El sector de la ciberseguridad en España: pasar de la filosofía a las matemáticas

Félix Arteaga | Investigador principal de Seguridad y Defensa, Real Instituto Elcano.

Si a quienes siguen las estrategias, políticas y documentos oficiales de ciberseguridad en España se les pidiera que cerraran los ojos y nos dijeran qué ven, si letras o números, seguramente coincidirían en que lo primero. Tanto en la Estrategia Nacional de Ciberseguridad como en los Informes Anuales de Seguridad Nacional se suceden los objetivos y las acciones escritos sin indicadores que fijen el estado o el nivel de avance sobre esos objetivos. Facilitan una historia cualitativa, de dónde estamos o hacia dónde nos movemos, pero no cuantitativa, para saber cuánto hemos progresado y cuánto queremos progresar.

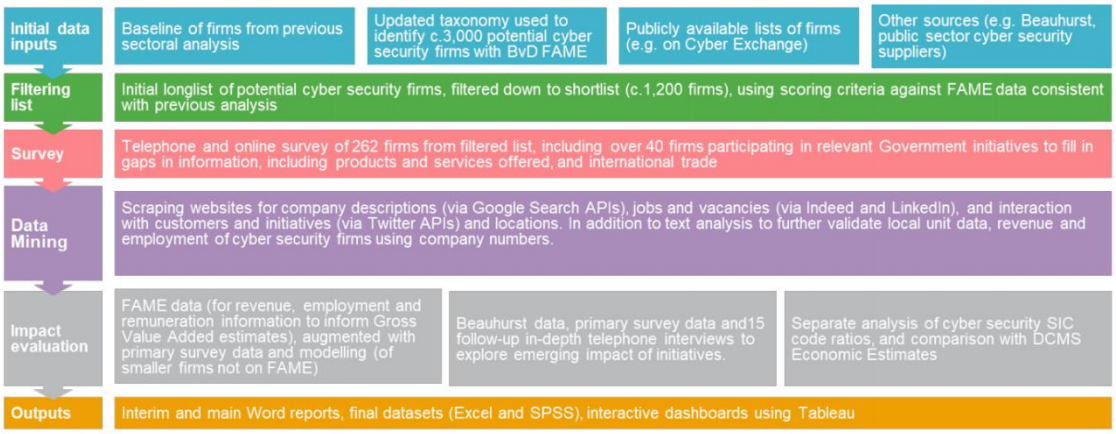
Si acaso, podemos observar una excepción estadística en los informes sobre "Ciberamenazas y Tendencias" que elabora el CCN-CERT todos los años, donde se incluyen datos numéricos por sectores sobre ciberincidentes, vulnerabilidades y tendencias de riesgo, de elaboración propia o recogiendo la de instituciones y consultoras internacionales. También se pueden consultar los datos desagregados sobre empresas del sector, como los del catálogo de 2020 del Centro de Ciberseguridad Industrial, o informes agregados como el de "Tendencias en el mercado de la ciberseguridad" del Incibe de 2016.

La limitada disponibilidad de datos cuantitativos responde, por un lado, a la relativa inmadurez del sector para conocer la relación entre inversiones e impacto y elaborar métricas que permitan evaluar la progresión hacia los objetivos que se señalan. Pero, además de la dificultad técnica, la falta de indicadores revela la renuencia de las Administraciones Públicas a facilitar indicadores que permitan calificar su gestión. Reconociendo la dificultad, la Estrategia Nacional de Ciberseguridad del Reino Unido 2016-2021 también admite la necesidad de elaborar una métrica que permita evaluar el estado del sector de la seguridad y adoptar políticas basadas en datos.

"La limitada disponibilidad de datos cuantitativos responde a la relativa inmadurez del sector para conocer la relación entre inversiones e impacto y elaborar métricas que permitan evaluar la progresión hacia los objetivos que se señalan".

A los lectores les propondría hojear el documento del Reino Unido que incluimos en el *CIBER elcano* de marzo "UK Cyber Security Sectorial Analysis 2020". Es una encuesta encargada por el Ministerio de Digital, Cultura, Medios de Comunicación y Deporte del Reino Unido para cuantificar el estado del sector de la ciberseguridad nacional a medio camino de la ejecución de la Estrategia (2019), una encuesta como varias otras que se llevan a cabo para objetivar la evaluación de las políticas públicas y que realizan instituciones independientes (en la Figura 1 se señalan la metodología y los autores).

Figura 1. Metodología de investigación



Fuente: Ipsos MORI, "Perspective Economics and the Centre for Secure Information Technologies" (2019).

Gracias a esta encuesta, el Centro Nacional de Ciberseguridad del Reino Unido (NCSC) dispone de datos como los que se enumeran a continuación para 2019. El sector cuenta con 1.221 empresas activas, 375 más que en 2017 (44%), y cada semana se añade una nueva empresa al sector. De ellas, el 90% son pymes que facturan anualmente 2.000 millones de libras (el 24% de las ganancias del sector). El sector da empleo a 43.000 profesionales, la mayoría (65%) en las grandes empresas, y el empleo crece a un ritmo acelerado (37% entre 2017 y 2019).

