Capítulo 3 SEGURIDAD DIGITAL

3 SEGURIDAD DIGITAL

Comunicación y seguridad digital
Teoría de números y aplicaciones criptográficas

JULIO MIRAVALLS

La criptografía nació con el fin de asegurar la comunicación confidencial entre dos sujetos, sin que terceros fueran capaces de conocer el contenido del mensaje, incluso aunque tuvieran acceso a él, enmascarándolo mediante claves secretas sólo conocidas por los dos interlocutores legítimos.

Se identifican formas primitivas de criptografía con 25 siglos de antigüedad, usadas en la guerra, para enviar mensajes que, aunque fuera capturado su portador, no podían ser descifrados por el enemigo. El procedimiento básico de encriptación consiste en reemplazar los caracteres que componen un mensaje por otros códigos que lo hacen ininteligible sin conocer la clave de sustitución.

La vieja criptografía, utilizada también en la política y en operaciones comerciales desde tiempos antiguos, podía apoyarse en codificaciones preestablecidos, o en artefactos singulares, compartidos por emisor y receptor del mensaje y utilizados para encriptar y desencriptarlo. La evolución ha llevado a una criptografía moderna que usa las tecnologías digitales y está completamente sustentada por las matemáticas.

En un mundo interconectado y dominado por internet, las comunicaciones privadas a través de correo electrónico y aplicaciones de mensajería instantánea, las transacciones comerciales y la comunicación de los ciudadanos con las administraciones se basan en la confianza de que el vehículo digital que las transporta preserva la privacidad del mensaje. O que, si es interceptado, como podía ocurrir en el caso del antiguo mensajero, el contenido permanecerá a salvo de ojos indiscretos.

Para ello se usan contraseñas de identificación que creemos seguras, aunque de tanto en tanto, demuestran no serlo, por la capacidad de los *hackers* para desentrañarlas, por falta de seguridad en la custodia de entidades con las que se mantiene una comunicación, o incluso por la venta fraudulenta.

La teoría de números lleva al menos 40 años proponiendo métodos más seguros para establecer las claves de seguridad que la improvisación individual. En el año 1979 tres profesores del MIT, Ron Rivest, Adi Shamir y Leonard Adleman, crearon el algoritmo RSA de clave pública. Las siglas que lo denominan son las iniciales de sus apellidos.

El algoritmo RSA está basado en la descomposición de un número en sus factores primos. Desde entonces la criptografía se ha pasado a métodos más sofisticados como las curvas elípticas, pasando antes por el sistema de logaritmo discreto de ElGamal.

La seguridad del mecanismo RSA, como en los ejemplos de antigua criptografía citados, se basa en que sólo los extremos de la comunicación deben tener acceso a los números primos en los que se basa la codificación del mensaje. De hecho, sólo el receptor del mensaje gestiona las dos claves que se utilizan en la operación, una privada y otra pública. Con la clave pública, compartida con el emisor, se encripta para su transporte el mensaje, que ya sólo puede ser descifrado después con la clave privada del receptor. Ni siquiera el emisor puede hacerlo. Los números primos utilizados son elegidos de manera aleatoria y las claves tienden a ser extremadamente largas. Difíciles de manejar.

El sistema de ElGamal, publicado por Taher ElGamal en 1984, se basa en el problema matemático de calcular el logaritmo discreto de un número primo, elegido aleatoriamente, con el que se genera la clave de cifrado.

La criptografía asimétrica de curvas elípticas (ECC), propuesta en 1985 por dos matemáticos que trabajaban por separado (Neal Koblitz y Victor Miller), aplica un modo de operar similar a RSA, con una clave pública para el intercambio del mensaje y otra privada para descifrarlo. Pero en este caso, la encriptación se basa en un procedimiento matemático para definir mediante una ecuación tres puntos, que son coordenadas en números enteros, de una curva definida sobre un cuerpo finito (el tercer punto es la suma de los dos primeros). La clave se establece con el logaritmo discreto en curvas elípticas del tercer punto. Es más corta que las que producen los métodos anteriores, aunque también extremadamente difícil de desentrañar.

