

MÉXICO ANTE LA TRANSICIÓN POST-CUÁNTICA 2026

Evidencia pública, atribución y madurez criptográfica observable

Panel analítico México · 50 unidades · Codebook v1.0

Corte de evidencia: 2 de septiembre de 2026

Corte de precisión factual: 18 de septiembre de 2026

HALLAZGO CENTRAL

Las dependencias criptográficas relevantes para una eventual transición son ampliamente observables. La transición post-cuántica organizacional local todavía no puede estimarse con cobertura suficiente a partir de evidencia pública.

ACERCA DEL ESTUDIO

Informe de investigación · Edición 2026

El estudio comprende un panel analítico de 50 unidades, el manual de codificación (Codebook) v1.0 congelado antes de la adjudicación definitiva y 500 decisiones entidad-dimensión. La evidencia pública elegible no satisface los umbrales de cobertura predefinidos para sostener una clasificación ordinal entre unidades; por ello, el informe presenta perfiles de evidencia en lugar de una jerarquización comparativa.

La investigación estima exclusivamente el grado de transición post-cuántica observable a partir de evidencia pública, atribuible y trazable. No infiere estados internos no divulgados, no imputa madurez a partir del silencio documental y no formula juicios sobre la calidad general de la ciberseguridad de las unidades analizadas. La unidad de análisis es una organización o componente operativo con un ámbito mexicano de atribución identificable; la unidad de codificación es una afirmación entidad-dimensión vinculada a evidencia y alcance explícitos.

CIERRE DEL PERIODO DE PRECISIÓN FACTUAL

Las 50 unidades fueron incluidas en el procedimiento formal de precisión factual. Al cierre, ninguna respuesta aportó una corrección material o una fuente pública elegible que modificara una adjudicación.

Autoría

Autor: Dr. Juan Pablo Ybarra Llamas

Entidad responsable de publicación: Zero Trust Consulting / ZTC Research

Sitio web: <https://zerotrust.consulting>

Corte principal de evidencia: 2 de septiembre de 2026

Corte del periodo de precisión factual: 18 de septiembre de 2026

Citación recomendada: Ybarra Llamas, J. P. (2026). México ante la Transición Post-Cuántica 2026: evidencia pública, atribución y madurez post-cuántica observable. ZTC Research / Zero Trust Consulting.

Este estudio no constituye auditoría, certificación, opinión de cumplimiento, recomendación de inversión ni dictamen sobre la seguridad interna de las organizaciones analizadas. Los resultados aplican únicamente al panel codificado y a la evidencia pública disponible bajo el protocolo documentado.

INDEPENDENCIA ANALÍTICA

En resguardo de la independencia analítica, ZEROPAN Core —bóveda criptográfica post-cuántica (PQC) con capacidades de tokenización, desarrollada por Zero Trust Consulting— quedó fuera del panel analítico y de la comparación internacional. Su evidencia no formó parte del corpus utilizado para la codificación, la adjudicación ni las conclusiones.

CONTENIDO

Índice

INTRO / Pregunta de investigación y alcance inferencial

00 / Hallazgos ejecutivos

01 / Fundamento técnico y problema de migración

02 / Metodología: diseño, selección del panel y estimación

03 / Comparación internacional y contexto de México

04 / Resultados consolidados

05 / Lectura sectorial

06 / Pagos: dependencia criptográfica interorganizacional

07 / Priorización por horizonte de exposición

08 / Del inventario criptográfico a la resiliencia operacional

09 / Panel analítico de 50 unidades / perfiles de evidencia

10 / Validez, fuentes y trazabilidad

— / Cierre / Implicaciones estratégicas

Introducción

La transición hacia la criptografía post-cuántica (PQC) plantea, antes que un problema de clasificación, un problema de medición bajo condiciones de observabilidad pública asimétrica. Una organización puede desarrollar trabajo interno sustantivo sin divulgarlo; inversamente, una declaración global, una capacidad de proveedor o una referencia promocional puede sugerir un grado de avance que no es atribuible al perímetro mexicano analizado.

La pregunta de investigación se formula en términos deliberadamente acotados, reproducibles y susceptibles de refutación empírica: ¿qué grado de transición post-cuántica puede sostenerse, al 2 de septiembre de 2026, para cada unidad analítica mexicana exclusivamente a partir de evidencia pública, atribuible, auditable y suficiente por dimensión? El objeto de estimación no es la preparación interna latente —inobservable para este diseño—, sino la madurez post-cuántica que puede demostrarse bajo un protocolo de evidencia preespecificado.

PREGUNTA DE INVESTIGACIÓN

¿Qué grado de transición post-cuántica puede demostrarse públicamente, con atribución local y evidencia dimensional suficiente, para cada unidad del panel a la fecha de corte?

Esta distinción gobierna la selección del panel, el tratamiento de datos no observados, las reglas de atribución, la separación entre cobertura y madurez y la decisión de no publicar una clasificación ordinal cuando la evidencia no satisface los umbrales de comparabilidad. El informe debe interpretarse, por tanto, como un estudio de observabilidad y evidencia de transición; no como una auditoría de controles internos, una calificación integral de ciberseguridad ni una estimación poblacional del mercado mexicano.

00 /

Hallazgos ejecutivos

Qué puede afirmarse responsablemente sobre la transición post-cuántica observable en el panel analítico.

Hallazgos ejecutivos

El resultado central no permite sostener una inferencia de rezago generalizado. Permite una conclusión más acotada y metodológicamente defendible: la evidencia pública elegible sobre transición post-cuántica organizacional en el panel analítico no alcanza todavía la cobertura necesaria para una comparación ordinal responsable entre las unidades del panel.

Bajo el protocolo aplicado al panel analítico de 50 unidades, ninguna unidad alcanzó la cobertura mínima necesaria para publicar un puntaje agregado de madurez observable (Observable Readiness Score, ORS).



INTERPRETACIÓN METODOLÓGICA

Que una dimensión permanezca como NE no significa M0, ausencia de preparación ni ausencia de trabajo interno. Significa que el protocolo no encontró evidencia pública suficiente, con el locus y la atribución requeridos, para estimarla. El diseño preserva el dato no observado como no observado; no lo transforma en una calificación negativa.

