El GOBIERNO aprueba la Estrategia de Seguridad Nacional 2021 poniendo especial foco en las ciberamenazas y alertando de su incremento

Entre las prioridades del **Gobierno de España** estaba elaborar una nueva Estrategia de Seguridad Nacional. Así, el 28 de diciembre de 2021 se aprobó el RD 1150 que actualiza el anterior documento. La nueva Estrategia consta de cinco capítulos: "Seguridad global y vectores de transformación", "Una España segura y resiliente", "Riesgos y amenazas", "Un planeamiento estratégico integrado" y, por último, "El Sistema de Seguridad Nacional y la Gestión de Crisis". Por supuesto, el ciberespacio y la ciberseguridad son conceptos claves que figuran en ella en varios apartados. Se resalta en la ENS que "la digitalización de todo tipo de actividades ha ampliado la superficie de exposición a posibles ciberataques…" dificultando la protección de la información.

Dos ciberriesgos

En el documento se identifican dos tipologías generales de amenazas en el ciberespacio. Por un lado, los posibles "ciberataques, entendidos como acciones disruptivas que actúan contra sistemas y elementos tecnológicos". Y, por otro, "el uso del ciberespacio para realizar actividades ilícitas, como el cibercrimen, el ciberespionaje, la financiación del terrorismo o el fomento de la radicalización". Y se recuerda el incremento creciente de la superficie de exposición por el teletrabajo y el cercano despliegue de 5G, que multiplicará la capilaridad de las redes y con ello aumentará su uso por personas, el segmento IoT y las comunicaciones M2M. Además, se destaca la importancia de la protección del dato (personal) y las redes en clave de Seguridad Nacional.

Planeamiento estratégico integrado

Frente a estas amenazas, la estrategia marca como uno de los principales aspectos la ciberseguridad y apuesta por impulsar "las capacidades tecnológicas y los sectores estratégicos", además de destacar la importancia de contar con "capacidad preventiva, de detección y respuesta frente a las estrategias híbridas".

TRIBUNA SIC

La ciberseguridad en la ESN 2021

La estrategia de seguridad nacional establece las líneas de acción político-estratégicas para la protección de los intereses nacionales frente a riesgos y amenazas. Las estrategias, por norma, deben revisarse cada cinco años. Sin embargo, el Consejo de Seguridad Nacional consideró conveniente adelantar la revisión de la Estrategia de Seguridad Nacional 2017.

Las razones que aconsejaron este cambio fueron principalmente tres: la primera fue las lecciones aprendidas de la pandemia del Covid-19 que, si bien en origen es de naturaleza sanitaria, ha tenido graves efectos en otros muchos campos como la economía, las cadenas de suministros, la inmigración irregular y la sociedad en general. La segunda razón es el aumento del empleo de las estrategias hibridas por parte de algunos países que contribuyen a la desestabilización de regiones geopolíticas con efectos en el resto de los países; y la tercera razón es la necesidad de afrontar las causas y los efectos del cambio climático.

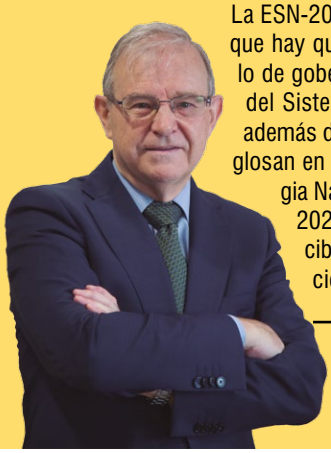
La Estrategia hace hincapié en la integración de la ciberseguridad en el Sistema de Seguridad Nacional con la participación de las CC.AA.

La gestión de la pandemia ha puesto de manifiesto la necesidad de digitalizar y extender el Sistema de Seguridad Nacional a las CC.AA. mediante la digitalización del sistema, lo que debe realizarse mediante una arquitectura que implique la ciberseguridad desde el diseño.

Las estrategias híbridas son capaces de emplear múltiples instrumentos, pero hay dos que son los primeros en ser utilizados: los ciberataques y las campañas de desinformación que aprovechan el potencial de difusión a través del ciberespacio, uniendo el ciberespacio y el espacio cognitivo.

En la ESN-2021 se considera que los riesgos se ven amplificados por la prevalencia de criterios comerciales frente a la seguridad del *hardware* y del *software*. A la hora de analizar las ciberamenazas, se considera que el riesgo también se incrementa por el aumento del perímetro de exposición derivado del teletrabajo y otros cambios de hábitos de los ciudadanos. Por otro lado, el *big data*, la IA y la computación cuántica, implican importantes avances, pero también riesgos para la Seguridad Nacional.

La protección del ciberespacio ya está detallada en su estrategia específica o de segundo nivel: la Estrategia Nacional de Ciberseguridad 2019, con la que se trabaja a buen ritmo y para la que se ha diseñado un Plan Nacional de Ciberseguridad que ya fue presentado en el último Consejo de Seguridad Nacional y está a la espera de su aprobación por el Consejo de Ministros con objeto de conformar una estructura nacional resiliente frente a los ciberataques.



La ESN-2021 plantea en su línea de acción nº 17 que hay que avanzar en la integración del modelo de gobernanza de ciberseguridad en el marco del Sistema de Seguridad Nacional. Y es que, además de las siete líneas de acción que se desglosan en 65 medidas que contempla la Estrategia Nacional de Ciberseguridad 2019, la ESN 2021 hace hincapié en la integración de la ciberseguridad en el SSN con la participación de las CC.AA.

Miguel Ángel Ballesteros
Director
Departamento de Seguridad Nacional – DSN
GABINETE DE PRESIDENCIA DE GOBIERNO