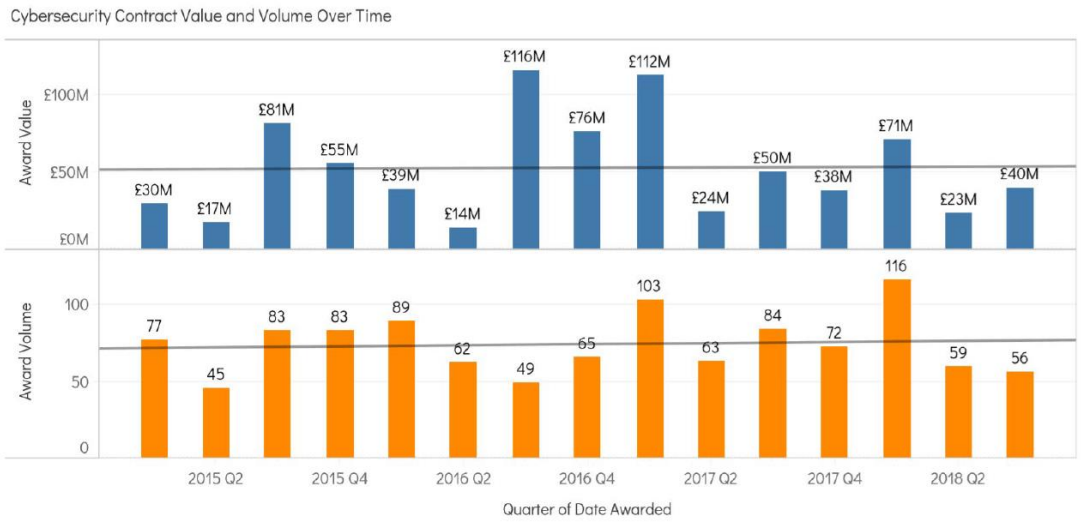
Empresas y empleados generaron unos 8.300 millones de libras anuales en 2019, con un incremento de 2.600 millones respecto a 2017 (46%) y un aumento de ingresos por empleado de casi 200.000 libras (7%). Descontados los costes, el valor agregado bruto del sector en 2019 llegó a 3.770 de los 8.300 millones, un 60% más que en 2017, lo que significa que se añade cada vez más valor por empresa y empleado (17% en este caso).

La encuesta muestra la importancia de los distintos subsectores del negocio: servicios profesionales (71%), inteligencia y análisis de riesgos (46%) y seguridad de terminales (37%), con un aumento significativo de indicios de crecimiento en los subsectores de sistemas de control industrial, criptografía, poscuántica o IoT. A estos datos, necesarios para orientar las estrategias del sector, se añade el análisis de las tendencias de riesgo y mercado. En conjunto, la encuesta permite tener una idea agregada del volumen de negocio y el procesamiento de los datos permite elaborar un mapa del sector dentro y fuera del Reino Unido, lo que visualiza su posición en el mercado mundial y su proximidad a los ecosistemas de investigación, desarrollo y tecnología. También permite conocer el destino y flujo de las inversiones en el sector, tanto por región como por tamaño, y las fuentes de financiación, así como el estadio de evolución y la valoración de cada empresa (dentro de un valor total estimado para todas ellas de 4.000 millones de libras, sólo una compañía, Darktrace, tiene dimensión de "unicornio" con un valor de 1.200 millones de libras).

Finalmente, la Figura 2 da una idea del interés inversor público en el sector presentando la cantidad (naranja) y el valor (azul) de la compra pública. El esfuerzo de trasparencia contable permite, por ejemplo, constatar que sólo una de cada cinco libras del

presupuesto público llega a las pymes cuando se pretendía que fuera una de cada tres (en 2022), a lo que hay que añadir los fondos para programas específicos de formación o apoyo al desarrollo del sector.

Figura 2. Contratación pública del Reino Unido en ciberseguridad según cantidad y valor



Fuente: UK Cyber Security Sector Analysis, p. 49

Conclusiones para España

Las políticas públicas en la era digital pueden y deben basarse en datos. Y al desarrollo de las dimensiones de seguridad y gobernanza deben seguir las de naturaleza económica, industrial y comercial del sector de la ciberseguridad. Encuestas como la mencionada del Reino Unido proporcionan una aproximación al estado y perspectivas del sector que ayudan a diseñar políticas y a tomar decisiones tanto en el sector público como en el privado.

“Sin capacidad de obtención y procesamiento de datos, nuestro sector de la ciberseguridad no podrá competir con otros como el del Reino Unido”.

Sin capacidad de obtención y procesamiento de datos, nuestro sector de la ciberseguridad no podrá competir con otros como el del Reino Unido, que disponen de mayor capacidad de inteligencia sobre el mercado de la ciberseguridad. Tanto el sector público como el privado tienen la responsabilidad de paliar esa carencia. Mejor en colaboración, como muestra la encuesta del Reino Unido, que por separado y sin liderazgo, como hasta ahora, una recomendación que reenvío al recién aprobado Foro Nacional de Ciberseguridad. En el sector de la ciberseguridad, los datos valen más que las palabras, por lo que hay que pensar en pasar de la filosofía a las matemáticas.