EL PAPEL DE ESPAÑA

El nuevo mundo digital es un territorio de insospechadas oportunidades y posibilidades económicas, a la vez que una amenaza para las vidas privadas de los individuos y la seguridad de la sociedad. Conjugar ambos aspectos crea una industria de ciberseguridad y una necesidad y oportunidad complementaria para el desarrollo de todas las restantes actividades digitalizadas.

La seguridad, basada en el conocimiento y en la tecnología, es un elemento en continua evolución, para el que en el futuro aparece como una amenaza, y a la vez una esperanza, la computación cuántica.

Las tecnologías presentes en la seguridad están basadas en matemáticas, un bien de los que se denominan a veces 'bien público de club': un teorema, una vez demostrado, puede ser usado por cualquiera. Aunque, para hacerlo, hace falta una preparación.

Ahí reside la oportunidad: desarrollar tecnología en seguridad y criptografía. Hay campo para la inversión pública y para iniciativas privadas corporativas y de emprendimiento. España, con jóvenes bien formados en matemáticas, puede conseguir un desarrollo tecnológico importante en una actividad que, fundamentalmente, precisa de materia gris. •

CON DATOS EN LA MANO

#3 Seguridad digital y criptografía

ANDRÉS VALDÉS

Si la digitalización es la expansión virtual de las actividades de una organización, la ciberseguridad es el techo y las paredes que cubren esas nuevas superficies. Lo que ocurre ahí dentro simplemente no puede quedar expuesto y es necesario proteger, con diferentes niveles y capas de seguridad, el funcionamiento ordinario de empresas, administraciones y hogares. La arquitectura física de nuestro mundo tiene traducción informática: Fabricantes de muros, puertas y llaves, así como los delincuentes que se dedican a violarlos, tienen homólogos virtuales.

El valor del mercado global de ciberseguridad ronda los 133.000 millones de dólares, pero, en el futuro cercano, la demanda de tecnología para protegerse de cibertaques estará cerca de duplicar esta cifra, con una facturación de 244.400 millones en 2024[1]. La mayor confianza en la digitalización, y dependencia, de las empresas, así como las cada vez más exigentes regulaciones de protección de datos de consumidores y clientes explican la proyección de la ciberseguridad. Finanzas, energía e industria son los objetivos principales de los delincuentes. (Fig. 1)

Parte de este incremento se apoya en los cada vez mayores presupuestos de ciberseguridad, con una previsión de aumento del 34% para este año respecto del anterior. Los mayores refuerzos se producen en industria pesada, finanzas, sanidad y en el propio sector de la tecnología[2].

La necesidad de proteger nuestro contenido y redes digitales impulsa la compra de soluciones y la contratación de personal en las empresas capaces de enfrentar amenazas cada vez más sofisticadas. La experiencia y la inversión en seguridad de sistemas ha preparado a las industrias contra los ataques sencillos, de manera que ya no son las brechas de ingeniería social o los ataques masivos dirigidos a empleados, normalmente poco preparados para estos incidentes, lo que preocupa a los directores de seguridad. El cibercrimen profesional, los *hackers* al servicio de Estados y los *insiders* con acceso a sistemas críticos[3] son las amenazas más serias según indican distintas organizaciones. Cada año, estos ataques arrancan el 0,8% del PIB mundial[4].

La expansión de las tecnologías en nube y del Internet de las Cosas no facilita la labor. En concreto, las empresas creen que las zonas más vulnerables de su edificio digital son la TI invisible, las redes móviles, los servidores de correo electrónico, los dispositivos de los empleados y las tecnologías emergentes, donde el IoT aparece como la mayor preocupación en cuestiones de seguridad[5]. Consecuentemente, el 70% de las brechas se localizan en los dispositivos *endpoint* o de punto final[6]. Para protegerlos, las herramientas más habituales son la encriptación de los datos -por lo que la información interceptada no es de ningún uso para los atacantes-, la detección y respuesta *endpoint* y las actualizaciones constantes de parches.

