“Ningún Estado miembro de la UE es capaz de protegerse por sus propios medios”

>Por **José de la Peña**
>Fotografía: **Jesús A. de Lucas**

Miguel Ángel Ballesteros

Director General del Departamento de Seguridad Nacional

En junio de 2018, Pedro Sánchez nombró al general del Ejército, Miguel Ángel Ballesteros, Director del Departamento de Seguridad Nacional (DSN) de la Presidencia del Gobierno. Experto en geopolítica, estrategia de seguridad y prevención del terrorismo, este militar de brillante trayectoria y buen conocedor del mundo de los satélites artificiales, está en los centros de decisión de la ciberseguridad española. Nadie mejor que él para enjuiciar el contenido y el alcance de la Estrategia Nacional de Ciberseguridad-ENCS 2019.

– Con la publicación de la ENCS 2019, España ha entrado ya en el club de los países que han revisado sus estrategias de ciberseguridad.

– Cierto. El Consejo de Seguridad Nacional, en su reunión de julio de 2018, presidido por S.M. El Rey, impuso el mandato de revisar la ECSN 2013. Estaba previsto tener el nuevo documento en julio de este año, pero se aceleró su confección para que estuviera listo antes de que finalizara la anterior legislatura. Así pues, la ENCS 2019 se aprobó por el Consejo de Seguridad Nacional el 12 de abril de este año, y se publicó en el BOE 18 días después.

La ENCS 2019 se adapta a la Estrategia de Seguridad Nacional de 2017 (ESN 2017) y a la legislación, especialmente emanada de la UE, como el RGPD y la directiva NIS, al tiempo que incorpora nuevos frentes en el ámbito de la gestión de riesgos, como por ejemplo los de las amenazas híbridas, la desinformación…, que forman parte de las preocupaciones en el escenario internacional.

– ¿Qué destacaría de la ENCS 2019?

– Que es un documento práctico. Para los que la tenemos que ejecutar es casi un guión, que expresa el propósito de proteger a los ciudadanos en el ciberespacio. Para ello, y de forma resumida, se desarrollan 5 objetivos particulares, 4 principios (los mismos que establece la ESN 2017) y 7 líneas de acción.

En la Estrategia se fija el papel de la ciberseguridad en el Sistema de Seguridad Nacional, y se precisa el cometido en la materia de sus integrantes con una filosofía de integración de las entidades y organismos pagados con dinero público, cerca de 600.

La ENCS 2019 establece la creación de un Foro Nacional de Ciberseguridad para estructurar la contribución de expertos y la colaboración público-privada.

– El documento plantea muchos retos. ¿Cuáles destacaría?

– La eficiencia y la proactividad. Y si me apura, la segunda: no podemos ser solo reactivos y defensivos. Hay que ir por delante. O lo conseguimos o nos podemos dar por derrotados.

– Antes mencionaba que la ENCS 2019 es "casi un guión". Pero me da la sensación de que en algunos pasajes es todavía más precisa. Por ejemplo, en el punto 5 de la Línea de Acción 2, se habla directamente del desarrollo del Centro de Operaciones de Ciberseguridad de la AGE.

– La creación del Centro está aprobada en Consejo de Ministros. Pero no se ha puesto en marcha por falta de recursos. Confío en que los próximos presupuestos Generales del Estado habiliten medios para que sea una realidad. Puedo decir que todo está preparado y listo a falta de recursos económicos.

También es verdad que el Centro previsto es modesto para lo que necesita la Administración de un país como España, cuyo peso estratégico global es muy elevado.

Voy a darle unos datos: el centro de ciberseguridad nacional británico, que integra todas las capacidades operativas excepto las de defensa y ciberdelitos, cuenta con cerca de 1.000 personas y un presupuesto aproximado de 1.900 millones de libras para 5 años.

Este es el camino en el que debemos avanzar. Alguien puede pensar que Reino Unido es una potencia mucho más significativa. Sin embargo, la realidad es que en el escenario ciber no nos distinguimos tanto, por lo que es necesario realizar un mayor esfuerzo en recursos humanos y materiales en nuestro país.

– La verdad es que a ciencia cierta no sabemos en España lo que estamos invirtiendo y gastando en ciberseguridad, ni en el sector público ni en el privado, ya a efectos globales ya en detalle.

– La ENCS 2019 pide que se desarrolle una métrica para saber lo que se invierte, lo que se gasta y para saber si los resultados que se vayan obteniendo son los esperados. En base a esta información, además de tener una idea clara de dónde estamos, dispondríamos de información para aplicar mayor o menor esfuerzo presupuestario en algunas áreas.

