Para lanzamiento inmediato

Contacto para medios:
FERNANDO UJALDÓN. 91 788 32 22
fernando.ujaldon@ketchum.com
LEIRE RUBIO 91 788 32 00
leire.rubio@ketchum.com

Un estudio de BSA sobre Leyes de Ciberseguridad en la UE identifica diferencias en relación a la preparación de los estados miembros en temas informáticos

Bruselas — 3 de marzo de de 2015 — El primer estudio sobre leyes y políticas para ciberseguridad en Europa encuentra diferencias y divisiones en relación a la preparación de los estados miembros en temas informáticos.

El informe, publicado hoy por BSA | The Software Alliance, evalúa las leyes, las normativas y las políticas nacionales en todos los 28 estados miembros de la UE en relación a 25 criterios estimados como esenciales para garantizar la protección efectiva en ciberseguridad. Este informe ha sido elaborado para ofrecer a los estados miembros de la UE una oportunidad para evaluar sus políticas nacionales frente a unas unidades de medida esenciales y representa un avance, ya que describe los principales componentes para el establecimiento de un sólido marco legal para ciberseguridad.

"Observamos un entorno desigual cuando hablamos de la protección informática en Europa. La mayoría de los estados miembros reconoce que la ciberseguridad es una prioridad, aunque las inconsistencias en sus enfoques dejan a todo el Mercado Único en una zona vulnerable a las amenazas", afirmó Thomas Boué, director de políticas de BSA EMEA. "La Directiva sobre Redes y Seguridad de la Información podría ayudar a establecer un nivel básico y más sólido en ciberseguridad y una mayor resistencia informática si se centra en armonizar la preparación de las infraestructuras más críticas de Europa y si introduce unos procesos comunes para la distribución y la elaboración de informes en todo el Mercado Único".

Entre las principales conclusiones del informe podemos destacar:

- La mayoría de estados miembros de la UE reconoce que la ciberseguridad es una prioridad nacional – especialmente en lo relativo a las infraestructuras críticas.

- Existen discrepancias considerables entre las políticas, los marcos legales y las capacidades operativas sobre ciberseguridad en los estados miembros, lo que crea unas diferencias notables en la protección general de la ciberseguridad en Europa.
- Casi todos los estados miembros de la UE han establecido equipos especializados para ocuparse de incidentes informáticos. Sin embargo, varían los objetivos y la experiencia de dichas entidades.
- Existe una preocupante falta de cooperación sistemática en los sectores público y privado y de colaboración en temas relacionados con la ciberseguridad entre los gobiernos de la UE / organismos no gubernamentales y partners internacionales.

El informe señala que España adoptó una Estrategia Nacional de Ciberseguridad en 2013, la cual es compatible tanto con el Plan Nacional de Seguridad como con las leyes de seguridad existentes, de modo que la estrategia y el marco legal trabajan en conjunto. Asimismo, España tiene varios equipos de respuesta ante emergencias informáticas operativos para hacer frente a las incidencias de ciberseguridad y seguridad informática. Y para garantizar la coordinación entre los sectores público y privado. El Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) funciona con grupos de trabajo sectoriales y está desarrollando planes de ciberseguridad específicos por sectores. Además, las asociaciones del sector privado son bastante activas y cuentan con dos amplios grupos dedicados específicamente a la seguridad informática y la ciberseguridad.

El informe anima a los estados miembros de la UE a centrarse en los cuatro elementos esenciales para un sólido marco legal en ciberseguridad:

- Desarrollo y mantenimiento de un marco legal completo - tanto político como legislativo-, basado en una estrategia de ciberseguridad a nivel nacional y complementada con planes de ciberseguridad específicos para cada sector.
- Establecimiento de entidades operativas con responsabilidades claras en seguridad informática, emergencias y respuesta a incidentes.
- Suscitar confianza y colaborar en alianza con el sector privado, ONG, partners y aliados internacionales.
- Promover la educación y la concienciación sobre riesgos y prioridades en ciberseguridad.

Al mismo tiempo, el informe advierte a los gobiernos europeos que eviten regímenes proteccionistas poco cooperadores que pueden debilitar, - en vez de mejorar-, las protecciones en ciberseguridad. En especial, los estados miembros deberían:

- Evitar requisitos innecesarios o poco razonables que pueden limitar la elección e incrementar costes, incluyendo la necesidad de pruebas o certificaciones exclusivos y específicos para cada país; exigencias de contenidos locales; la obligación para dar a conocer información confidencial como, por ejemplo, código fuente o claves de encriptación y restricciones sobre posesión por parte de extranjeros de propiedad intelectual.
- Evitar la manipulación de estándares, en vez de ofrecer apoyo a estándares técnicos utilizados por la industria y reconocidos internacionalmente.
- Evitar normativas para localización de datos y garantizar el tráfico gratuito de información en los mercados.

- Evitar las preferencias por tecnologías domésticas que pueden obstruir el acceso a competencia extranjera y dañar la innovación mundial.

El informe completo de los 28 países, además de los resúmenes detallados para cada estado miembro de la UE, se encuentran disponibles en www.bsa.org/EUcybersecurity.

Acerca de BSA

BSA | The Software Alliance (www.bsa.org) es el principal impulsor de la industria del software a nivel mundial ante los gobiernos y el mercado internacional. Sus miembros se encuentran entre las empresas más innovadoras del mundo, creando soluciones de software para impulsar la economía y mejorar la vida moderna. Con sede en Washington, DC, y operaciones en más de 60 países de todo el mundo, BSA es pionera en programas de cumplimiento que promueven el uso de software legal y aboga por políticas públicas que estimulan la innovación tecnológica e impulsan el crecimiento en la economía digital.