LA REALIDAD DE LA COMPUTACIÓN CUÁNTICA: DATOS PERSONALES, RESPONSABILIDAD PROACTIVA Y ESTADO DE LA TÉCNICA

CafeLab 26 de octubre de 2026

La sesión reunió a especialistas en tecnologías cuánticas, criptografía, ciberseguridad y protección de datos para examinar una cuestión compartida: cómo prepararse ante una amenaza cuya fecha de materialización es incierta, pero que ya debe tenerse en cuenta al decidir sobre la seguridad de la información.

El debate no se limitó a las posibilidades de los ordenadores cuánticos. Se centró, sobre todo, en los tiempos de adaptación de las organizaciones a las obligaciones del RGPD, la dependencia de proveedores y las actuaciones que podrían impulsar las autoridades públicas.

1. NOTA DE CONCEPTO

1.1 Contexto y marco conceptual

La seguridad de la mayor parte de los datos personales que circulan hoy descansa en la criptografía asimétrica. Un ordenador cuántico suficientemente potente podría romperla. Aunque esa máquina aún no existe, la amenaza ya es presente por el llamado «recoger ahora y descifrar después» (*Harvest Now, Decrypt Later* o *HNDL*): un atacante puede capturar hoy tráfico cifrado y descifrarlo cuando la tecnología lo permita. Para datos con un ciclo de confidencialidad largo (historias clínicas, datos genéticos, biométricos, de menores o judiciales), el riesgo no es futuro, sino actual.

El artículo 32 del RGPD obliga a aplicar medidas de seguridad apropiadas «teniendo en cuenta el estado de la técnica». Esa referencia es dinámica: lo adecuado ayer puede ser insuficiente hoy. Y el estado de la técnica ha dado un salto. En 2024, el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) publicó sus primeros estándares finales de criptografía poscuántica (ML-KEM, ML-DSA y SLH-DSA).

El principio de responsabilidad proactiva (arts. 5.2 y 24 del RGPD) exige no solo cumplir, sino acreditar el cumplimiento. Aplicado a la amenaza cuántica, esto se podría traducir en obligaciones documentales concretas, como disponer de:

1. Inventario criptográfico. Saber qué algoritmos protegen qué tratamientos, dónde, con qué proveedores y con qué dependencias. Sin este mapa no hay análisis de riesgos defendible.
2. Análisis de riesgos con horizonte temporal. La gestión del riesgo (arts. 24, 25, 32, 33 y 35) debe considerar cuánto tiempo deben permanecer confidenciales los datos y si ese plazo supera la fecha estimada de ruptura de los algoritmos actuales.
3. Privacidad desde el diseño (art. 25). La criptoagilidad (diseñar sistemas y tratamientos capaces de sustituir algoritmos sin rediseño completo) pasa a ser una medida de diseño exigible, y los esquemas híbridos (clásico + poscuántico) una vía razonable de transición.
4. Priorización razonada. El RGPD pondera el coste de implantación y la naturaleza, alcance y contexto del tratamiento. No se exige migrar todo de inmediato, pero sí justificar por qué unos tratamientos se protegen antes que otros.
5. Cadena de encargados (art. 28). Los contratos con proveedores *cloud*, de firma electrónica o de comunicaciones deberían incorporar compromisos y plazos de migración poscuántica.

El artículo 34.3.a) exime de comunicar una brecha a los interesados si los datos resultan ininteligibles para terceros. Esa exención presupone que el cifrado es robusto hoy y mientras dure el impacto de dichos datos. Si un algoritmo pierde esa condición, una exfiltración pasada de datos cifrados puede convertirse en una brecha relevante, con obligaciones de notificación a la autoridad de control y a los afectados. La valoración del riesgo en brechas debe incorporar, por tanto, el riesgo de descifrado futuro.

La exigencia no proviene solo del RGPD. NIS2, DORA en el sector financiero, eIDAS2 y, en España, el Esquema Nacional de Seguridad con las guías del Centro Criptológico Nacional (CCN) convergen en la misma dirección. A nivel europeo existen una estrategia, la Estrategia de la Europa Cuántica COM (2025) 363 final; un pacto cuántico, el Quantum Pact, auspiciado en 2023 bajo la presidencia española del Consejo de la Unión; y, en breve, la Quantum Act. La Recomendación (UE) 2024/1101 de la Comisión instó a definir una hoja de ruta coordinada. Los Estados miembros adoptaron esa hoja de ruta en junio de 2025, con el compromiso de iniciar la transición a finales de 2026; para 2030 deberá completarse la

migración de los sistemas de alto riesgo y para 2035 la de los casos de riesgo medio y bajo. Además, la UE prepara la Quantum Act, cuya publicación estaba prevista para 2026.