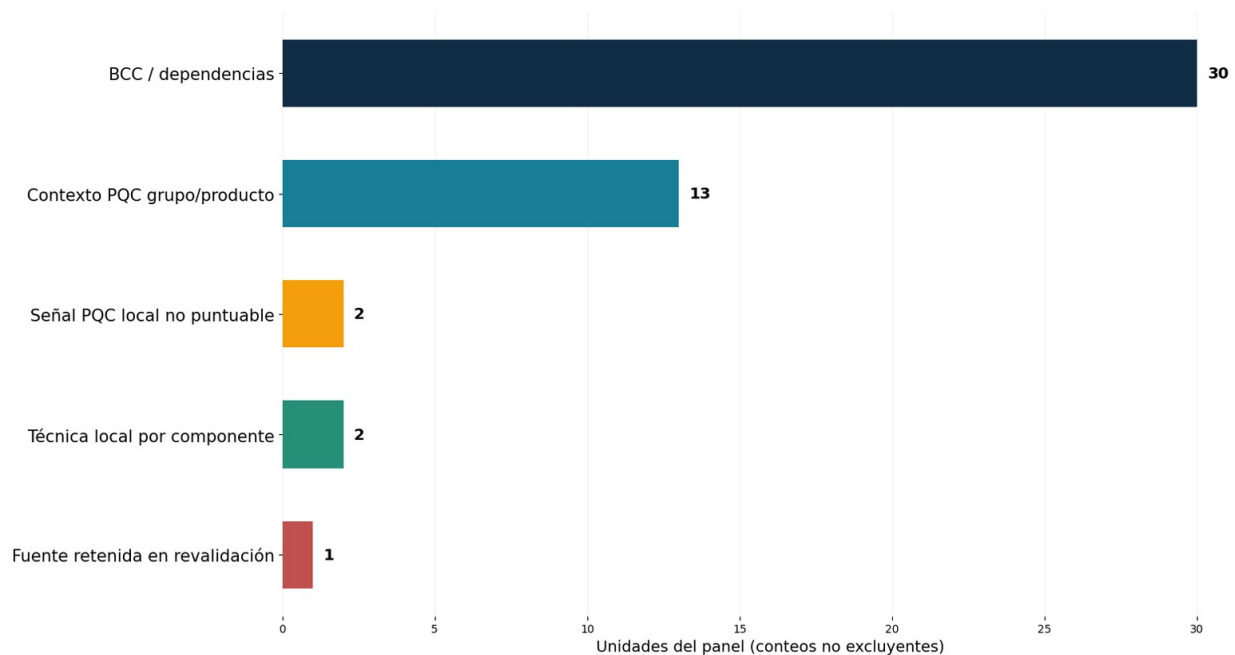


Figura 1. Patrón central del panel. Los conteos son no excluyentes. BCC describe dependencias criptográficas convencionales públicamente observables; no equivale a evidencia PQC.

Cinco hallazgos principales

- Las dependencias criptográficas relevantes para una eventual transición son considerablemente más observables que la transición post-cuántica misma. En 30 de 50 unidades se identificaron dependencias criptográficas convencionales - HSM, KMS, PKI, TLS, cifrado, tokenización o controles equivalentes -, mientras la evidencia PQC localmente estimable aparece sólo en cuatro decisiones entidad-dimensión.
- La infraestructura de nube es el único sector del panel en el que se identificó capacidad técnica post-cuántica operativa y localmente atribuible a componentes concretos en México. AWS Mexico Central y Google Cloud Querétaro alcanzan M4 únicamente en D5 y D8, con EC de 20%. Este resultado describe dos dimensiones estimables por unidad; no autoriza una inferencia de madurez organizacional equivalente al 80%.
- La evidencia global no se atribuye automáticamente a una operación mexicana. Trece unidades presentan contexto PQC a nivel de grupo o producto, pero el Codebook exige un vínculo explícito de atribución cuando la afirmación pretende describir una unidad con locus mexicano.
- Se identificaron señales locales; sin embargo, una señal no equivale a madurez demostrada. Santander México y Banorte presentan señales PQC locales; ninguna satisface, por sí sola, la puerta de evidencia requerida para adjudicar una dimensión organizacional.
- La comparación internacional muestra institucionalización pública mediante mecanismos heterogéneos: órdenes ejecutivas, hojas de ruta, lineamientos, pilotos financiados, infraestructura y estandarización. El corpus mexicano incluye evidencia de capacidad académica e I+D en PQC, pero al corte no se identificó un instrumento nacional de transición comparable con los marcos más estructurados del corpus internacional.

TESIS DEL ESTUDIO

Las dependencias criptográficas relevantes para una eventual transición son ampliamente observables; la transición post-cuántica organizacional local, en cambio, no alcanza todavía cobertura suficiente para una estimación organizacional a partir de evidencia pública.

01 /

Fundamento técnico y problema de migración

La transición post-cuántica excede la sustitución algorítmica: requiere transformar dependencias, modelos de confianza, interoperabilidad y ciclos de vida criptográficos.

De la estandarización algorítmica a la migración operacional

La estandarización algorítmica reduce una fuente de incertidumbre, pero desplaza el problema principal hacia la migración de arquitecturas reales, la interoperabilidad y la continuidad de los mecanismos de confianza que las sostienen.

El 13 de agosto de 2024 se publicaron los primeros tres Federal Information Processing Standards (FIPS) derivados del proceso de estandarización post-cuántica de NIST: FIPS 203 (ML-KEM) como mecanismo de encapsulación de claves, y FIPS 204 (ML-DSA) y FIPS 205 (SLH-DSA) para firmas digitales. La normalización reduce incertidumbre algorítmica, pero no resuelve por sí sola inventario, interoperabilidad, ciclo de vida, dependencias de terceros ni retiro de componentes heredados.