El Informe de Seguridad Nacional de 2018, aprobado el pasado marzo, se elaboró con la idea de que fuera una herramienta útil para informar a la ciudadanía, al sector empresarial y a los entes más directamente concernidos por los temas de seguridad nacional –que como sabe, comprende 15 ámbitos, uno de los cuales es el de la ciberseguridad–; y por otro lado, un documento adecuado para servir de base al desarrollo de estrategias y políticas.

Por eso, en el Informe no solo se trata lo acontecido en 2018, sino que se introduce un análisis de tendencias en el ámbito de la seguridad digital. Fíjese que en el sector empresarial el informe recoge 102.000 ciberincidentes, de los que más de 700 afectaron a Infraestructuras Críticas. En este frente, el número de incidentes conocidos ha bajado frente a otros años. No así en las administraciones públicas, que han experimentado un crecimiento enorme.

En suma, que establecer una métrica e indicadores a escala nacional nos va a permitir parametrizar, detectar tendencias, crear y ajustar políticas, desarrollar planes, justificar inversiones y darles una continuidad con fundamento.

Sabemos que un buen análisis sobre lo que invierte y gastan las administraciones públicas en ciberseguridad, nos serviría para priorizar acciones y maximizar sinergias en el contexto de nuestro país, que está muy descentralizado. Tenemos que ser aún más eficientes en el uso del dinero público.

– Pero hay cosas que sabemos: por ejemplo, que hacen falta personas expertas en las distintas materias que componen la práctica de la Ciberseguridad.

– Es un problema global que afecta especialmente a Europa. Se calcula que en poco tiempo vamos a dejar sin cubrir en el territorio de la UE medio millón de puestos de trabajo en el ámbito ciber por falta de personal cualificado. La medición del estado del arte nos ha de servir para identificar cuánto personal se va a necesitar y con qué perfiles en base a los derroteros que tome la transformación digital. Tenemos claro que es necesario identificar las necesidades actuales y de futuro para que la formación profesional y la universitaria estén alineadas con las necesidades del sector de ciberseguridad.

– Entidades que dicen representar al sector privado han sugerido a diputados, senadores, instancias gubernamentales y autoridades administrativas la creación de una agencia de ciberseguridad nacional con rango de secretaría de estado, dependiente de Presidencia. La razón principal que aducen es que el reparto de potestades y cometidos entre ministerios y organismos diferentes resulta excesivamente compleja y poco operativa. ¿Qué opina?

– Actualmente disponemos de un sistema de ciberseguridad nacional que está funcionando razonablemente bien y así lo reconocen nuestros socios europeos, pero todo es susceptible de revisión y de mejora.

“Un buen análisis sobre lo que invierte y gastan las administraciones públicas en ciberseguridad, nos serviría para priorizar acciones y maximizar sinergias en el contexto de nuestro país, que está muy descentralizado. Tenemos que ser aún más eficientes en el uso del dinero público”

– La ENCS 2019 prevé la creación de un Foro Nacional de Ciberseguridad. Cuando se constituya será el espacio en el que se analicen los pros y contras de esta y de otras propuestas que pudieran surgir.

Además, en el último capítulo del documento, dedicado al Sistema de Seguridad Nacional, se habla de mejorar la integración de todos los organismos públicos dedicados a la ciberseguridad. Si unimos las propuestas a las que se ha referido usted y esta indicación estratégica de integración que acabo de expresar, en algún momento estaremos en disposición de saber si es útil crear una Agencia o hay otras fórmulas más beneficiosas.

– ¿Cuándo está previsto poner en marcha el Foro Nacional de Ciberseguridad?

– Como le decía, hay que crearlo y definir los requisitos que habrán de cumplirse para formar parte de él. Al tiempo, hemos de establecer sus relaciones con el resto de componentes del Sistema de Seguridad Nacional.

Como norma general, las estrategias nacen con horizontes de 10 años; pero a los 5 años se tienen que revisar. En el caso de la de ciberseguridad, estos tiempos se acortan notablemente, pudiéndose llegar incluso al año, porque la velocidad de cambio es enorme.

Tenemos previsto constituir el Foro y convocar su primera reunión en poco tiempo. Para la ciberseguridad es muy relevante, porque será el ente en el que se institucionalice a escala estratégica la colaboración público-privada. En el campo de la seguridad digital, sin CPP no es posible gestionar los riesgos.

– Parece claro que a usted la ENCS 2019 le parece inmejorable…

– Todo se puede mejorar; pero me parece un excelente documento gubernamental. Hasta donde llegan mis responsabilidades como Director General del Departamento de Seguridad Nacional voy a potenciar su desarrollo y aplicación.

