## Comentario THIBER:

# Estrategia Nacional de Ciberseguridad 2019

**AUTOR:** Guillem Colom,
Director de THIBER



**Foto:** Moncloa

A finales del pasado mes de abril, el gobierno aprobaba la nueva Estrategia Nacional de Ciberseguridad que desarrolla las provisiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la seguridad de nuestro ciberespacio especifico.

Esta nueva estrategia supone una evolución notable respecto a la de 2013*; convirtiendo a la ciberseguridad en uno de los ámbitos indispensables para la modernización del concepto de Seguridad Nacional.

La digitalización es el habilitador utilizado por el gobierno para darle peso a una estrategia esencial para el desarrollo socio-económico de nuestra nación.

*En 2013, el gobierno aprobó la Estrategoa de Ciberseguridad Nacional, cuya denominación debería haber sido Estrategia Nacional de Ciberseguridad. Mientras la Seguridad Nacional es un concepto, definido por un expresión sustantiva, la Ciberseguridad es una función y el carácter de la estrategia que lo dirige es nacional (como adjetivo).

# La digitalización es el habilitador utilizado por el gobierno para darle peso a una estrategia esencial para el desarrollo socio-económico de nuestra nación



La estrategia realiza un análisis acertado del actual panorama de amenazas en el ciberespacio y pone foco en el desarrollo de los principios rectores de la Seguridad Nacional: unidad de acción, anticipación, eficiencia y resiliencia. Además, define un detallado conjunto de objetivos y líneas de acción – muy alineadas con la mayoría de las estrategias nacionales de ciberseguridad de nuestros principales aliados y socios- que, paradójicamente, ponen de manifiesto los principales gaps y contradicciones de la actual ciberseguridad nacional.

Desde THIBER, consideramos que hay un conjunto de acciones que deben ser priorizadas y aceleradas respecto al resto para hacer posible llevar a buen puerto la nueva estrategia:

- **Gobernanza**: La dirección actual bajo el CNI ofrece mejores oportunidades de gobernanza y desarrollo a la ciberseguridad nacional. Pero si la ciberseguridad crece en la medida que se espera, deberá alejarse en un futuro cercano de la incubadora de inteligencia donde se encuentra para encontrar su propia autonomía.

- **Sector privado:** En aplicación del principio de responsabilidad compartida, el sector público debe mantener estrechas relaciones con las empresas que gestionan los Sistemas de Tecnologías de la Información y las Comunicaciones relevantes para los intereses nacionales, intercambiando el conocimiento que permita una adecuada coordinación entre ambos y una cooperación efectiva que genere una sinergia apropiada dentro del entorno de la ciberseguridad. Esto permitirá tener un nivel de coordinación e integración apropiado en caso de ciberincidentes a nivel global.

- **Industria nacional e incentivos:** Será necesario adoptar 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 ciber-delitos. Fortalecer la industria nacional de ciberseguridad es fundamental para desarrollar las capacidades necesarias para hacer frente a los desafíos y amenazas de nuestro ciberespacio especifico. Para ello, será necesario implementar 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, bajo las siguientes premisas:

  1. Distribución de los costes de la ciberseguridad entre todos los actores involucrados, es decir, ciudadanía, empresas y las propias administraciones públicas.
  2. Premiar a las organizaciones comprometidas con la protección de los sistemas de información.
  3. Desarrollar el mercado de productos y servicios de ciberseguridad a través del impulso de la oferta.
  4. Estimular la demanda de herramientas de ciberseguridad por parte de usuarios y organizaciones.
  5. Fomentar la investigación y el desarrollo en soluciones y productos de ciberseguridad.
  6. Estimular la resiliencia de todo el ecosistema que compone el ciberespacio

- **Ciberseguridad Internacional.** El multilateralismo cibernético es esencial. España pertenece a la Unión Europea y la OTAN, donde la ciberseguridad se encuentra entre las principales prioridades políticas. En el caso de la Alianza Atlántica, quizás la lección que mejor han

aprendido es que la limitada regulación, la anonimidad, la apertura, la libertad de acción o la asimetría típicas de este entorno permiten a muchos actores proyectar su poder e influencia enmascarando sus actividades, dificultando la atribución de sus acciones y burlando cualquier hipotética respuesta aliada. Y es que, hoy por hoy, estas actividades tienden a realizarse en la 'zona gris' situada por debajo del umbral del conflicto armado. En el caso de la ciberdefensa aliada, España deberá trabajar en: homogeneizar las ciber-capacidades de los estados miembros y nivelar el nivel de madurez tecnológica, doctrinal u organizativa de los Veintinueve. Es por ello que las Fuerzas Armadas y Fuerzas y Cuerpos de Seguridad del Estado deberán contar con los recursos necesarios para tener un papel relevante en el ámbito internacional (y por supuesto, en el ámbito nacional)

- **Cultura Ciberseguridad**. Para crear esta cultura de la ciberseguridad será necesario poner en marcha un ambicioso plan nación de concienciación como están realizando otros países de nuestro entorno como Estados Unidos o Reino Unido.

Para poder llevar alcanzar los objetivos enumerados en la estrategia nacional de Ciberseguridad será necesario un compromiso presupuestario importante, al igual que están haciendo otros países de nuestro entorno como Francia, Reino Unido o Estados Unidos.

En definitiva, la nueva estrategia supone un importante avance respecto a la de 2019, aunque pone de manifiesto que aún queda mucho trabajo por hacer. El compromiso del gobierno debe materializarse en planes alcanzables en el corto-medio plazo, sustentados estos por una dotación presupuestaria notable. De no ser así, corremos el riesgo de que la estrategia se quede en papel mojado.

Para poder llevar alcanzar los objetivos enumerados en la estrategia nacional de Ciberseguridad será necesario un compromiso presupuestario importante