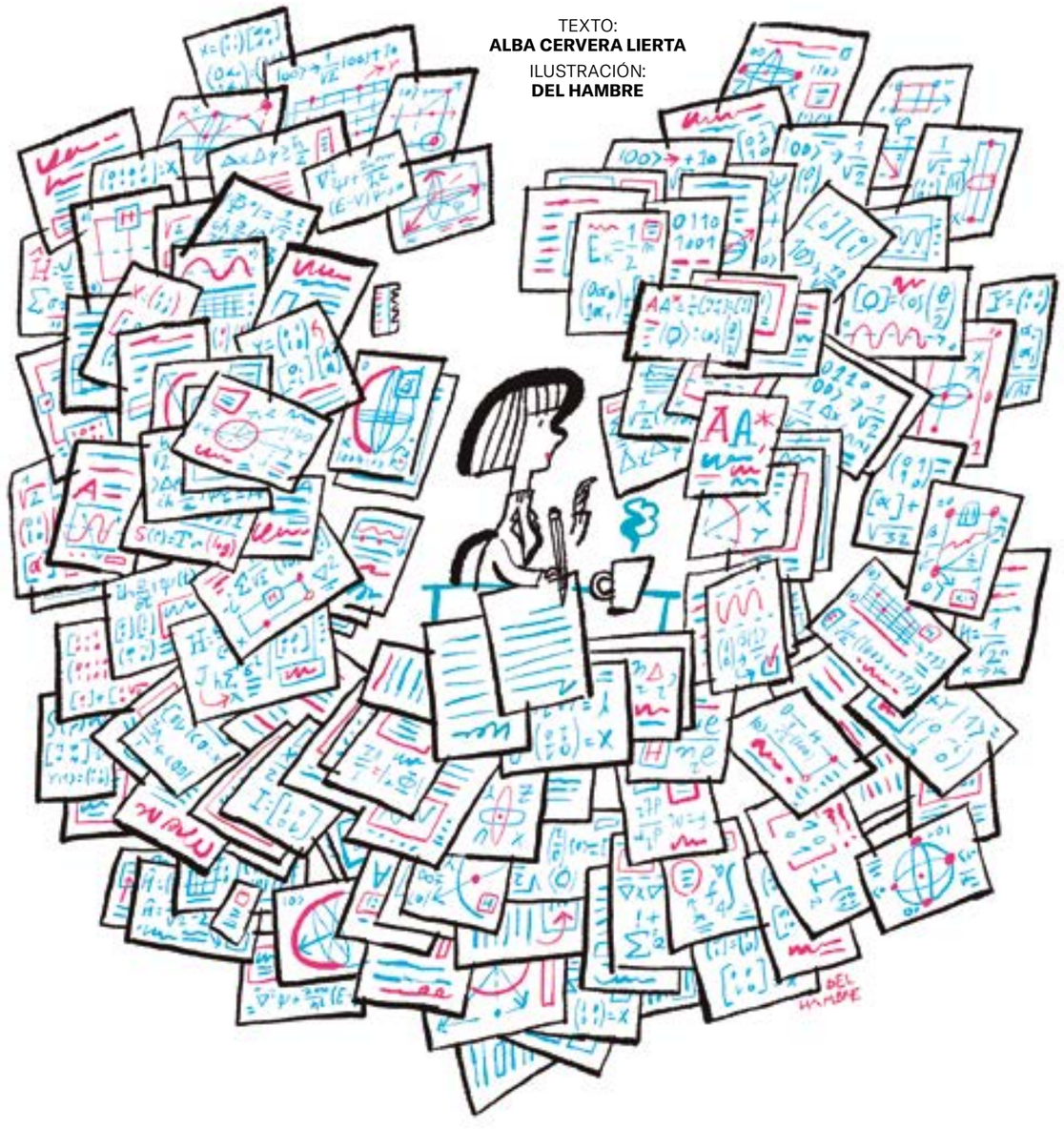
TEXTO:
ALBA CERVERA LIERTA
ILUSTRACIÓN:
DEL HAMBRE



CARTA A MI YO DEL FUTURO

La autora, doctora en Física de Partículas y coordinadora del proyecto Quantum Spain en el Barcelona Supercomputing Center retrata, mediante un original relato epistolar, la situación actual de la computación cuántica y algunas de las incógnitas que se plantean sobre su futuro.