La encriptación sostiene todos los negocios en internet. El intercambio de información que necesariamente debe salir de los puntos finales de los sistemas y llegar a los puertos de los receptores se cifra para evitar que caigan en las manos equivocadas. En sanidad y finanzas, la protección de ficheros personales es imperativo legal, de la misma forma que los servicios de pago por internet cumplen con estándares exigentes para que los datos bancarios o la dirección del cliente esté asegurada contra ciberasaltos.

1 *Global Cybersecurity Market Forecasts, 2019-2024.* Business Wire, 2019

2 *The Cybersecurity Imperative Pulse Report.* ESI Thoughtlab, 2019

3 idem

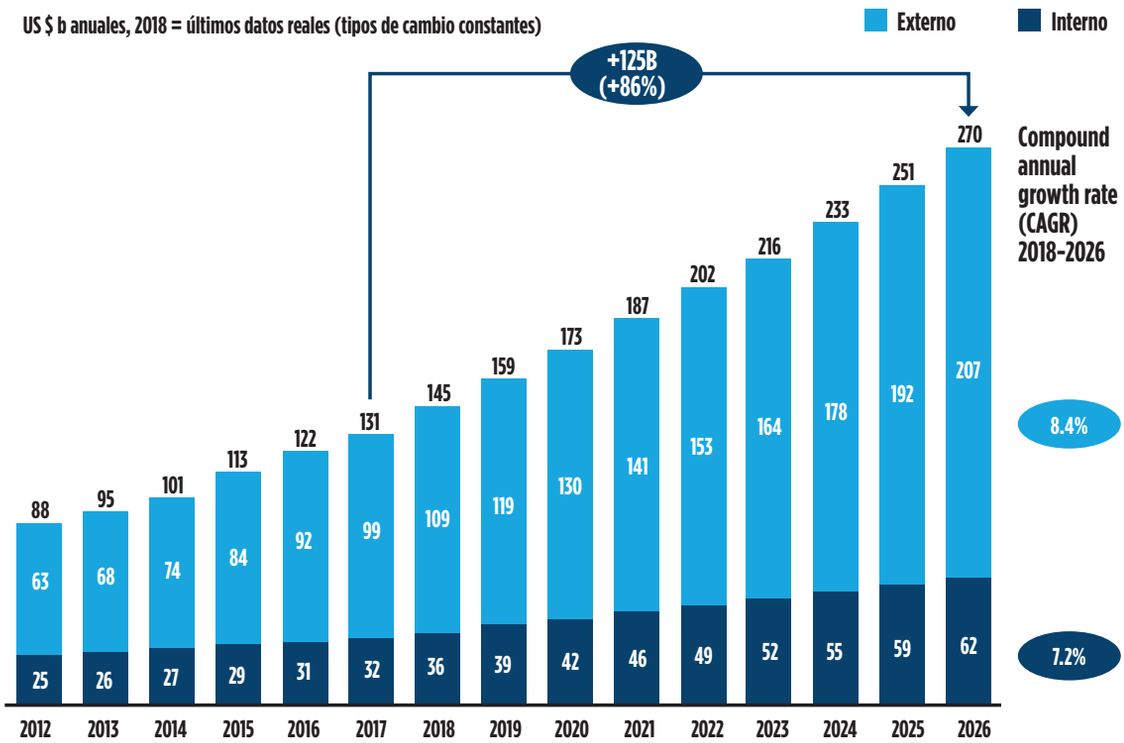
4 *Panorama actual de la Ciberseguridad en España.* Google, 2019

5 *The Cybersecurity Imperative Pulse Report.* ESI Thoughtlab, 2019

6 *2019 Endpoint Security Trends Report.* Absolute, 2019

Fig. 1 **GASTO GLOBAL EN CIBERSEGURIDAD**

Gasto hasta 2019 y proyección en soluciones de seguridad para prevenir brechas dentro de las organizaciones (internas) y amenazas externas.