1.2. Preguntas para el debate

1. ¿Qué otras medidas deberían adoptar responsables y encargados y que complementen las medidas indicadas anteriormente?
2. El Omnibus plantea que los datos seudonimizados no sean necesariamente personales si el tenedor no puede razonablemente reidentificar a las personas. La seudonimización suele apoyarse en criptografía. Si la capacidad de reidentificación depende de la fortaleza de un algoritmo con fecha de caducidad, ¿cómo afecta esta flexibilización del concepto en el contexto del riesgo cuántico?
3. La iniciativa Omnibus de datos, aunque todavía no finalizada, en su propuesta traslada las notificaciones de brechas del RGPD a un punto único de entrada, eleva el umbral a «alto riesgo» y amplía el plazo a 96 horas. Si prospera, el responsable tendrá que documentar por qué una brecha no es de alto riesgo. ¿Cómo se gestiona el escenario «*harvest now*, *decrypt later*» cuando ese juicio dependerá de si el cifrado comprometido seguirá siendo robusto en el horizonte de confidencialidad de los datos?
4. Hay críticas que señalan que la Quantum Act no vendrá acompañada de una dotación específica, ni creará un mecanismo de inversión rápida capaz de competir con el capital de EE. UU. y China. Esto es particularmente crítico en relación con la adecuación de las pymes a un nuevo entorno de amenazas a la protección de datos personales. ¿Qué acciones podría realizar una autoridad de protección de datos en este sentido?
5. ¿Está preparada la comunidad de delegados de protección de datos y de asesores en protección de datos para abordar soluciones desde el diseño de los tratamientos en un entorno tecnológico que combine la amenaza cuántica y el poder ofensivo de los agentes de IA? ¿Qué deben saber?

2. DESARROLLO DE LA DISCUSIÓN

2.1. Del riesgo futuro a las decisiones presentes

Una de las principales preocupaciones que se plantearon entre los asistentes a la sesión fue la estrategia conocida como «recoger ahora y descifrar después» (*harvest now*, *decrypt later*). Un atacante puede conservar comunicaciones cifradas obtenidas hoy y tratar de

descifrarlas cuando disponga de medios suficientes. Aunque no se conoce públicamente ningún ordenador cuántico capaz de romper a gran escala los principales sistemas asimétricos empleados actualmente, esa posibilidad afecta ya a información que debe permanecer confidencial durante muchos años.

Se discutió la dificultad de establecer fechas fiables. Las previsiones de 2030 o 2035 pueden alterarse por avances que no dependen únicamente del número de cúbits, sino también de su fidelidad y de la corrección de errores. Se mencionaron resultados recientes en este ámbito como muestra de la rapidez con que cambian las estimaciones. Asimismo, se recordó que determinadas capacidades de criptoanálisis podrían mantenerse secretas por su valor estratégico, sin que esa posibilidad permita afirmar que ya existan.

La conversación cuestionó la utilidad de seguir esperando una fecha precisa. Para una organización, lo decisivo es conocer cuánto tardaría en sustituir sus sistemas y si ese plazo resulta compatible con el período durante el cual necesita protegerlos. También se advirtió del efecto «Pedro y el lobo»: las alertas reiteradas, todavía sin una materialización visible, pueden favorecer la pasividad. La respuesta defendida fue anticiparse sin alarmismo, mediante decisiones graduadas y verificables.

2.2. Qué información proteger y frente a qué amenazas

Se insistió en que la urgencia no es idéntica para todos los datos. Algunas comunicaciones pierden valor en cuestión de horas; la información sanitaria, genética, biométrica o relativa a menores puede conservar su sensibilidad durante décadas. El horizonte de confidencialidad debe incorporarse a la evaluación del riesgo, junto con el plazo de conservación y las consecuencias de una eventual exposición.

El intercambio permitió diferenciar la criptografía asimétrica, como RSA o determinados sistemas de curvas elípticas, de la simétrica, como AES-256. La primera se encuentra especialmente expuesta a futuros ataques cuánticos capaces de comprometer los problemas matemáticos en los que se basa. En cambio, el cifrado simétrico robusto ofrece una resistencia considerable frente a los ataques cuánticos conocidos. Se subrayó que la protección real depende también de la solidez de los procedimientos de establecimiento de la relación de claves. Un archivo cifrado puede seguir protegido mientras no se comprometan esas claves, aunque otros elementos del sistema resulten vulnerables.

Se aclaró igualmente la diferencia entre criptografía poscuántica, basada en algoritmos ejecutables sobre infraestructuras convencionales, y distribución cuántica de claves, que utiliza sistemas físicos específicos. Se comentaron experiencias de comunicaciones por fibra y satélite, pero también sus limitaciones de distancia, infraestructura y precio. Para la

adaptación general de las comunicaciones digitales, el debate se orientó principalmente hacia la criptografía poscuántica.

