

El Instituto Español de Ciberseguridad y THIBER presentan su segundo estudio de ciberseguridad

EL SPANISH CYBER SECURITY INSTITUTE Y THIBER INSTAN AL GOBIERNO A TOMAR MEDIDAS PARA FOMENTAR EL DESARROLLO DE LA CIBERSEGURIDAD

> *El Estudio propone una serie de medidas, de carácter legal y organizativo, que el Ejecutivo podría poner en práctica para generar un ecosistema digital seguro y resiliente.*

> *Solo el desarrollo de una sociedad digital capaz de proteger sus intereses, a sus ciudadanos y a sus empresas, en un mundo cada vez más dependiente de la tecnología, garantizará la prosperidad económica y social.*

> *En los últimos tiempos el número de ciberataques ha crecido exponencialmente, ocasionando pérdidas que solo en EEUU en 2012 superaron los 300.000 millones de dólares.*

El **Instituto Español de Ciberseguridad** (SCSI, Spanish Cyber Security Institute), iniciativa de ISMS Forum Spain, y **THIBER**, *the cyber security think tank*, presentan su segundo estudio, **“Incentivando la adopción de la ciberseguridad”**, para fomentar la adopción de medidas de ciberseguridad por parte del sector empresarial. El Estudio, en la misma línea que el primer documento publicado, **“[La Ciberseguridad Nacional, un Compromiso de Todos](#)”**, mantiene el objetivo de mejorar la capacidad de las empresas para hacer frente a las ciberamenazas, y fomentar una cultura de ciberseguridad basada en la prevención y en la resiliencia. Sin embargo, añade un paso más y **propone como eje de acción el estímulo de la inversión y el desarrollo de capacidades de protección en el ciberespacio.**

La evolución de las Tecnologías de la Información y las Comunicaciones ha supuesto una auténtica revolución social cargada de beneficios, tanto en la rapidez de las comunicaciones y en la dimensión de la información disponible, como en la capacidad para analizar grandes cantidades de información; pero también ha servido como plataforma para la consecución de fines ilícitos. **Los ciberataques, en todas sus variantes, constituyen una problemática para gobiernos, empresas y ciudadanos que adquiere relevancia a la vez que suma víctimas y causa estragos en una sociedad hiperconectada.** Es una realidad que la mitad de las empresas españolas ha sido víctima de un ciberataque en los últimos dos años.¹ En este sentido, muchos países han desarrollado estrategias nacionales de ciberseguridad² para mejorar su capacidad de respuesta ante estos ciber-incidentes.

¹ <http://www.delitosinformaticos.com/06/2014/delitos/fraudes-y-estafas/la-mitad-de-las-empresas-espanolas-sufrieron-ciberdelitos-en-los-ultimos-dos-anos>

² Estrategias nacionales de ciberseguridad en el mundo. THIBER. http://www.thiber.org/?page_id=242

En respuesta a este panorama, SCSÍ y THIBER proponen una serie de medidas legales, de financiación, de reconocimiento público y de colaboración público-privada, entre otras, con el objetivo de poner en marcha **políticas orientadas a estimular la creación y desarrollo de un mercado específico de ciberseguridad, que facilite la adopción de medidas de prevención y protección ante ciberdelitos**. En opinión de los autores, *“fortalecer el mercado de la ciberseguridad es fundamental para desarrollar las capacidades necesarias para hacer frente a los desafíos y amenazas del ciberespacio”*.

Para ello proponen un **enfoque basado en el incentivo público** para aquellas empresas que adopten medidas de ciberseguridad, frente al tradicional modelo impositivo y sancionador de cumplimiento normativo, con el fin de sensibilizar al sector empresarial y facilitar el desarrollo de cibercapacidades que permitan proteger el activo más importante de gobiernos, empresas y ciudadanos: la información.

“Es necesario generar las condiciones favorables para que las organizaciones consideren la seguridad y la protección del ciberespacio como un valor y una inversión en lugar de como un coste. Una sociedad que premie las empresas que operan en su territorio y que demuestren el compromiso con la protección de la información e infraestructuras tecnológicas de los ciudadanos en calidad de clientes y usuarios, sin lugar a dudas, resultará más eficaz”.

Situación en otros países

Son numerosos los estados que ya han tomado medidas para mejorar su capacidad, en términos agregados, para hacer frente a las ciberamenazas. Reino Unido, La India, EEUU, o Irlanda, han invertido en planes de impulso en materia de ciberseguridad como vector de crecimiento económico (tejido empresarial, capacitación, nuevos puestos de trabajo, etc.). En términos de financiación, China, Corea del Sur, Japón y EEUU, facilitan directa o indirectamente el acceso al crédito.

Pero sin duda, destaca el caso israelí por el alto nivel de inversión mantenido por el gobierno desde los años noventa, con las “incubadoras tecnológicas” como máximo exponente, con subvenciones que oscilan entre los 350.000 y los 600.000€.

Medidas en el marco de la Estrategia de Ciberseguridad Nacional

El Estudio propone en última instancia el desarrollo de políticas de impulso y apoyo a aquellas organizaciones comprometidas con la protección de los sistemas de información e infraestructuras tecnológicas, como parte ineludible de la implementación práctica de las líneas de acción identificadas en la [Estrategia de Ciberseguridad Nacional \(ECN\)](#)³, definida el pasado 5 de diciembre de 2013 por el presidente del Gobierno, Mariano Rajoy, como “el marco de referencia de un modelo integrado basado en la implicación, coordinación y

³ Estrategia Nacional de Ciberseguridad Nacional
<http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf>

armonización de todos los actores y recursos del Estado, en la colaboración público-privada, y en la participación de la ciudadanía”.

Los autores de este Estudio destacan que en una economía como la española, con un 90% de PIB basado en los sectores servicios, energía e industria, el riesgo de no tomar medidas puede ser elevado ya que estos sectores son especialmente dependientes de las nuevas tecnologías de la información y la comunicación.

Sobre ISMS Forum Spain

La Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, es una organización sin ánimo de lucro fundada en enero de 2007 para promover el **desarrollo, conocimiento y cultura de la Seguridad de la Información en España**. Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. ISMS Forum Spain tiene ya a **más de 120 empresas asociadas y más de 800 profesionales asociados**. La Asociación es ya, por tanto, la mayor red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España.

El **Instituto Español de Ciberseguridad (SCSI, Spanish Cyber Security Institute)** es la última iniciativa puesta en marcha en el seno de la Asociación. Su misión es impulsar y contribuir a la mejora de la Ciberseguridad en España y crear un estado de conciencia sobre la necesidad de la Ciberseguridad para controlar y gestionar el estado de riesgo que genera la dependencia que el desarrollo socio-económico del país tiene respecto de las Tecnologías de la Información y la Comunicación (TIC).

PARA MÁS INFORMACIÓN:

DEPARTAMENTO DE COMUNICACIÓN DE ISMS FORUM

Tel.: 91 186 13 50

comunicacion@ismsforum.es

www.ismsforum.es

Síguenos en [Twitter](#) y [LinkedIn](#)