Los informes de Seguridad Nacional nos irán marcando en qué grado se van alcanzando los objetivos marcados en la ENCS e incluso servirán para valorar si resulta conveniente proponer al Consejo de Seguridad Nacional que se revise la Estrategia.

– ¿Es partidario de reconocer la figura del CISO o del responsable de Seguridad Digital y sus funciones en empresas concernidas por las legislaciones PIC y NIS, entre otras?

– En las grandes empresas el CISO existe. Y en el ENS existe una figura reconocida. Con independencia de cuál pueda ser mi opinión personal al respecto, la ENCS, en tanto que documento gubernamental, no es el lugar para reconocer o no la figura y la función, ni para decir a las organizaciones cómo tienen que organizar la gestión de la ciberseguridad.

Más bien creo que el ámbito para reflejar esto, si procede, es el de la legislación NIS, y en la confluencia posible NIS-PIC. Como sabe, la directiva NIS hubo que transponerla de urgencia a la legislación española mediante un Real decreto-ley, cuyo desarrollo reglamentario está pendiente. Será, por tanto, en la actual legislatura, cuando se concrete este re-

glamento y otros asuntos.
No obstante, teniendo la UE un entorno NIS y siendo España una de las potencias destacadas de la UE, parece razonable que avancemos en la armonización europea, también en la regulación de la figura del CISO.

– ¿No le inquieta la dependencia tecnológica tan acusada que en el ámbito digital tiene la UE y particularmente España?

– Mucho. Por eso como país estamos apoyando al máximo todas las acciones de Europa en hardware, software, certificación de productos, sistemas y servicios, I+D+i, ciberseguridad industrial... Tenemos ahora el 5G, que ha metido de lleno a la ciberseguridad en las tensiones de la guerra comercial.
Solo hay una forma de alcanzar protección real: tener tu propia industria y ser autónomo en la certificación y el desarrollo tecnológico.

– El mes pasado, el Consejo Europeo decidió establecer un marco para imponer medidas restrictivas concretas para disuadir y contrarrestar ciberataques con repercusiones importantes que supongan una amenaza exterior para la UE o sus Estados miembros. ¿Cómo enjuicia esta iniciativa?

– La iniciativa, importantísima, alcanza incluso a los ciberataques y el uso ilícito del ciberespacio con fines de desinformación. Es legítimo utilizar todas las herramientas que nos brinda la ley para hacer frente a hechos malintencionados y hostiles de autoría probada. El ciberespacio es una pieza clave para que los Estados miembros de la UE, en vez de renacionalizar capacidades y potestades, profundicen en la integración. Cada país, por sus propios medios, no puede protegerse.

– Israel bombardeó hace poco un edificio palestino en el que, según indicó, se armaban ciberataques contra su país.

"La intención es crear cuanto antes sea posible el Foro Nacional de Ciberseguridad. Para ello tenemos que definir los requisitos que habrán de cumplirse para formar parte de él y, al tiempo, establecer sus relaciones con el resto de componentes del Sistema de Seguridad Nacional"

– El caso de Israel es muy particular, porque su entorno es hostil. Y a la historia me remito.
El problema que se plantea aquí es probar la autoría de un ciberataque y poder atribuirlo de forma legal a un estado, a un gobierno o a un colectivo organizado, aunque lo haya ejecutado materialmente otra entidad. Ante esta dificultad, hay algunos países que están hablando ya de atribución política. Es un asunto complejo. Como dice el general Valeri Guerásimov, actual Jefe del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia: es muy barato ciberatacar y muy difícil atribuirlo.

– ¿Tenemos bien organizada la ciberdefensa militar española?

– Aunque soy general, la competencia en este particular es del JEMAD. Pero ya que me pregunta le diré que la tenemos bien organizada, y eso que sus estructuras, por ejemplo el MCCD, son jóvenes. Como en todo, sería deseable un mayor esfuerzo presupuestario para la ciberdefensa militar y, en conjunto, para la defensa militar.

– Pero, ¿estamos a la altura de las capacidades de los países de nuestro entorno geopolítico?

– Todo es mejorable. Eso hay que irlo consiguiendo cada día. En defensa y en ataque.

– Una última pregunta: ¿tienen todas las estructuras de la ciberseguridad nacional buena sintonía con la Agencia Española de Protección de Datos?

– Colaboramos estrechamente: notificaciones de ciberataques, denuncias... Tenga en cuenta que en un alto porcentaje de incidentes, media la exposición de datos personales. ■

"La creación del SOC para la AGE está aprobada en Consejo de Ministros. Pero no se ha puesto en marcha por falta de recursos. Confío en que los próximos Presupuestos Generales del Estado habiliten medios para que sea una realidad. Puedo decir que todo está preparado y listo a falta de recursos económicos"