QUERIDA YO: ¿HICIMOS BIEN DEDICÁNDONOS A LA COMPUTACIÓN CUÁNTICA?

Querida Alba:

Como sabes, mucha gente se pregunta cómo será el futuro de la computación cuántica. Te escribo esta carta con la esperanza de que la recibas, nos des las respuestas y encuentres la manera de enviarla de vuelta al año 2026.

La primera pregunta que todas nos hacemos es: ¿tenéis ordenadores cuánticos?

En estos tiempos decimos que tenemos y utilizamos ordenadores cuánticos, pero las dos sabemos que no es del todo así: no tenemos corrección de errores y, por tanto, los dispositivos cuánticos de 2026 no pueden hacer computación cuántica universal.

Lo sé, lo sé, podemos hacer y probar muchas cosas interesantes con los ordenadores cuánticos actuales, tratar de controlar en la medida de lo posible sus errores experimentales y sacar el máximo provecho con la ayuda de los ordenadores convencionales, pero ambas somos conscientes de que, para tener aplicaciones más allá de las capacidades de los ordenadores tradicionales, vamos a necesitar mucho más.

En los últimos dos años, hemos visto las primeras demostraciones de corrección de errores en ordenadores cuánticos. Es fascinante ver cómo la tecnología sigue avanzando y la era de la computación cuántica tolerante a fallos está más cerca, pero nos queda un largo camino por recorrer... ¿o quizás no tan largo?

En pocos años hemos pasado de tener chips cuánticos de 5 cúbits a dispositivos de más de 100 con ratios de error muy bajos. Aunque la corrección de errores cuántica requiera de miles (o millones) de cúbits muy buenos, no veo descabellado que en cinco años tengamos dispositivos con unas decenas de cúbits "perfectos" que nos permitan soñar con aplicaciones realmente sofisticadas. Creo que habrá que esperar al menos diez años para poder explotar plenamente las aplicaciones que todos esperamos, pero quizás peco de prudencia (¿o de optimismo?).

Y esto me lleva a la segunda pregunta: ¿de qué están hechos los ordenadores cuánticos del futuro? ¿Superconductores, iones atrapados, átomos neutros, fotónicos, quizás una mezcla...? Parece que la carrera tecnológica ya no la dominan solo los cúbits superconductores como hasta ahora; los átomos neutros están mostrando unas capacidades increíbles, y los iones atrapados tienen ahora la mayor calidad en las operaciones. ¿Pero podrán escalar su tamaño?

Esto de que se puedan hacer ordenadores cuánticos con diferentes tecnologías (a diferencia de los ordenadores convencionales, que están basados en los semiconductores) complica bastante las cosas y, sobre todo, la toma de decisiones por parte de empresas y grupos de investigación, sobre qué tecnología escoger para el desarrollo de su prototipo.

"En cinco años podríamos disponer de dispositivos con decenas de cúbits perfectos, pero probablemente habrá que esperar al menos diez para poder explotar plenamente las aplicaciones que todos esperamos"

Me pregunto si en el futuro habrá una tecnología cuántica dominante o el diverso abanico actual (¡o incluso más!).

Imagino que, como ocurrió en el nacimiento de esta tecnología, algunas plataformas se abandonarán por falta de avances o por encontrar limitaciones fundamentales que impidan escalar los prototipos. Al fin y al cabo, aquí también impera una suerte de selección natural: solo las tecnologías que se adaptan a los nuevos progresos (¡y rápido!) acaban sobreviviendo. Me aventuro a especular que, en los próximos diez años, veremos cómo todas las plataformas que se usan hoy en día extensamente (como las mencionadas anteriormente) alcanzarán prototipos funcionales de ordenadores cuánticos tolerantes a fallos, es decir, con corrección cuántica de errores. Luego, pasaremos unos años probándolas todas y, finalmente, solo las que sean más baratas de producir y de gestionar, se quedarán.