2.3. Inventarios, plazos de migración y criptoagilidad

Uno de los puntos de mayor interés fue que el tiempo necesario para migrar a soluciones poscuánticas puede superar el período disponible antes de la aparición de capacidades que puedan comprometer determinados algoritmos. En productos complejos, los mecanismos criptográficos están dispersos entre aplicaciones, dispositivos y bibliotecas. Identificarlos, sustituirlos, probar los cambios y desplegarlos puede exigir varios años. Algunas organizaciones podrían descubrir que, conforme a sus propios tiempos de adaptación, ya llegan tarde.

Por ello se propuso empezar por un inventario criptográfico: qué algoritmos y protocolos se utilizan, qué tratamientos y sistemas protegen, dónde están sus componentes, quién los mantiene y de qué proveedores dependen. Ese conocimiento permitiría calcular plazos y establecer prioridades, atendiendo a la sensibilidad de los datos, la duración de la confidencialidad y la criticidad de los servicios.

Especial protagonismo tuvo la «criptoagilidad»: diseñar sistemas capaces de sustituir algoritmos y mecanismos criptográficos sin rehacer toda su arquitectura. La migración no puede tratarse como una operación definitiva. Se recordó que durante los procesos de estandarización poscuántica se han descartado candidatos tras descubrirse debilidades; también los seleccionados deberán seguir evaluándose a medida que se generalice su uso.

Se valoraron las soluciones híbridas, que combinan mecanismos clásicos y poscuánticos, como alternativa de transición. Pero se advirtió que la coexistencia de tecnologías puede dejar puntos débiles si subsisten componentes vulnerables. La idea compartida fue que importa tanto elegir una solución resistente como poder sustituirla rápidamente cuando sea necesario.

2.4. Estado de la técnica, responsabilidad proactiva y brechas

En el plano jurídico, el debate se concentró en los artículos 24 y 32 del RGPD, en conexión con la protección de datos desde el diseño y las evaluaciones de impacto. Se consideró que las obligaciones actuales ya exigen atender a la evolución de las amenazas: el estado de la técnica no es estático y una medida apropiada al implantarse puede dejar de serlo. Ello no equivale a imponer a todos los responsables una migración inmediata, sino a exigir una evaluación razonada y medidas proporcionadas a los riesgos.

La responsabilidad proactiva exige asimismo poder acreditar las decisiones. Inventarios, análisis con horizonte temporal, prioridades de actualización, medidas transitorias y

revisión de contratos pueden ayudar a demostrar una actuación diligente. Se destacó la necesidad de formar a los delegados de protección de datos para que puedan participar en estas decisiones sin tener que convertirse en especialistas en ingeniería cuántica.

Una de las cuestiones jurídicas más sugestivas fue la valoración de las brechas de datos cifrados. El RGPD contempla la ininteligibilidad de la información para terceros como circunstancia que puede excluir su comunicación a las personas afectadas. ¿Cómo evaluar, entonces, la sustracción actual de datos cuya confidencialidad podría perderse años después? Se sostuvo que el riesgo de descifrado futuro debe tenerse en cuenta, especialmente para información sensible de larga duración.

Quedó abierta una cuestión distinta: qué ocurre cuando un avance posterior modifica el riesgo asociado a una brecha ya conocida y si procede revisar su valoración o las comunicaciones realizadas. No se afirmó que una evolución criptográfica constituya automáticamente una nueva brecha. También se mencionaron los efectos posibles sobre ciertas técnicas de seudonimización y sobre las medidas complementarias de seguridad empleadas en transferencias internacionales, sin asumir que todas queden comprometidas por igual.

2.5. Proveedores, pymes y responsabilidades pendientes

El debate destacó la dependencia de servicios en la nube, soluciones de firma, comunicaciones y programas gestionados por terceros. Para numerosas pymes, buena parte de la transición llegará mediante actualizaciones de sus proveedores. Aun así, deberán conocer sus sistemas, las garantías disponibles y los compromisos de adaptación. Se propuso elaborar cláusulas contractuales que contemplen información sobre vulnerabilidades, actualización criptográfica y calendarios de migración.

Una intervención planteó un supuesto jurídico de especial interés: el del encargado que advierte al responsable de que necesita nuevas medidas de seguridad y del responsable que se niega a financiarlas. Se compartió la experiencia de proveedores que prefieren dejar de prestar servicios antes que continuar protegiendo sistemas cuyos titulares rechazan mejoras necesarias. ¿Qué deberes de advertencia corresponden al encargado y hasta dónde puede continuar la relación contractual sin comprometer sus propias obligaciones? La pregunta quedó sin respuesta cerrada y se identificó como materia para profundizar, también ante la creciente IA ofensiva.