Fuente: AustCyber, 2019

Asimismo, la operativa de la industria farmacéutica y tecnológica blinda con sistemas de cifrado su investigación para protegerla del espionaje industrial[7]. El coste de imagen, el riesgo de demandas de clientes y las pérdidas económicas causada por un ataque exitoso -148 dólares por cada registro confidencial robado[8]- son razones suficientes para que el resto de sectores invierta en sistemas de cifrado de archivos. El 53% de los ataques causa daños de más de medio millón de dólares[9]. (Fig. 2)

La encriptación es, al igual que las cajas fuertes en el mundo físico, la capa final de seguridad que previene del uso ilegítimo del contenido en caso de que el resto de medidas –cortafuegos, *software antimalware* y prevención de intrusiones- fallen. Existen dos estándares principales en función del destino de la información protegida. En el caso de que la información vaya a ser intercambiada con terceros se utiliza fundamentalmente el sistema de clave pública y clave privada, o asimétrico, basado en el algoritmo RSA.

Si el objetivo es blindar archivos almacenados, es más habitual recurrir al Advanced Encryption Standard-256 (AES-256)[10].

El cifrado RSA ha resistido 40 años de ataques con éxito, por lo que se ha convertido en el algoritmo base para encriptar las comunicaciones más sensibles de la red. Sin embargo, hace décadas que se demostró que la computación cuántica es potencialmente capaz de resolver las claves que abren el candado criptográfico RSA, por lo que la estabilidad de las transacciones *online* está amenazada por los ordenadores que operan con *cubits* y no con *bits*[11]. Un ordenador cuántico podría descifrar el RSA-1024, un popular algoritmo de cifrado, en cuestión de horas[12]. La amenaza cuántica sigue firme mientras el porcentaje de páginas de internet que incorpora un

7 *What is Endpoint Encryption?* McAfee, 2020

8 *2018 Cost of a Data Breach Study: Global Overview.* Ponemon Institute, 2018

9 *Informe de Ciberseguridad Anual.* Cisco, 2018

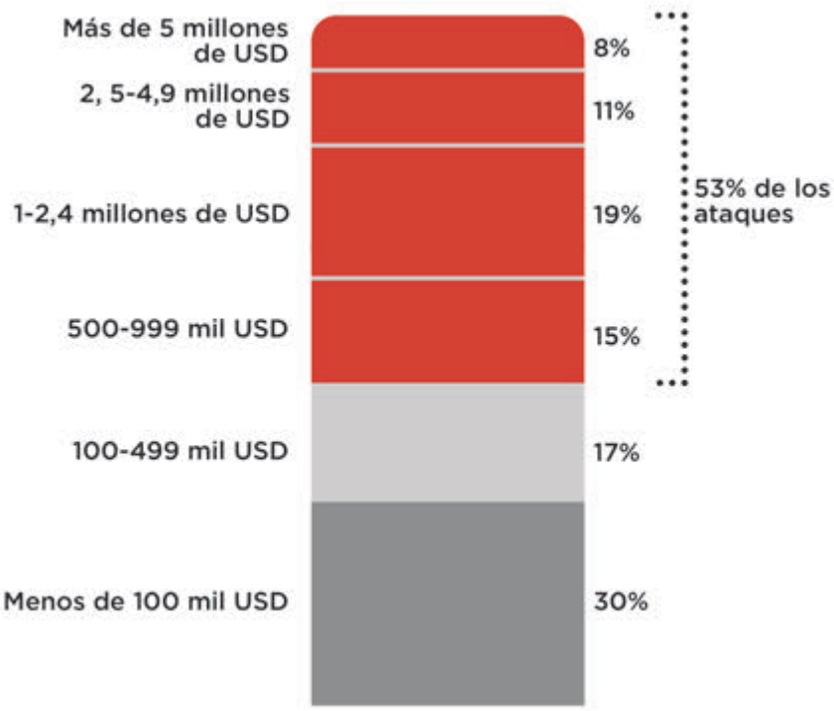
10 *What is Endpoint Encryption?* McAfee, 2020

11 *RSA Encryption – Keeping the Internet Secure.* American Mathematical Society, 2014

12 *Los ordenadores cuánticos, una futura amenaza para la ciberseguridad.* MIT Technology Review, 2018

Fig. 2 COSTE DE LAS BRECHAS DE SEGURIDAD PARA LAS ORGANIZACIONES

Más de la mitad de los ataques suponen pérdidas superiores a los 500.000 dólares.