La unidad efectiva de migración

Dependencia	Qué cambia	Por qué la habilitación algorítmica no es suficiente
Claves / KMS / HSM	Algoritmos, tamaños, APIs, rotación	La capacidad del proveedor no demuestra adopción ni compatibilidad de extremo a extremo.
Certificados / PKI	Formatos, cadenas, firma y repositorios de confianza	Interoperabilidad y renovación pueden dominar el calendario.
TLS / VPN / SSH	Negociación criptográfica, grupos híbridos y bibliotecas	Clientes, proxies, dispositivos especializados e intermediarios de protocolo deben interoperar sin degradación.
Código y artefactos	Firma de software, repositorios y cadena de suministro	Cambiar mecanismos de firma afecta validadores, HSM, cadenas de integración/entrega y dispositivos heredados.
Datos de larga vida	Prioridad por horizonte de confidencialidad	El riesgo puede acumularse antes de que exista capacidad práctica para comprometer la criptografía de clave pública.
Terceros	Hojas de ruta, contratos y dependencias	La organización puede gobernar un riesgo que técnicamente reside en un proveedor.

Harvest Now, Decrypt Later: una relación entre horizontes de exposición y migración

El riesgo Harvest Now, Decrypt Later (HNDL) —capturar información cifrada en el presente con la expectativa de descifrarla en el futuro— exige atención anticipada cuando la suma de la vida útil de confidencialidad del dato y el tiempo requerido para migrar resulta comparable con, o superior a, el horizonte de una amenaza criptanalítica relevante. Dado que ese horizonte es incierto, el estudio no asigna una fecha de materialización: emplea la longevidad del dato y el tiempo de migración como variables de priorización, no como predicción de una fecha de ruptura.

CRITERIO DE INTERPRETACIÓN

La adopción de PQC no sustituye los controles criptográficos y de seguridad vigentes. Segmentación, gestión de claves, rotación, mínimo privilegio, resiliencia y control de terceros siguen siendo relevantes durante y después de la transición.

02 /

Metodología: diseño, selección del panel y estimación

El estudio separa madurez observable, confianza y cobertura; la ausencia de evidencia se trata como dato no observado y no como valor cero.

Diseño metodológico y Codebook v1.0

El constructo central es la transición post-cuántica observable sustentada por evidencia pública, atribuible y auditable. El diseño no pretende estimar estados internos no divulgados; busca establecer qué afirmaciones pueden sostenerse de manera reproducible para cada unidad, dimensión y alcance.

Diseño de investigación y objeto de estimación

El estudio adopta un diseño observacional, transversal y basado en fuentes abiertas, con fecha de corte explícita. El objeto de estimación es una propiedad documentalmente observable: la madurez de transición PQC que puede atribuirse a una unidad mexicana bajo evidencia elegible. Esta propiedad no debe confundirse con la madurez interna real, que puede ser mayor, menor o simplemente no observable desde el registro público.

La unidad de análisis es una organización o componente operativo con identidad y locus mexicano distinguibles; por locus se entiende el ámbito territorial, organizacional o de servicio al que puede atribuirse válidamente una afirmación. Por esa razón, el informe utiliza “unidad analítica” y no “empresa” como categoría general: el panel incluye tanto organizaciones como componentes regionales técnicamente separables. La unidad de codificación es una afirmación entidad-dimensión vinculada a una o más fuentes y acompañada, como mínimo, por locus de alcance, modo de dependencia, clase de evidencia, estado de la fuente, confianza y justificación de adjudicación. La inferencia se restringe al alcance que esas variables permiten sostener.

ALCANCE INFERENCIAL

La validez externa del panel es analítica, no estadística. Los resultados permiten describir patrones dentro del corpus seleccionado y contrastar mecanismos de observabilidad; no estiman prevalencias para la totalidad del mercado mexicano ni asignan probabilidades de selección a las organizaciones del país.

Selección del panel analítico de 50 unidades

El panel constituye una muestra intencional de máxima variación (Patton, 2015), diseñada para cubrir configuraciones heterogéneas de confianza, dependencia criptográfica, longevidad del dato y régimen institucional. El tamaño $n=50$ fija una frontera analítica que permite revisar 500 decisiones entidad-dimensión con profundidad y diversidad estructural. La selección priorizó variación estructural, centralidad interorganizacional y diversidad de regímenes de observabilidad dentro de los estratos definidos. El diseño es no probabilístico y no estima parámetros poblacionales.

El perímetro final de 50 unidades quedó fijado antes de la adjudicación definitiva. La inclusión fue independiente de la presencia, calidad o ausencia de evidencia PQC.

Procedimiento de conformación del panel

Etapa	Regla de selección	Función metodológica
1. Estratificación funcional	Definir, antes del cierre de adjudicación, los ocho estratos analíticos y las superficies criptográficas que debían estar representadas.	Evita que la selección dependa de notoriedad pública o de resultados PQC posteriores.

Etapas	Regla de selección	Función metodológica
2. Elegibilidad de candidatos	Identificar unidades con nexo mexicano, materialidad criptográfica y separabilidad suficiente para aplicar reglas de atribución.	Reduce ambigüedad sobre qué entidad o componente constituye la unidad de análisis.
3. Selección intencional	Priorizar variación estructural, centralidad interorganizacional y diversidad de regímenes de observabilidad dentro de los estratos.	Amplía el rango de configuraciones sobre el que se somete a prueba el instrumento.
4. Congelamiento	Fijar el perímetro antes de la adjudicación definitiva y mantener la inclusión independiente de la evidencia PQC observada.	Limita selección ex post y grados de libertad analíticos.
5. Control de enmiendas	Documentar por separado cualquier modificación del panel sin alterar constructo, pesos, puertas o umbrales.	Preserva trazabilidad entre versiones y comparabilidad interna.