¿Aparecerá alguna tecnología nueva que no esté en mi radar hoy en día? ¿O alguna propuesta más antigua (como NMR —Nuclear Magnetic Resonance— o los esquivos cúbits topológicos) dará el salto y se pondrá a la cabeza? ▶

El primer caso lo veo difícil, ya que todos los esfuerzos globales se están concentrando en unas pocas tecnologías. Pero, quién sabe, quizás exista alguna irreductible *aldea gala* que resiste en algún rincón del mundo y que hace un descubrimiento revolucionario que nos permita tener millones de cúbits *buenos, bonitos y baratos*.

Esto me lleva a preguntarme cómo se estructurará la estrategia cuántica en el futuro: ¿sigue habiendo espacio para la física fundamental o se ha convertido todo el campo en un problema de ingeniería?

“Los ordenadores cuánticos del futuro podrán descifrar los mensajes cifrados, pasados y actuales. Se deben actualizar los protocolos de encriptación hoy para hacerlos resistentes a la computación cuántica”

Actualmente quedan muchos retos fundamentales por resolver para poder construir ordenadores cuánticos universales, pero debo reconocer que la mayoría de los esfuerzos se encaminan cada vez más a abaratar costes, escalar prototipos y mejorar la operación de los dispositivos, más que a buscar nuevas tecnologías cuánticas o aplicaciones que no hayamos imaginado aún.

¿Seguiremos estando de moda? ¿La computación cuántica ya es *mainstream*?

No pienso que sea algo malo, significaría que este campo ha llegado a todas las disciplinas científicas y se ha convertido en una herramienta más (este era uno de sus objetivos). Como física, un futuro con los principales problemas fundamentales resueltos no me motiva demasiado. ¡Espero que queden retos por resolver en los próximos años o nos tocará cambiar de campo!

Hablando de retos fundamentales, en 2026 estoy empezando varios proyectos sobre ordenadores cuánticos analógicos, en gran parte debido a que en el Barcelona Supercomputing Center (BSC) estamos terminando la instalación de un uno de ellos que formará parte de la primera red europea de computadores cuánticos. Muchos pensamos que, antes de que consigamos ordenadores cuánticos digitales universales, las primeras aplicaciones industriales y académicas las traerán los ordenadores cuánticos analógicos. De hecho, ya está ocurriendo con los simuladores cuánticos en algunos problemas de física básica. La duda que tenemos es si, en el futuro, este tipo de ordenadores sobrevivirán. En una era donde tengamos computación cuántica digital universal, técnicamente no hará falta la computación analógica. Pero me atrevo a aventurar que quizás aguantarán más años de los esperados. Al fin y al cabo, la mayoría de las aplicaciones que se nos ocurren para la computación cuántica son más naturales de programar de forma analógica que digital.

Otro reto fundamental será la conexión de los ordenadores cuánticos entre sí. ¿Tenéis internet cuántico en el futuro?

No me imagino cómo podréis tener ordenadores cuánticos de millones de cúbits en un solo chip o dispositivo. Tendréis que haber conseguido dominar la conexión entre ordenadores cuánticos a través de comunicaciones cuánticas también. Imagino que la fotónica seguirá siendo la líder en este campo, ¿o habéis ideado un nuevo mecanismo para ello?

Respecto a las conexiones cuánticas, aunque no trabajamos en comunicación cuántica (al menos en 2026) tengo mucha curiosidad: ¿estáis en la era post-cuántica todavía o la distribución cuántica de claves ya está implementada?

Hoy en día, todos se están pasando a los nuevos protocolos post-cuánticos, los resistentes a ataques de ordenadores cuánticos, con la esperanza de que, más adelante, no se puedan leer los mensajes del presente. Me pregunto si eso ha quedado también obsoleto (o parcialmente obsoleto) y la generación de claves criptográficas utiliza protocolos cuánticos más seguros.