Fuente: Cisco, 2018

certificado de encriptación simétrica o asimétrica se acerca al 100%[13].

Se prevé que gobiernos y grandes empresas tengan acceso a esta revolucionaria forma de computación a lo largo de la presente década[14], un nuevo mercado que tendrá un valor estimado de 10.000 millones de dólares en 2024[15]. Los actores ya se preparan para este gigantesco reto de seguridad aumentando la complejidad de los cifrados simétricos e invirtiendo en soluciones post-cuánticas. El encriptado en retícula o enrejado, el cifrado basado en Teoría de Código o las firmas digitales de *hashes*[16], entre otros, son los sistemas más populares de la naciente ciberseguridad post-cuántica. El valor de este sector alcanzará los 759 millones de dólares en 2025[17]. (Fig. 3)

A escala global, el segmento del *software* de criptografía registró un valor global de 6.820 millones de dólares en 2019, pero el impacto de la computación cuántica y las necesidades de protección extra que reclaman el IoT y la operación en nube impulsarán la facturación de este nicho hasta los 22.740 millones en 2027[18].

La ciberseguridad representa una gran oportunidad y también una necesidad para nuestro país, que presenta un importante contraste entre el desarrollo que alcanza el área en el ámbito de la investigación y la administración frente al tejido empresarial.

El pequeño tamaño de la gran mayoría de nuestras empresas es la causa de que el 99,8% de ellas consideren que no son un objetivo deseable para los ciberdelincuentes, por lo que el grado de concienciación y preparación contra intrusiones es bajo[19]. Sin embargo, y debido precisamente a su menor protección, las pymes y los particulares son los objetivos principales de los ciberataques. En 2018 se registraron 102.000 incidentes en España, la mayoría lanza-

13 *Panorama actual de la Ciberseguridad en España.* Google, 2019

14 *The Impact of Quantum Computing on Cybersecurity.* Okta, 2019

15 *Wielding a double-edged sword. Preparing cybersecurity now for a quantum world.* IBM, 2018

16 idem

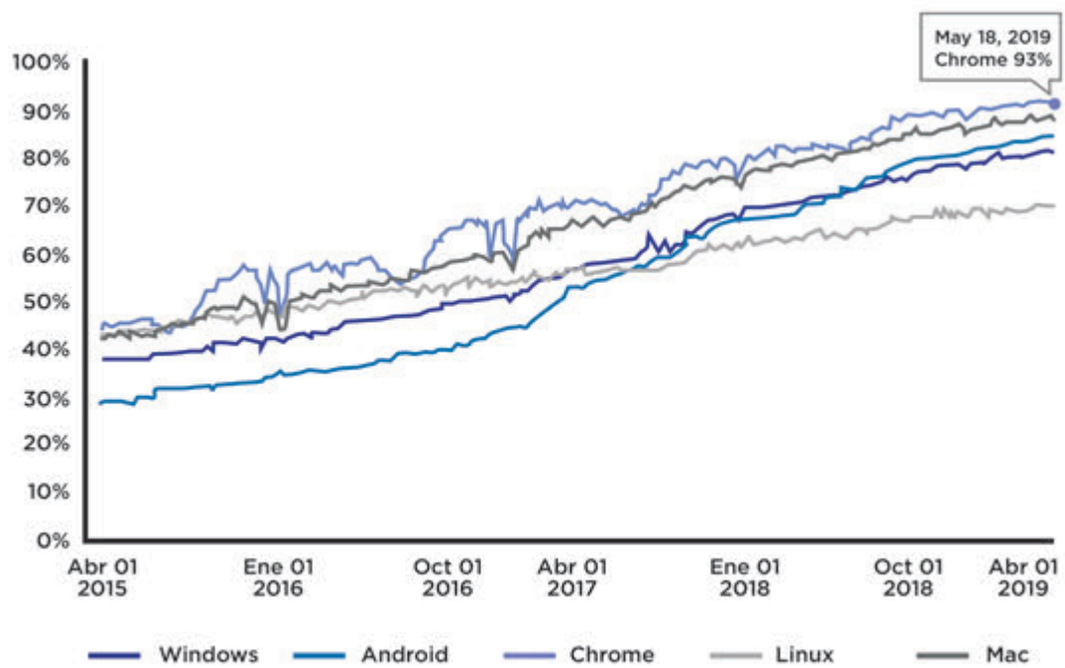
17 *Global Quantum Cryptography Market is Expected to Reach USD 759.51 Million by 2025: Fior Markets.* Globe Newswire, 2019