Criterio de inclusión	Operacionalización	Riesgo metodológico que controla
Nexo mexicano identificable	Entidad mexicana o componente operativo con locus territorial, regulatorio o de servicio distinguible.	Evita atribuir a México evidencia puramente global.
Materialidad criptográfica	Control o dependencia de identidades, pagos, PKI/KMS/HSM, canales cifrados, firmas, datos de larga vida u otras funciones de confianza.	Evita unidades sin relación sustantiva con el constructo.
Centralidad interorganizacional	Participación en cadenas de confianza, infraestructura, procesamiento, nube, telecomunicaciones, identidad o servicios públicos.	Captura dependencias que trascienden una sola organización.
Variación sectorial	Cobertura deliberada de banca, pagos/fintech, telecomunicaciones, nube/datos, seguros, energía/crítica, salud y gobierno digital.	Reduce concentración excesiva en un único régimen de divulgación.
Separabilidad analítica	La unidad debe poder distinguirse razonablemente de su grupo, producto o proveedor para evaluar atribución.	Reduce doble conteo y ambigüedad de locus.
Independencia respecto del resultado	La existencia de evidencia PQC positiva, negativa o ausente no determina la inclusión.	Evita selección condicionada a la variable dependiente.

Composición sectorial y función analítica

La distribución sectorial no replica cuotas de mercado. Se utiliza para cubrir superficies criptográficas heterogéneas y regímenes de observabilidad distintos, de modo que el instrumento pueda probar sus reglas de atribución y evidencia en contextos comparables sólo dentro de su alcance.

Estrato analítico	n	Justificación analítica
Banca y autoridad monetaria	9	Transacciones, HSM/PKI, identidad, continuidad y estructuras grupo-local.
Pagos y fintech	12	Tokenización, APIs, redes de pago y dependencias interorganizacionales.
Telecomunicaciones	6	Identidad, confianza de red e infraestructura con ciclos de vida prolongados.
Nube / datos	5	KMS/HSM/TLS, regiones locales y dependencia de capacidades de proveedor.
Seguros	5	Datos personales/financieros de larga vida y estructuras corporativas complejas.
Energía / crítica	5	Convergencia IT/OT, certificados, firmware, disponibilidad y raíces de confianza.
Salud	4	Datos sensibles de larga retención, identidad e infraestructura institucional.

Estrato analítico	n	Justificación analítica
Gobierno digital	4	Identidad poblacional, fiscal/aduanero y servicios públicos con confianza de largo plazo.

JUSTIFICACIÓN DE LA COMPOSICIÓN DEL PANEL

Las 50 unidades se seleccionaron para maximizar variación estructural dentro de los ocho estratos definidos. La exclusión de otras entidades respondió a redundancia funcional, ausencia de un locus mexicano separable o concentración sectorial. Dentro de un mismo grupo se conservaron unidades separadas únicamente cuando existía un perímetro operativo o regulatorio distinguible. En proveedores de nube, una región mexicana identificable delimita el componente evaluado.

Protocolo de identificación, cribado y versionado de fuentes

La recopilación se ejecutó por unidad y dimensión, con prioridad para fuentes primarias institucionales y técnicas. Las fuentes secundarias se utilizaron como mecanismos de descubrimiento o contexto, no como sustitutos automáticos de evidencia primaria cuando la afirmación exigía trazabilidad técnica o atribución local. Cada hallazgo se evaluó contra una afirmación concreta, un ámbito de aplicación y una fecha de corte; la mera aparición de términos PQC no bastó para hacerlo elegible.

Fase	Regla operativa	Función de control
1. Descubrimiento	Búsqueda por unidad, dimensión y superficie criptográfica en dominios oficiales, documentación técnica, normativa, repositorios, comunicados y materiales institucionales.	Maximizar sensibilidad sin convertir menciones aisladas en evidencia elegible.
2. Cribado	Exigir pertinencia a la dimensión, identificabilidad de la fuente, vigencia al corte y alcance atribuible.	Excluir ruido semántico, duplicados y evidencia fuera de alcance.
3. Jerarquización	Priorizar fuentes primarias y técnicas; tratar fuentes secundarias como señales auxiliares salvo corroboración suficiente.	Reducir dependencia de interpretación mediada y lenguaje promocional.
4. Versionado	Registrar estado de la fuente y retener cambios o desapariciones detectados durante la revalidación.	Hacer visible la deriva documental y evitar sustituciones silenciosas.
5. Cierre	Cerrar la búsqueda por fecha de corte y completitud del protocolo, no por una presunta saturación del universo web.	Evitar presentar el corpus como exhaustivo o estadísticamente completo.

DEFINICIÓN OPERATIVA DEL ESTIMANDO

Para cada unidad i y dimensión d , el objeto de estimación es el mayor nivel M1-M5 que puede sostenerse con evidencia pública elegible al corte, después de aplicar las reglas de atribución y alcance. Si la puerta de elegibilidad no se supera, el estado permanece indefinido para fines de madurez (NE), no se fija en cero. EC_i expresa la proporción de las diez dimensiones que resultan estimables; cualquier agregación ORS queda subordinada a los umbrales de reportabilidad congelados.

Modelo de inferencia y tratamiento de datos no observados

La estimación se ejecuta en tres etapas secuenciales. Primero se determina si la evidencia es elegible para la afirmación y el alcance definidos; sólo entonces puede adjudicarse un nivel M1-M5. Finalmente, la cobertura de dimensiones estimables determina qué modalidad de resultado puede reportarse. Este orden evita que una fuente técnicamente sólida pero mal atribuida produzca una adjudicación local no sustentada.

Etapa	Pregunta metodológica	Salida
1. Elegibilidad	¿La fuente es pública, atribuible, vigente y suficiente para la dimensión y el locus definidos?	Estimable / NE
2. Madurez condicional	Si es estimable, ¿qué nivel M1-M5 demuestra la evidencia sin exceder su clase y alcance?	M1-M5 por dimensión
3. Reportabilidad	¿La cobertura EC permite agregar y reportar un ORS bajo los umbrales congelados?	Perfil / ORS parcial / ORS completo

La ausencia de evidencia pública no se presume aleatoria. La propensión a divulgar puede variar por sector, régimen regulatorio, modelo de negocio, sensibilidad operativa y práctica documental. En consecuencia, el estudio no adopta el supuesto estadístico de datos faltantes al azar (missing at random; Little y Rubin, 2019), no imputa valores y no construye promedios sectoriales de madurez a partir de celdas NE. EC mide cobertura documental elegible; no desempeño interno.

