El Instituto Español de Ciberseguridad publica su primer estudio de ciberseguridad

EL SPANISH CYBER SECURITY INSTITUTE ABOGA POR UNA ESTRATEGIA DE CIBERSEGURIDAD NACIONAL LIDERADA POR EL GOBIERNO

> El actual escenario obliga al Estado a incluir el ciberespacio como un elemento clave en la gestión global de riesgos de la seguridad nacional.

> Es necesario concienciar a la sociedad española sobre la necesidad de disponer de un ciberespacio seguro para garantizar la prosperidad de nuestra sociedad y economía.

> El éxito de un ciberataque contra alguna de las infraestructuras críticas puede provocar devastadores efectos, como la suspensión de servicios básicos como la electricidad o el caos en los transportes o el sistema financiero.

El Instituto Español de Ciberseguridad (SCSI, Spanish Cyber Security Institute) de la Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum, ha elaborado un estudio que reclama al Gobierno que asuma el liderazgo en materia de ciberseguridad para proporcionar un ciberespacio seguro, que garantice la prosperidad social, cultural y económica de España, así como las libertades fundamentales de los ciudadanos a través de una cultura basada en la prevención y la resiliencia. Para ello, se requiere desarrollar una Estrategia Nacional de Ciberseguridad que cree un conocimiento de la ciber-situación estable y actualizado, mejore la resiliencia nacional frente a las ciberamenazas, y conciencie a la sociedad para fomentar una cultura de ciberseguridad.

De este modo, se solicita que el ciberespacio sea considerado como nueva dimensión del entorno operativo junto a los ya tradicionales (tierra, mar, aire y espacio), ya que en la actualidad representa un elemento clave en la gestión global de riesgos de la seguridad nacional. En cualquiera de sus dimensiones o ámbitos, ésta es una responsabilidad esencial de cualquier Gobierno y requiere los **recursos humanos, económicos y técnicos** suficientes.

SCSI e ISMS Forum proponen una estructura organizativa de alto nivel que posibilitará dirigir, controlar y gestionar la Ciberseguridad Nacional, que incluye la creación de un Órgano Nacional de Ciberseguridad, encargado de la dirección; y un CERT[1] Nacional de Referencia y un CERT de Defensa, con capacidad para la detección, prevención, contención y respuesta ante cualquier ataque o contingencia cibernética. Se destaca que hay que fomentar la **colaboración público-privada** en materia de ciberseguridad, ya que, entre otros motivos, el sector privado es dueño y gestor de gran parte de las infraestructuras críticas. También es

[1] *Computer Emergency Response Team*

necesario desarrollar un programa nacional de ciberconcienciación, tanto para favorecer el uso de las TIC sin riesgos como para generar demanda de ciberseguridad entre los ciudadanos. Así, se proponen campañas de sensibilización o la inclusión del tema en los planes de estudio.

El estudio aboga por **evolucionar de una cultura reactiva a una de prevención y resiliencia**. Un compromiso que exige la integración de todos los actores e instrumentos, públicos o privados, para aprovechar las oportunidades de las nuevas tecnologías y hacer frente a los retos de un **contexto de riesgo global**. De este modo desarrolla una aproximación a los conceptos de ciberespacio y ciberseguridad, a los riesgos y amenazas conocidos y a la gestión existente en España; lo que pone de manifiesto la necesidad de desarrollar un sistema nacional de ciberseguridad. Se destaca que aún **no se ha alcanzado un grado de ciberseguridad nacional acorde al estado de riesgo del ciberespacio**.

Según abogan sus autores, "la estrategia nacional de ciberseguridad debe ser un instrumento que guíe a los responsables de la dirección y gestión de la Ciberseguridad Nacional así como de sus beneficiarios pero, además, deberá servir como instrumento de **disuasión para sus potenciales transgresores**".

La ciberseguridad, una emergente preocupación mundial

La ciberseguridad se encuentra actualmente en las agendas de empresas y autoridades políticas internacionales y es considerada como una de las mayores preocupaciones mundiales, como destaca el Foro Económico Mundial (Word Economic Forum) en su último informe sobre *Riesgos Globales*. Los **actores de los ciberataques, y sus motivaciones, han cambiado**. Ahora priman las bandas de crimen organizado que buscan conseguir grandes sumas de dinero, los Estados que los utilizan como **ciberarma**, organizaciones privadas que buscan **información secreta** de empresas, colectivos guiados por principios ideológicos o políticos, como el ciberterrorismo o hacktivismo. También ha crecido el **tráfico de datos personales** que violan la privacidad de los ciudadanos. Se trata de riesgos reales, contrastados, que causan y/o podrían causar devastadores efectos, no sólo económicos. Puesto que los ciberataques podrían hacer fallar los servicios públicos esenciales, provistos por las infraestructuras críticas de un país como el sistema energético o los transportes, o, incluso, poner en riesgo la propia seguridad nacional.

En los últimos años, países de nuestro entorno han puesto en marcha estrategias nacionales de ciberseguridad, entre los que destacan las experiencias del Reino Unido, con una fuerte inversión presupuestaria; y a nivel Europeo se está preparando una Estrategia Europea para la Ciberseguridad, cuya presentación está prevista para finales de año, según anunció en la pasada XI Jornada Internacional de Seguridad de la Información de ISMS Forum el Jefe de Unidad Adjunto de la Dirección General de Sociedad de la Información y Medios de Comunicación de la Comisión Europea, Andrea Servida.

En términos globales, un país como el Reino Unido estima que la ciberdelincuencia le cuesta unos 33 mil millones de euros al año. Esto es más que el PIB de países como Honduras. Además, la ciberseguridad genera una actividad económica de 50.000 millones de dólares anuales, según la firma Ultra Electronics. Los daños económicos pueden llegar a ser catastróficos. Sony atribuyó unos costes de 132 millones de euros a los ataques a su red de PlayStation en 2011. Según el Informe de Amenazas CCN-CERT, "Ciberamenazas 2011 y Tendencias 2012" los **incidentes registrados en la Administración Pública española** han elevado su nivel de criticidad (durante 2011 se registraron 93 incidentes catalogados con una severidad de muy alto o crítico).

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 100 empresas asociadas y más de 750 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).

Descarga del estudio: https://www.ismsforum.es/noticias/noticia.php?idnoticia=346

PARA MÁS INFORMACIÓN:
DEPARTAMENTO DE COMUNICACIÓN DE ISMS FORUM
Juan Antonio Ibáñez
Tel. directo: 651119764
comunicacion@ismsforum.es

www.ismsforum.es
Síguenos en Twitter y Linkedin