18 *Global Encryption Software Market. Opportunities and Forecast 2020-2027.* Allied Market Research, 2020

19 *Ciberseguridad: el sector que va a necesitar 350.000 empleos en tres años.* El Mundo, 2020

Fig. 3 **PÁGINAS CARGADAS CON CERTIFICADO DE SEGURIDAD**

Porcentaje de páginas con protocolo HTTPS en Chrome, por plataformas.



Fuente: Google 2019

dos contra estos pequeños usuarios. Cuando la brecha tiene éxito, el coste medio para la víctima ronda los 35.000 euros. Apenas un 40% de los negocios de este tamaño logra sobrevivir a las consecuencias del ciberataque[20].

El conjunto de las empresas españolas están por debajo de la media europea en el *ranking* de ciberseguridad elaborado por la consultora BitSight, al mismo nivel que Portugal e Italia y por debajo de Francia, Alemania y Reino Unido[21].

A pesar de las oportunidades que ofrece el mercado, las empresas que buscan incorporar profesionales a sus líneas de defensa encuentran problemas para encontrar especialistas en ciberseguridad[22], una situación que se da en el 40% de las compañías del país con reclutamientos abiertos en esta área. Nuestro país tiene una tasa de profesionales de las tecnologías de la Información y la Comunicación inferior al 3% de la fuerza de trabajo. Es además un colectivo muy masculinizado[23].

Sin embargo, la robusta estructura legal levantada en los últimos años en el país -que aglutina la transposición de la normativa de provisión y notificación de incidentes, la Ley de Protección de Datos y la Estrategia Nacional de Ciberseguridad-, es terreno fértil para que crezca la demanda de soluciones de seguridad TIC[24]. La suma de iniciativas legislativas, de difusión, técnicas y organizacionales del país, recogidas por la Unión Internacional de Telecomuncaciones en un indicador compuesto que permite comparar el grado de compromiso de los estados con este campo, coloca a España dentro de los diez países del mundo con mayor proyección en ciberseguridad[25].

En investigación académica, el país cuenta con más de un centenar de centros asociados a la Red de Excelencia Nacional de Investigación en Ciberseguridad