REGLA DE DATOS NO OBSERVADOS

NE es un estado epistemológico, no un nivel de madurez. Convertir NE en M0 produciría una clasificación dominada por prácticas de divulgación y no por evidencia de transición post-cuántica.

Dimensiones y ponderación

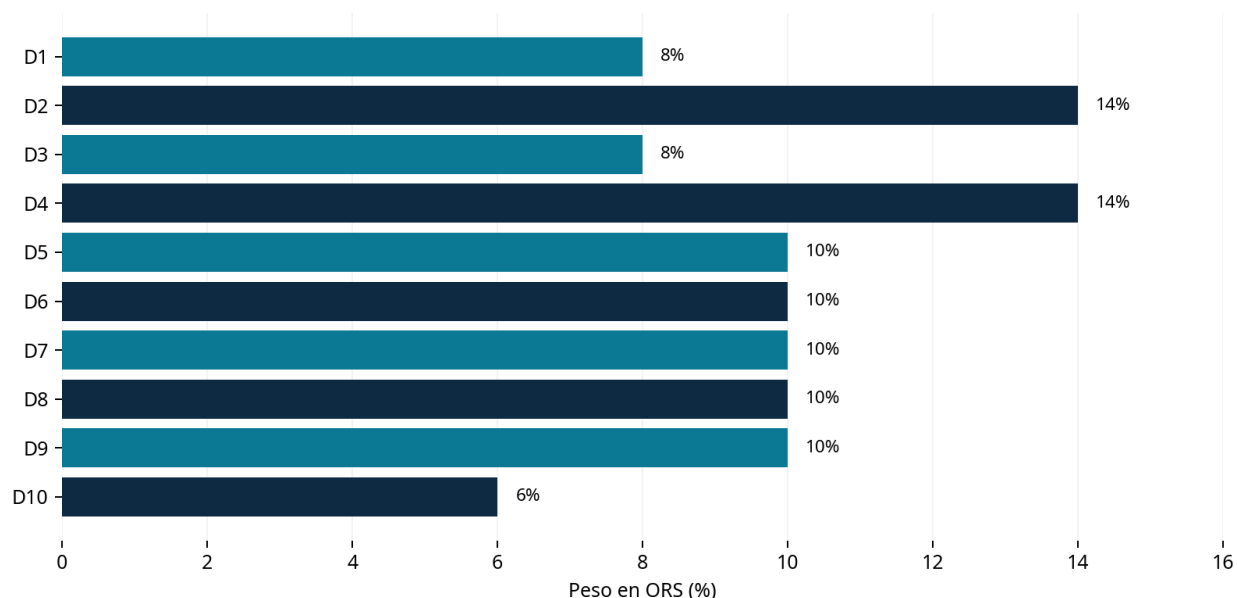


Figura 2. Ponderación del Observable Readiness Score (ORS). D2 y D4 tienen 14%; D10, 6%; el resto se distribuye entre 8% y 10%.

ID	Dimensión	Peso	Puerta
D1	Gobernanza y rendición de cuentas	8%	No
D2	Inventario criptográfico y descubrimiento de dependencias	14%	Sí
D3	Longevidad del dato y priorización del riesgo cuántico	8%	No
D4	Criptoagilidad y arquitectura objetivo	14%	Sí
D5	Infraestructura de claves, certificados y confianza	10%	No
D6	Estándares PQC y diseño de migración	10%	Sí

ID	Dimensión	Peso	Puerta
D7	Pruebas, interoperabilidad y rendimiento	10%	No
D8	Despliegue y transición de componentes heredados	10%	Sí
D9	Transición de terceros y cadena de suministro	10%	Sí
D10	Aseguramiento de migración y resiliencia	6%	No

Tres variables metodológicamente independientes

ORS - OBSERVABLE READINESS SCORE

Madurez ponderada únicamente sobre dimensiones estimables y reportables. No se calcula cuando la cobertura es insuficiente.

EC - EVIDENCE COVERAGE / COBERTURA DE EVIDENCIA

Porcentaje de dimensiones para las que una unidad puede estimarse bajo el protocolo. Determina qué modalidad de resultado puede reportarse.

ECS - EVIDENCE CONFIDENCE SCORE / CONFIANZA EN LA EVIDENCIA

Calidad y trazabilidad de la evidencia elegible. Informa la confianza en una adjudicación, pero no se multiplica por el ORS.

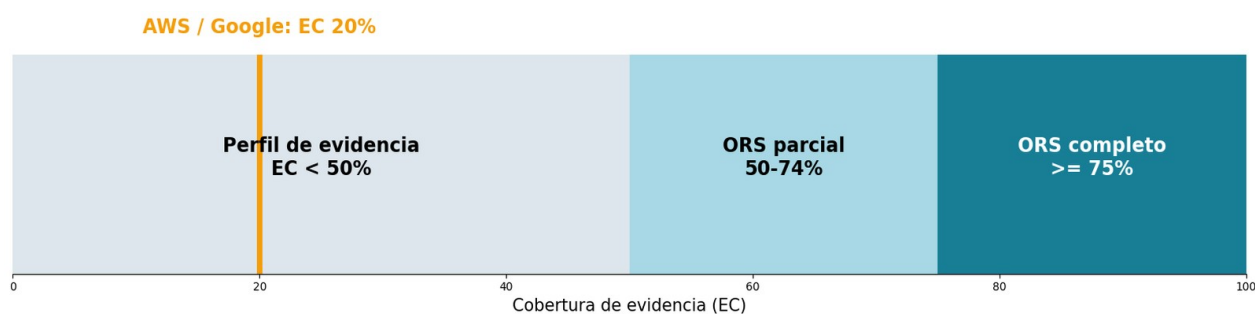


Figura 3. La cobertura es una puerta de publicación, no un multiplicador de la madurez. AWS y Google permanecen como perfiles de evidencia con EC=20%.

