Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional
[*BOE* n.º 103, 30/IV/2019]

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Estamos ante una norma ciertamente particular, de las que no es frecuente encontrar dada la ausencia de articulado en la misma. Ahora bien, esta circunstancia no resta un ápice de importancia al valor de la misma, no solo desde su perspectiva práctica, sino también desde el propio ámbito jurídico. Hay que destacar que la Estrategia Nacional de Ciberseguridad es una norma en sí misma que desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 (Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017) y de la propia Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo.

En los tiempos presentes y más en los futuros, las actividades que se desarrollan en el ciberespacio son y serán fundamentales para la sociedad. La tecnología e infraestructuras que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio uno de los principales riesgos para nuestro desarrollo como nación, siendo preciso garantizar su protección sin que ello implique ningún tipo de menoscabo de su empleo. Por ello, lo que se ha dado en denominar seguridad en el ciberespacio es un objetivo prioritario en las agendas de la mayoría de gobiernos en aras de garantizar su Seguridad Nacional y una competencia del Estado para crear una sociedad digital en la que la confianza es un elemento fundamental.

Alcanzar un ciberespacio seguro y fiable, desde un enfoque multidisciplinar abarcando aspectos más allá de los puramente técnicos, implica tomar como punto de partida conocer y comprender las amenazas a las que nos podemos enfrentar, especialmente aquellas nuevas y emergentes, a la par que se han de tener presentes las oportunidades que presente el ciberespacio. De todo ello se encarga el primer capítulo de la Estrategia.

El segundo capítulo, bajo el rótulo «Las amenazas y desafíos en el ciberespacio», contribuye a fijar las principales amenazas del ciberespacio que, en su condición de espacio global común, genera las mismas. Precisamente la elevada tecnificación de estas y de la gran conectividad existente, que posibilita la amplificación del impacto ante cualquier ataque, hacen de estas amenazas algo realmente necesario de ser controlado. Para ello, la norma, viene a clasificar estas amenazas y desafíos en dos categorías: por un lado, las que amenazan a activos que forman parte del ciberespacio; y, por otro, aquellos que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo.

Ars Iuris Salmanticensis,
vol. 7, Diciembre 2019, 247-249
eISSN: 2340-5155

La interdependencia de esta estratega con la de Seguridad Nacional es el eje del tercer capítulo, que, titulado «Propósito, principios y objetivos para la ciberseguridad», aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a cinco objetivos específicos: seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales; uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso; protección del ecosistema empresarial y social y de los ciudadanos; cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas y finalmente la seguridad del ciberespacio en el ámbito internacional. Su desarrollo, se viene a forjar en el cuarto capítulo titulado «Líneas de acción y medidas», donde se establecen siete líneas de acción y se identifican las medidas para el desarrollo de cada una de ellas.

Dichas líneas de acción se dirigen a: reforzar las capacidades ante las amenazas provenientes del ciberespacio; garantizar la seguridad y resiliencia de los activos estratégicos para España; impulsar la ciberseguridad de ciudadanos y empresas; reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio; impulsar la ciberseguridad de ciudadanos y empresas; potenciar la industria española de ciberseguridad y la generación y retención de talento, para el fortalecimiento de la autonomía digital; contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo de los intereses nacionales, y desarrollar una cultura de ciberseguridad de manera que se contribuya al Plan Integral de Cultura de Seguridad Nacional.

El carácter organizativo del quinto capítulo, «La ciberseguridad en el Sistema de Seguridad Nacional», se aprecia con la definición de la arquitectura orgánica de la ciberseguridad. Bajo la dirección del presidente del Gobierno, la estructura se compone de tres órganos: el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Ciberseguridad, que apoya al Consejo de Seguridad Nacional y asiste al presidente del Gobierno en la dirección y coordinación de la política de Seguridad Nacional en el ámbito de la ciberseguridad, y fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, y el Comité de Situación, que, con el apoyo del Departamento de Seguridad Nacional, apoyará la gestión de las situaciones de crisis en cualquier ámbito que, por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales.

Se complementa este sistema con la Comisión Permanente de Ciberseguridad, que facilita la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad, siendo el órgano que asistirá al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad; las autoridades públicas competentes y CSIRT (Computer Security

Ars Iuris Salmanticensis,
vol. 7, Diciembre 2019, 247-249
eISSN: 2340-5155

Incident Response Team) de referencia nacional, y se incorpora la creación de un elemento novedoso de colaboración público privada, el foro Nacional de Ciberseguridad.

No debemos olvidar que, en este último capítulo, también se exponen a modo de conclusión una serie de consideraciones finales, a la par que se especifican los mecanismos para la actualización y evaluación de la Estrategia, en aras de prolongar su validez y eficacia, siendo conscientes del carácter voluble que reviste a la misma en función de los avances tecnológicos.

Daniel TERRÓN SANTOS
Profesor de Derecho Administrativo
Universidad de Salamanca
datersa@usal.es

Ars Iuris Salmanticensis,
vol. 7, Diciembre 2019, 247-249
eISSN: 2340-5155