20 *Panorama actual de la Ciberseguridad en España.* Google, 2019

21 *Estado de la Ciberseguridad de las empresas españolas.* Telefónica, 2017

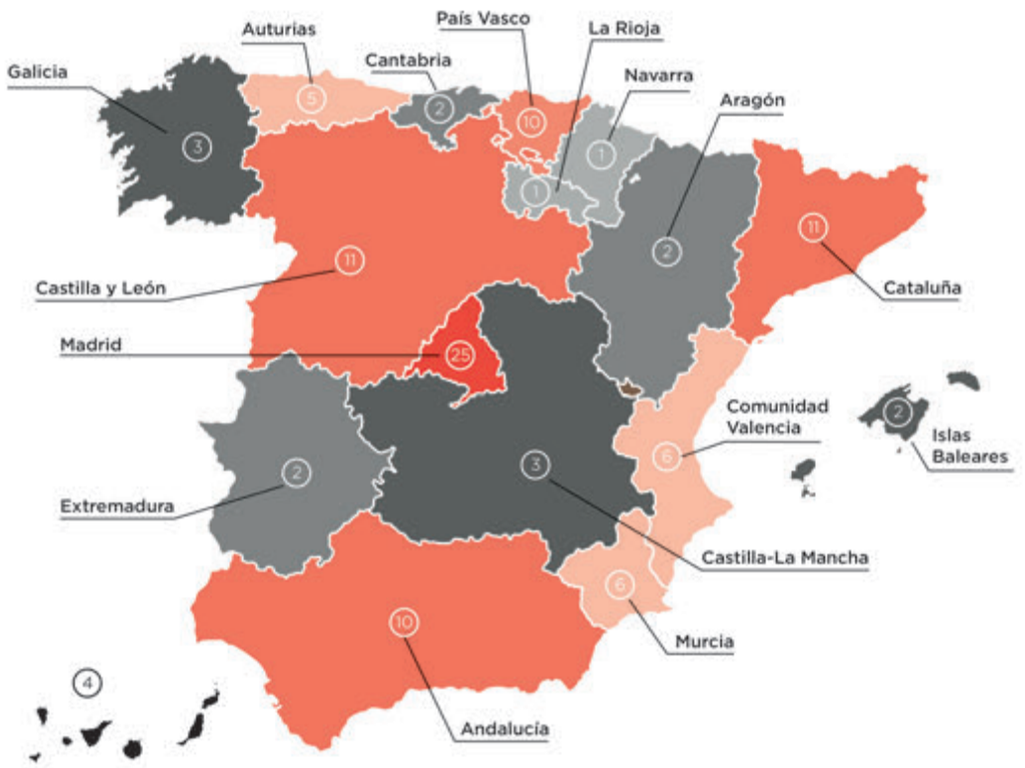
22 *Instantánea del estado actual de la ciberseguridad en España.* Xataka, 2018

23 *Panorama actual de la Ciberseguridad en España.* Google, 2019

24 idem

25 *Global Cybersecurity Index (GCI).* UIT, 2018

Fig. 4 ¿CUÁNTOS EQUIPOS DE INVESTIGACIÓN EN CIBERSEGURIDAD HAY EN ESPAÑA?



Fuente: Google 2019

ridad[26]. El país alberga el tercer clúster público-privado de centros de I+D+i en este área más relevante de Europa[27]. (Fig. 4)

En 2018, el sector alcanzó en España un valor de 1.200 millones de euros, un 11,6% más que el año anterior. Se trata de un mercado dominado por la consultoría TIC, que representa alrededor del 70% de la facturación. Las soluciones de *software* y *hardware* agrupan el resto de las ventas[28].

En cualquiera de sus variantes, el sector tiene posibilidades de expansión a lo largo de toda la transformación digital de España. Gobernanza, movilidad, servicios financieros y seguros, industria y medio ambiente son mercados verticales en los que se despliegan nichos como ciberresiliencia para infraestructuras críticas, protección de industrias inteligentes y redes eléctricas distribuidas, seguridad *fintech* y detección de fraude y otras actividades que cubren la digitalización de la sanidad y la educación[29].

La cultura de ciberseguridad logra, poco a poco, calar en un usuario cada día más consciente de los riesgos que implica su expansión personal y profesional por el ciberespacio. De su capacidad para acompañarle y hacerle sentir seguro dependerá que el miedo no frene su voluntad por construir una vida digital aún más importante. •

26 *Panorama actual de la Ciberseguridad en España.* Google, 2019

27 *Cibersecurity Competence Survey.* CE, 2108

28 *El mercado de ciberseguridad en España crecerá por encima del 10%.* IT Security, 2019

29 *Tendencias en el mercado de la ciberseguridad.* Incibe, 2016