Propiedades de medición y umbrales de reportabilidad

Los niveles M1-M5 constituyen una escala ordinal operacional: expresan estados crecientes de evidencia y madurez observable, pero el diseño no supone que la distancia entre categorías adyacentes sea constante. El ORS es, por tanto, un índice compuesto definido por el Codebook y no una escala psicométrica de intervalo ni una estimación directa de una variable latente. Cualquier traducción numérica de categorías ordinales dentro del ORS debe leerse como una convención de puntuación transparente; si futuras ediciones alcanzan cobertura suficiente para agregar resultados, deberán acompañar esa agregación con análisis de sensibilidad frente a mapeos monotónicos alternativos.

Los umbrales EC de 50% y 75% son reglas preespecificadas de agregación y reportabilidad, no puntos de corte “naturales” inferidos de los datos. Del mismo modo, los pesos dimensionales son convenciones de diseño congeladas en v1.0, no coeficientes estimados empíricamente. Como ninguna unidad supera EC=20%, ni los pesos ni las variaciones marginales de los umbrales alteran el resultado inferencial principal.

NE, BCC y evidencia S/F/T

NE significa “no estimable con evidencia pública suficiente para la afirmación y el alcance definidos”. Si una dimensión es NE, la madurez queda sin estimar y nunca se transforma en M0. La etiqueta BCC conserva por separado las dependencias criptográficas convencionales observables - HSM, KMS, PKI, TLS, tokenización, cifrado u otras equivalentes - sin convertirlas en evidencia de transición PQC.

Clase	Qué prueba	Techo típico
S · Señal	Reconocimiento del riesgo, vacante, declaración ejecutiva o señal promocional sin control formal demostrado.	M1
F · Formal	Hoja de ruta, política, mandato, programa, adquisición o requerimiento contractual.	M2, salvo evidencia adicional
T · Técnica	Prueba, implementación, inventario, repositorio, protocolo, API o documentación técnica verificable.	Hasta M5

Atribución y aplicabilidad local

La calidad intrínseca de una fuente no garantiza que responda a la pregunta local. El Codebook distingue MX-DIRECT, MX-COMPONENT, GROUP-GLOBAL, PRODUCT-GLOBAL, JURISDICTION y UNKNOWN. Para atribuir una capacidad de grupo a una unidad mexicana se exige un vínculo explícito: cobertura de México, plataforma compartida con aplicabilidad demostrada, despliegue identificado, política obligatoria de grupo aplicable a la subsidiaria o evidencia local corroborante.

- La evidencia global no se atribuye automáticamente a México. La pertenencia corporativa o el uso de un proveedor común no constituyen, por sí solos, vínculos de atribución.
- La capacidad de un proveedor no constituye evidencia de madurez del cliente. Deben demostrarse uso, control y alcance.
- Un piloto o prueba de concepto puede demostrar actividad de prueba, pero no despliegue productivo salvo que exista un perímetro de producción explícito y verificable.
- El vocabulario declarativo -por ejemplo, “implemented”, “deployed” o “quantum-safe”- no establece M4/M5 por sí mismo; se exige evidencia operativa suficiente.

Confiabilidad, codificación independiente y congelamiento

El proceso incluyó rondas de codificación independiente sin consulta cruzada previa, revalidaciones focales y adjudicación documentada de discrepancias. Las afirmaciones de confiabilidad se circunscriben a los subconjuntos efectivamente doble-codificados (Krippendorff, 2018). El Codebook v1.0 quedó congelado y versionado antes del cierre de adjudicación.

REGLA DE CONGELAMIENTO Y CONTROL DE GRADOS DE LIBERTAD

Durante el procedimiento de precisión factual, una fuente pública recién identificada sólo podía reabrir la dimensión afectada si era elegible conforme al corte principal. Los pesos, las puertas metodológicas, los umbrales, las reglas de herencia y el Codebook permanecieron congelados. Este control limita los grados de libertad analítica y reduce ajustes ex post orientados por los resultados.

Prueba de robustez del umbral de reportabilidad

La cobertura máxima observada es $EC=20\%$. En consecuencia, ninguna unidad dispone de un ORS organizacional reportable bajo cualquier umbral estrictamente superior a 20% ; el resultado permanece lejos de las puertas de 50% y 75% . El análisis de sensibilidad muestra que la conclusión principal no depende de una elección marginal del umbral y no justifica relajar el Codebook.

Escala de madurez M1-M5

Nivel	Lectura	Carga de evidencia
M1	Riesgo o necesidad reconocida	Reconocimiento o intención con vínculo explícito a PQC.
M2	Dirección formal definida	Responsable, método, diseño, hoja de ruta o requerimiento formal.
M3	Ejecución verificable	Inventario ejecutado, prueba realizada o piloto controlado con resultado.
M4	Operación controlada	Producción o proceso repetible con ciclo de vida, monitoreo, reversión controlada o decisiones gobernadas.
M5	Integración continua	Capacidad incorporada al ciclo de ingeniería/riesgo con medición, evolución y retiro de componentes heredados.

M4 y M5 exigen evidencia operativa sustancialmente más fuerte. Verbos como “implemented”, “deployed” o “quantum-safe” no bastan, por sí solos, para establecer esos niveles.

03 /

Comparación internacional y contexto de México

La comparación internacional no construye una clasificación de países: contrasta tipos de instrumentos públicos, autoridad, alcance, hitos y señales de ejecución.

Comparación internacional y contexto de México

La comparación internacional sólo es interpretable cuando se distingue la naturaleza del instrumento. Una orden ejecutiva, una hoja de ruta gubernamental, un lineamiento técnico, un programa piloto financiado o una capacidad de proveedor representan formas distintas de institucionalización y ejecución y no deben tratarse como unidades equivalentes.

