Estrategia Nacional de Ciberseguridad. España 2019
Una prioridad, un reto y un compromiso para todos.

Recientemente se ha publicado la Orden PCI/487/2019, de 26 de abril, sobre la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional (BOE de 30 de abril de 2019).

La Estrategia Nacional de Ciberseguridad española desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo.

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

Hacemos el resumen de la norma que, aún siendo una guía de bases generales, se manifiesta de manera clara y concisa en sus objetivos y esquema de planteamiento.

El documento se estructura en cinco capítulos.

El primero, titulado “El ciberespacio, más allá de un espacio común global”, proporciona una visión de conjunto del ámbito de la ciberseguridad, los avances realizados desde la aprobación de la Estrategia de 2013, las razones que afianzan la elaboración de la Estrategia Nacional de Ciberseguridad 2019, así como las principales características que impulsan su desarrollo.

El adecuado desarrollo y aplicación de este planteamiento, exige trabajar con un enfoque multidisciplinar en todos los sentidos, que englobe aspectos más allá de los básicamente técnicos, En este sentido, el sector privado juega un papel relevante como uno de los gestores y propietarios mayoritarios de los activos digitales de España, por lo que las capacidades de ciberseguridad residen en gran medida en las de sus empresas y entidades públicas.

Por otro lado, la adecuada transición de un modelo de ciberseguridad de carácter preventivo y defensivo hacia un esquema que incorpore elementos de mayor fuerza disuasoria requerirá de un contexto global de mayor competencia geopolítica.

Finalmente, la rápida evolución de las ciberamenazas aconseja una aproximación y desarrollo más proactivo de la ciberinteligencia.

El segundo capítulo, titulado “Las amenazas y desafíos en el ciberespacio”, determina las principales amenazas que derivan de su condición global y común, de la elevada tecnificación y de la gran conectividad que posibilita la amplificación del impacto ante cualquier ataque.

Clasifica estas amenazas y desafíos en dos categorías: por un lado, las que implican 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.

El tercer capítulo, 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.

Su desarrollo principal, se plasma en el cuarto capítulo, titulado “Líneas de acción y medidas”, donde se establecen siete líneas de acción y se identifican las medidas para la implementación 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 ciberdelincuencia 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 quinto capítulo, titulado “La ciberseguridad en el Sistema de Seguridad Nacional”, define 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 recursos habituales.

Consideraciones finales y evaluación

A modo de conclusión, en la nueva Estrategia Nacional de Ciberseguridad española 2019, se exponen una serie de consideraciones finales y se concretan los mecanismos para la actualización y evaluación de la propia Estrategia.

La experiencia adquirida desde la Estrategia de Ciberseguridad Nacional de 2013, ha permitido plasmar en este nuevo documento una actualización de las amenazas y los desafíos a los que nos enfrentamos, siempre en continua evolución.

Para adecuarse a este nuevo escenario cambiante, se propone un conjunto de Líneas de Acción y medidas más dinámicas, que permitan, si fuese necesario, una rápida adaptación del ecosistema de ciberseguridad nacional, basado en un modelo de gobernanza con una considerable madurez, donde debe participar activamente el sector privado y el resto de la sociedad civil.

En este sentido, la Estrategia se concibe como un documento vivo que ha de irse ajustando a la evolución de la ciberseguridad, por lo que deberá ser objeto de revisión continua, como también los planes específicos y sectoriales que de ella se deriven.

Se elaborará un informe anual de evaluación de la Estrategia donde figurará el grado de ejecución y cumplimiento de sus objetivos generales y particulares.

Por otro lado, a la vista del incremento de las amenazas y desafíos a la ciberseguridad y cómo los afrontan países de nuestro entorno, resulta cada vez más urgente dotarse de recursos económicos, humanos y materiales para hacer frente a los mismos. Una de las acciones especialmente relevantes en este marco es que el Centro de Operaciones de Ciberseguridad de la Administración General del Estado se encuentre adecuadamente dotado.

En resumen, la Estrategia Nacional de Ciberseguridad 2019 establece la posición de España ante una nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional.

La nueva ciberseguridad se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social.