La financiación atravesó buena parte de la conversación. No es comparable la capacidad de una gran organización con la de una pequeña empresa. Se defendió valorar las medidas exigibles atendiendo a los riesgos, las circunstancias y los costes de implantación, sin convertir la escasez de recursos en una exención automática. Se planteó que contar con

inventarios y planes razonables puede ser una manifestación de diligencia, aunque no sustituya las medidas efectivamente necesarias. También se sugirió desarrollar herramientas públicas o compartidas de descubrimiento criptográfico y apoyo a las pymes.

2.6. Soberanía tecnológica y dimensión geoestratégica

La estandarización poscuántica liderada por el NIST estadounidense suscitó un debate sobre soberanía europea. Se señaló la importante participación de investigadores y universidades europeos en el desarrollo de algoritmos, pero también la distancia entre investigar, establecer estándares, fabricar componentes y controlar las implementaciones comerciales. La vulnerabilidad ROCA sirvió para recordar que un algoritmo sólido puede fallar por una implementación defectuosa.

Se recordó asimismo la existencia de iniciativas europeas de coordinación de la migración y de políticas de desarrollo de tecnologías cuánticas. Los participantes señalaron que los calendarios orientativos no resuelven, por sí solos, la falta de financiación, personal especializado o productos preparados. Se preguntó hasta qué punto la futura regulación europea vendrá acompañada de instrumentos industriales y económicos capaces de convertir los objetivos de transición en actuaciones efectivas.

Se discutieron la dependencia de proveedores extranjeros, la concentración del mercado, la fabricación de chips y la conveniencia de apostar por capacidades industriales europeas. El código abierto y la interoperabilidad aparecieron como posibles respuestas a la cautividad tecnológica; quedó planteada, aunque no resuelta en la sesión, la pregunta sobre su relación con la resistencia a ataques cuánticos.

La perspectiva geoestratégica añadió dos escenarios: que un Estado disponga de capacidades criptográficas avanzadas y las mantenga secretas, o que anuncie poseerlas sin haberlas alcanzado. Incluso este segundo supuesto podría alterar la confianza en el comercio electrónico y las comunicaciones. La discusión conectó la protección de los datos con la seguridad nacional y la guerra cognitiva: controlar información significa también disponer de capacidades de inteligencia e influencia. Se sugirió que algunas inversiones en protección podrían articularse como infraestructuras o servicios compartidos, y no recaer únicamente en cada empresa.

2.7. IA ofensiva y actuaciones esperadas de las autoridades

Se contrastó la incertidumbre temporal de la amenaza cuántica con los efectos ya perceptibles de la inteligencia artificial aplicada a los ciberataques. Se mencionó un aumento muy acusado del ritmo reciente de notificaciones de brechas a la AEPD, con proyecciones anuales que serían preocupantes si persistiera esa intensidad; se trataba de

una extrapolación expuesta durante el debate, no de una cifra anual consolidada. La automatización de ataques y el volumen de incidentes plantean dificultades crecientes para la respuesta institucional.

También se cuestionó si las administraciones públicas están preparándose con suficiente anticipación. Gestionan grandes volúmenes de datos, a menudo sensibles y sujetos a conservación prolongada, pero afrontan limitaciones presupuestarias y dependencias tecnológicas semejantes a las de otros sectores. Se insistió en que deberían estar entre las primeras organizaciones en conocer su exposición criptográfica y planificar la adaptación, con apoyo de los organismos públicos especializados en ciberseguridad.

En la parte final se preguntó expresamente qué deberían hacer las autoridades de protección de datos. Las propuestas convergieron en guías para evaluar riesgos cuánticos, criterios de priorización, ejemplos prácticos, modelos de cláusulas con proveedores y orientación sobre cómo documentar una transición diligente. Se subrayó la conveniencia de coordinar esos criterios con los organismos de ciberseguridad y las autoridades europeas, evitando respuestas fragmentadas y exigencias desproporcionadas para las pymes.

También se informó de la preparación de una guía sectorial de migración poscuántica y se ofreció colaboración desde el mundo empresarial y universitario para organizar nuevos encuentros. El diálogo entre juristas y especialistas técnicos fue valorado como una necesidad permanente: permite traducir amenazas complejas en decisiones concretas, obligaciones comprensibles y políticas públicas viables.

La sesión dejó coincidencias claras sobre la necesidad de anticiparse, inventariar, priorizar y desarrollar criptoagilidad, pero también interrogantes que merecen trabajo posterior: la valoración de brechas con riesgo de descifrado diferido, las responsabilidades entre responsables y encargados, la financiación de la adaptación y la autonomía tecnológica europea.

La aportación principal de la sesión fue situar la computación cuántica no como una amenaza remota que deba esperar a una fecha definitiva, sino como un factor que ya debe integrarse, con proporcionalidad, en la gestión de la seguridad y la protección de datos.