Jurisdicción	Instrumento público	Alcance	Lectura metodológica
Estados Unidos	Executive Order 14412, 22-jun-2026	Sistemas federales, adquisiciones y apoyo a infraestructura crítica	Hitos federales ordenados; requisitos de adquisición y aceleración de validación.
Canadá	Cyber Centre - hoja de ruta del Gobierno de Canadá	Departamentos/agencias federales	Plan inicial abr-2026; alta prioridad 2031; resto 2035.
Reino Unido	NCSC - calendario de migración PQC	Organizaciones públicas y privadas; orientación nacional	Descubrimiento y plan inicial en 2028; alta prioridad en 2031; migración en 2035.
Unión Europea	Coordinated Implementation Roadmap	Estados miembros, sector público e infraestructura crítica	Hoja de ruta coordinada; hitos y enfoque de coexistencia / criptoagilidad.
Singapur	Quantum-Safe Migration Handbook + QRI	CII, gobierno y organizaciones	Guía operativa + instrumento de autoevaluación publicado jul-2026.
Australia	ASD planning for PQC	Organizaciones públicas y privadas	Plan 2026; iniciar críticos 2028; completar 2030.
Japón	Cybersecurity Strategy 2025	Gobierno; extensión a infraestructura crítica y privado	Gobierno apunta a 2035; hoja de ruta para el ejercicio fiscal 2026.
Corea del Sur	KISA - programa piloto de transición 2026	Telecom, finanzas, transporte, defensa y espacio	Pilotos financiados para transición y validación de infraestructura.
Brasil	Portaria ITI nº 38/2026 · GTT-PQC/ICP-Brasil	ICP-Brasil y ecosistema de confianza digital	Grupo técnico formal; diagnóstico, plan de migración, actualización normativa y estrategia de ejecución.
México	I+D pública y capacidad académica; sin instrumento nacional comparable identificado al corte	Investigación académica; registro público federal revisado	IPN/INAOE aportan evidencia de I+D en PQC; no se identificó un instrumento nacional de transición equivalente al corte.

Conclusiones válidas del comparativo internacional

La institucionalización pública de la transición ya ocurre mediante instrumentos heterogéneos. Un país puede adoptar una orden ejecutiva; otro, una hoja de ruta técnica; otro, pilotos financiados; otro, una guía acompañada de una herramienta de autoevaluación. Esos instrumentos difieren en autoridad, alcance, obligatoriedad y grado de ejecución; el estudio los utiliza como comparadores de arquitectura institucional, no como una clasificación nacional de seguridad.

México: I+D en PQC; sin un instrumento nacional de transición comparable identificado al corte

El registro público mexicano revisado documenta actividad académica y de I+D: CIC-IPN reporta en 2026 un proyecto para desarrollar una infraestructura de clave pública (PKI) post-cuántica para aplicaciones en el IPN, e INAOE mantiene PQC entre sus líneas de investigación. Al corte, el protocolo no identificó en el registro público revisado un programa nacional de transición post-cuántica a escala federal o sectorial.

04 /

Resultados consolidados

Las 50 unidades permanecen como perfiles de evidencia. Sólo dos unidades presentan evidencia técnica local estimable, y únicamente en dos dimensiones cada una.

Resultados consolidados

0 / 50

ORS completo · EC 75-100%

0 / 50

ORS parcial · EC 50-74%

50 / 50

Perfil de evidencia · EC <50%

Sólo AWS Mexico Central y Google Cloud Querétaro presentan dimensiones localmente estimables, cada una con dos de diez dimensiones. Ninguna unidad alcanza un EC de al menos 50%; por tanto, el protocolo no autoriza publicar un ORS parcial ni completo.

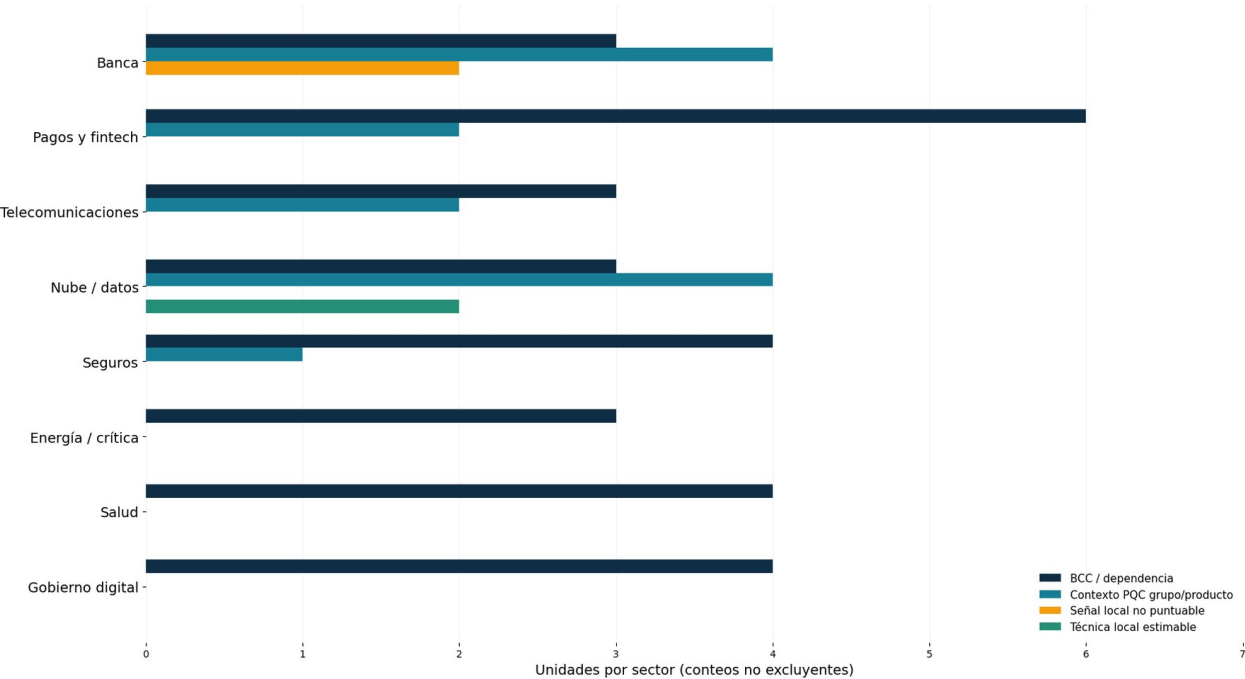


Figura 4. Observabilidad por sector dentro del panel. Los conteos son no excluyentes y no constituyen tasas poblacionales.

