nos referimos ha llevado a esta publicación a dedicar la segunda edición de Espacio TiSec del año (18 y 19 de junio, presencial y en *streaming*) precisamente a tratar este asunto, de la mano de notables especialistas de organismos supervisores y del sector privado que atesoran un conocimiento en la gestión de riesgos tecnológicos, riesgos de ciberseguridad, riesgos de negocio y riesgos de incumplimiento. A ellos se suman especialistas del sector de seguro y mediación, cuyo concurso para cubrir algunos daños causados por ciberataques en insustituible y necesario. Se juntarán en el programa CISOs y especialistas en gestión de ciberseguridad en las empresas, cuyo papel se está viendo reforzado por las normas y las requisitorias de buen gobierno. Y también su nivel de estrés, al compartir con sus altas direcciones y consejos responsabilidades en la mejora efectiva de las posiciones de ciberseguridad de sus organizaciones. El programa del evento está disponible en [www.revistasic.com](http://www.revistasic.com).

• **Plan Nacional de Ciberseguridad 2022.** El Gobierno de España ha aprobado un conjunto de actuaciones de ciberseguridad y ciberdefensa –para completar las medidas incluidas en el Plan Nacional de Ciberseguridad 2022– que contarán con una inversión de 1.157 millones de euros. Las actuaciones se enmarcan en el Plan Industrial y Tecnológico para la Seguridad y la Defensa.

Las entidades que recibirán estos fondos adicionales, son (por orden de cuantía): El ministerio de Defensa (CNI–CCN, CESTIC y MCCE), El ministerio para la Transformación Digital y de la Función Pública (Agencia Estatal de Administración Digital, SETID-Red.es-Incibe), ministerio del Interior y Departamento de Seguridad Nacional. La aprobación de liberar estos fondos adicionales viene en gran parte motivada por las circunstancias geopolíticas y las demandas de mayor inversión en defensa, y, al tiempo, por el fortalecimiento de la (ciber)Seguridad Nacional, la (ciber)Defensa y la lucha contra la (ciber)delincuencia.

La aplicación de estos fondos a las organizaciones y entidades mencionadas, y su alcance a los proveedores de mercado, por ahora, son materia reservada.

**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](mailto:info@revistasic.com) [www.revistasic.com](http://www.revistasic.com) **Editor:** Luis Fernández Delgado **Director:** José de la Peña Muñoz **Redacción:** Ana Adeva, José Manuel Vera **Colaboran en este número:** Ana Adeva, Eli Bernal, Laura Betanzos, Juan Antonio Calles, Julio Castilla, José Manuel Delgado, Fátima Corpas, Jorge Dávila, Nicolás Gponzález, Reylany Gonzalez, Juan Carlos García, Isaac Guasch, José Carlos Jiménez, César López, Moisés López, Axel Losantos, Juan Pedro Manrique, José María Mezcuca, José Ramón Monleón, Rafael Ortiz, Alberto Partida, Antonio Ramos, Diego Rodríguez, Mónica Salas, Pablo San Emeterio, José Valiente, José Manuel Vera **Departamento de Marketing/Publicidad:** Rafael Armisén Gil, Fernando Revilla Guijarro **Administración y suscripciones:** Susana Montero, Maitte Montero, Mercedes Casares **Fotografía:** Jesús A. de Lucas **Ilustración:** Fernando Halcón **Diseño y producción:** MSGráfica | Miguel Salgueiro **Imprime:** Monterreina **ISSN:** 1136-0623

**SIC CIBERSEGURIDAD, SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD** no comparte necesariamente las opiniones vertidas por los autores de los artículos. Prohibida la reproducción total o parcial de cualquier información digital, gráfica o escrita publicada en SIC sin autorización escrita de la fuente.