

• **Securmática cumple 30 años.** En 2019, el congreso Securmática cumplirá treinta años de existencia, tres décadas de contribución decisiva a la seguridad de los datos personales y a la hoy llamada ciberseguridad, la privada, la pública, la de derechas, la de izquierdas, la de centro; la de arriba y la de abajo; tres décadas en las que varias generaciones de CISOs (del sector privado y del público, sin distinciones) y proveedores de servicios de primera división han ido presentando sus planes, sus proyectos, sus iniciativas, sus logros, sus sinsabores; tres décadas propiciando que las personas que trabajan a un lado y al otro del gremio se conozcan y colaboren; tres décadas constituyéndose en el imán de reuniones alrededor del evento; tres décadas apoyando la función de seguridad de la información y de seguridad IT; tres décadas aprendiendo y creando cultura de ciberseguridad, y dándole a todo un sentido.

La trigésima edición tendrá lugar en Madrid los días 23, 24 y 25 de abril, en su tradicional sede del Campo de las Naciones, que estará reacondicionada y modernizada para la ocasión.

Sería petulante exhibir cifras de número de congresistas, de número de conferencias pronunciadas y de proyectos presentados, de CISOs participantes, de copatrocinadores... Eso lo dejamos para aquellos que solo valoran lo cuantitativo. Y no es el caso de la revista SIC, organizadora de Securmática. Somos muchos, pero lo más importante es que queramos siempre ser mejores.

• **EE.UU. enseña las uñas.** La Administración Trump ha publicado una nueva Estrategia Nacional de Ciberseguridad, que sustituye a la de 2003. Como era de esperar, desde aquel año al presente la dependencia del ciberespacio ha ido creciendo en cualquier estado. Y también han ido aumentando las operaciones hostiles de todo corte, tanto del otro lado del Atlántico como desde este.

Por esta razón, EE.UU. ha considerado oportuno consagrar en su Estrategia la ejecución de acciones ofensivas si lo cree justificado, dejando la puerta abierta a la creación de una unidad de “disuasión cibernética”. Algo similar a lo planteado en plena carrera nuclear en los años 50.

Y es que “la Administración reconoce que EE.UU. está inmerso en una competencia continua contra adversarios estratégicos, estados deshonestos y redes terroristas y criminales. Rusia, China, Irán y Corea del Norte usan el Ciberespacio como un medio para desafiar a EE.UU. ...”

En suma, que en lo que toca a ponerse serios por escrito, la Estrategia USA marca un antes y un después, hecho que no habrá pasado desapercibido al lector, a quien se recomienda leer la sección ‘En Construcción’ de esta edición, en la cual su autor, Jorge Dávila, comenta con su mítica sagacidad algunos contenidos bastante llamativos de este documento.

• **Libro Blanco del CISO.** Por iniciativa del ISMS Forum y con apoyo institucional de INCIBE, en octubre vio la luz este documento, de obligada lectura para todos los profesionales involucrados en la gestión de riesgos, y muy especialmente para aquellos expertos en gestión de la seguridad de la información y ciberseguridad.

La obra, producto del trabajo de veinticinco personas, en su mayoría CISOs (de las que solo dos son mujeres), ofrece una visión bien documentada de la realidad de la función, de sus ubicaciones en los modelos de referencia y en los distintos tipos de organización, en la legislación y normativas por las que está concernida y de sus relaciones con otros directivos de la organización.

Sin duda, la aparición del Libro Blanco del CISO en estas fechas no es casual; antes bien puede decirse que está elaborado para ayudar al equipo de expertos que está trabajando en el desarrollo reglamentario del Real Decreto-ley por el que se transpuso la Directiva NIS para dar un justo reconocimiento a la función del responsable de seguridad de la información, reconocimiento que más allá de coyunturas, la revista SIC siempre ha apoyado y defendido desde hace muchos años, porque CISOs hay desde hace casi tres décadas en España. Y tampoco sería coherente no reconocer la función, sus responsabilidades y cometidos cuando el ENS sí los reconoce en el ámbito que regula.

Cosa diferente es que el acrónimo CISO-Chief Information Security Officer (Responsable de Seguridad de la Información) tenga que modificarse para describir mejor el universo completo sobre el que tiene arbitrio. Y en este sentido, no estaría de más prestar oídos a Gartner, que apuesta por la denominación de responsable de seguridad digital. ¿Alguien tiene una mejor?

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 **Sección Laboratorio SIC:** Javier Areitio Bertolin **Colaboran en este número:** Richard Barrell, Jorge Bermúdez, Stefan Beyer, José María Blanco, John Butler, Albaro Cañadas, Manuel Carpio, Federico Carvajal, Rafael Company, Jorge Dávila, Jorge Esperón, Josep Estévez, Carlos Galán, Jesús Hernández, Alberto Partida, Israel Pérez, Jose A. Reinoso, Antonio Requena, Francisco J. Rodríguez, Teresa Rodríguez, Facundo Rojo, Guillermo Sanz, Javier Zubieta **Departamento de Marketing/Publicidad:** Rafael Armisén Gil, Fernando Revilla Guijarro **Administración y suscripciones:** Susana Montero, Maite Montero, Mercedes Casares **Fotografía:** Jesús A. de Lucas **Producción, diseño y maquetación:** MSGráfica **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.