¿Cómo de cerca estáis de romper la criptografía de finales de siglo XX, los protocolos tipo RSA? Estimamos que se necesitarán millones de cúbits para poder implementar los algoritmos cuánticos que rompen las claves, pero quizás habéis encontrado la forma de reducir ese número (o el número ya no es un problema porque podéis hacer ordenadores cuánticos arbitrariamente potentes). Me pregunto qué mensajes del pasado habréis podido desencriptar, al menos alguno de los anteriores a la implementación de la criptografía post-cuántica, pues no todos saben que las claves de encriptación son públicas, y que nadie nos impide guardar miles de datos y mensajes cifrados esperando llegar a vuestra época y desencriptarlos con un ordenador cuántico.

Otra pregunta recurrente es cuántos ordenadores cuánticos tenéis. Creo que sobre esta tengo una opinión bastante clara (espero que no me dejes mal). Estamos viendo cómo el acceso se está democratizando cada vez más: plataformas como Amazon o Microsoft Azure ofrecen cada vez más tipos de ordenadores cuánticos, mientras que prácticamente todos los centros de supercomputación del mundo han instalado o tienen planeado instalar algún tipo de ordenador cuántico. Por tanto, estimo que en un futuro muy próximo (de hecho, ya está ocurriendo), todos los centros de supercomputación contarán con ordenadores cuánticos en sus instalaciones, e incluso las universidades y los centros de investigación puede que tengan el suyo propio. Es decir, habrá tantos ordenadores cuánticos como supercomputadores tradicionales, ¡si no más! Aun así, no creo que todos tengamos en casa uno, pues no se me ocurre qué problema computacional cotidiano podría requerir de un ordenador cuántico.

Lo que no es tan evidente es quién va a fabricarlos: ¿habrá conseguido Europa ser soberana en esta tecnología? De momento, los esfuerzos europeos son significativos y hay cada vez más empresas empeñadas en construir sus propios ordenadores cuánticos sin depender de tecnología de países no pertenecientes a la Comunidad Europea.

Soy optimista en que, si ya estamos viendo los frutos de estos esfuerzos hoy en día, seguiremos mejorando con los años hasta alcanzar el nivel de otras grandes potencias tecnológicas. Aunque para mí ya sabes lo que es más importante saber... ¿han colonizado ya los ordenadores cuánticos toda la capilla del Barcelona Supercomputing Center (BSC)? En 2026, un tercio de la urna en la capilla es para ordenadores cuánticos, pero el resto está reservado para más máquinas de supercomputación que permitan hacer inteligencia artificial (ya sabes, la moda en estos tiempos...). Ya sé que preguntarte sobre el estado de la IA en el futuro daría para una carta mucho más larga que esta, pero me conformo con que me confirmes si uno de estos escenarios se ha cumplido: ¿el *hardware* necesario para hacer IA ocupa tanto espacio que sitios como el BSC ha necesitado destinar todo un nuevo edificio dedicado solo a ello? ¿Ha quedado libre la capilla para los ordenadores cuánticos?

Segundo escenario: ¿los ordenadores cuánticos se han vuelto tan importantes que el BSC ha necesitado destinar todo un nuevo edificio dedicado solo a ellos? ¿Han dejado libre la capilla para que vuelva a albergar a los supercomputadores de antes? Y, por último, esta opción: ¿la computación cuántica se ha integrado completamente con la supercomputación tradicional? ¿Los chips integran ambas, de modo que no hace falta hacer ninguna distinción de espacios y todos son partes del mismo ordenador?

Me encantaría que el tercer escenario fuera en el que tú vives ahora, aunque el segundo tampoco estaría mal. Todos los veo más que posibles.

Para despedirme, iré al grano: ¿para qué usáis ordenadores cuánticos? Después de más de 40 años de investigación activa, conocemos muy pocos tipos de algoritmos cuánticos, y aunque todos ellos son de vital importancia y nos llevan a numerosas aplicaciones, muchas esperamos que las mayores ventajas estén por descubrirse y que en 2026 ni nos las imaginemos, como ocurrió con la computación tradicional. Ayudaría mucho que me sugirieras alguna de estas aplicaciones por adelantado.

Un beso de mi (tu) parte,
Alba
24 de febrero de 2026.