Infraestructura de nube: único ámbito con evidencia técnica localmente estimable

Unidad	Dimensiones estimables	EC	Alcance	Resultado reportable
AWS Mexico Central	D5 = M4; D8 = M4	20%	MX-COMPONENT / DIRECT	Perfil de evidencia
Google Cloud Querétaro	D5 = M4; D8 = M4	20%	MX-COMPONENT / DIRECT	Perfil de evidencia

AWS KMS documenta ML-KEM híbrido en TLS para endpoints no FIPS de todas las regiones de la partición aws; la región AWS Mexico (Central), mx-central-1, opera desde el 14 de enero de 2025. Google Cloud documenta la disponibilidad general de ML-DSA, SLH-DSA y ML-KEM en Cloud KMS; el servicio está disponible en northamerica-south1 (México), cuyas zonas de infraestructura se localizan en Querétaro. Bajo el Codebook, esta combinación permite atribuir capacidad a componentes locales concretos; no permite inferir madurez organizacional completa ni adopción por clientes.

RESTRICCIÓN DE INTERPRETACIÓN DEL NIVEL M4

M4 describe la madurez de una dimensión estimable, no de la organización en su conjunto. Con EC=20%, el Codebook prohíbe producir un ORS agregado. “Dos dimensiones en M4” y “80% de madurez organizacional” son afirmaciones metodológicamente distintas; sólo la primera está sustentada.

Santander México y Banorte: señales locales sin evidencia suficiente para una adjudicación de madurez

Santander México presenta una señal local pública relacionada con PQC, pero las iniciativas del Grupo Santander no se atribuyen a México sin un vínculo explícito. Banorte presenta una señal local que no supera la puerta de evidencia requerida para adjudicar madurez.

Lectura del resultado de 500 decisiones dimensionales

De las 500 decisiones entidad-dimensión, cuatro resultaron estimables. Las 496 restantes no superaron la puerta de evidencia para la afirmación, el alcance y la dimensión definidos. La metodología conserva esas decisiones como no estimables y evita imputar valores allí donde el registro público no permite observarlos.

ROBUSTEZ DEL RESULTADO PRINCIPAL

El EC máximo observado es 20%. En consecuencia, la conclusión “0 ORS organizacionales reportables” se mantiene para cualquier umbral de reportabilidad superior a 20%. La distancia respecto de 50% y 75% indica que el resultado no depende de una variación marginal de los umbrales congelados.

Implicaciones ejecutivas

- Esta edición no publica una clasificación ordinal entre unidades. Construir la con cobertura insuficiente introduciría una precisión aparente no sustentada por la evidencia.
- La ausencia de puntuación agregada es un resultado metodológico: identifica dónde falta evidencia local, atribuible y dimensionalmente suficiente.
- En futuras ediciones, el instrumento está diseñado para detectar variación temprana en inventario, vínculos locales de atribución, pruebas y gobernanza de terceros antes de requerir evidencia de despliegues de gran escala.

ALCANCE INFERENCIAL

Con un EC máximo de 20%, ninguna de las 50 unidades alcanza la cobertura exigida para un ORS organizacional. El resultado reportable es, por tanto, un perfil de evidencia.

05 /

Lectura sectorial

La observabilidad varía entre sectores. Documentación, arquitectura, tercerización y ciclo de activos condicionan lo que puede demostrarse públicamente.

Lectura sectorial

Sector	n	Ctx	BCC	Señal	Téc.	Fuente retenida	Lectura
Banca y autoridad monetaria	9	4	3	2	0	1	La principal restricción de estimabilidad es la ausencia de vínculos públicos de atribución entre programas de grupo y sistemas mexicanos.
Pagos y fintech	12	2	6	0	0	0	Dependencias criptográficas visibles; rara vez conectadas públicamente con una estrategia PQC local.
Telecom.	6	2	3	0	0	0	Contexto global y BCC existen, pero la evidencia local es fragmentaria.
Nube / datos	5	4	3	0	2	0	Único sector con técnica local estimable; mayor observabilidad documental, no necesariamente mayor madurez interna.
Seguros	5	1	4	0	0	0	Datos de larga vida y BCC observable; escasa evidencia PQC organizacional local.
Energía / crítica	5	0	3	0	0	0	La criticidad no autoriza a inferir transición; no hay evidencia local suficiente para estimar.
Salud	4	0	4	0	0	0	BCC en todo el subpanel; longevidad relevante para HNDL, sin presuponer migración.
Gobierno digital	4	0	4	0	0	0	Dependencias convencionales visibles; no se identificó transición PQC localmente estimable.

La observabilidad está condicionada por el régimen de divulgación

Los proveedores de nube publican documentación técnica, APIs, regiones, algoritmos y hojas de ruta con un grado de detalle que permite cerrar locus y capacidad a nivel de componente. Bancos, aseguradoras, instituciones de salud o infraestructuras críticas pueden desarrollar trabajo interno sustantivo y divulgar muy poco. Este mecanismo de datos faltantes es plausiblemente no aleatorio; por ello, las diferencias sectoriales de observabilidad no se interpretan como una jerarquía de seguridad ni de madurez. Los conteos sectoriales describen el registro público del panel, no la prevalencia de preparación interna; comparar sectores como si compartieran una misma propensión a divulgar produciría una inferencia que el diseño no sustenta.

06 /

Pagos: dependencia criptográfica interorganizacional

En pagos, la transición post-cuántica no se agota en ML-KEM: involucra claves, firmas, certificados, PAN, tokenización, APIs, procesadores, redes y terceros dentro de una arquitectura interoperable.

La transición como cadena de confianza interorganizacional

La superficie criptográfica sujeta a migración atraviesa límites organizacionales; por ello, la gobernanza de proveedores constituye un componente estructural de la transición.

Los sistemas de pago combinan componentes que rara vez cambian al mismo ritmo: HSM, PIN/EMV, TLS, PKI, tokenización, claves de red, APIs, software de terminal, procesadores y acuerdos con terceros. La migración post-cuántica puede fallar aun cuando la selección algorítmica sea correcta si algún eslabón no puede negociar, rotar, validar o retirarse de manera coordinada. En este contexto, PAN se refiere al número primario de cuenta (Primary Account Number).

Cinco fuentes estructurales de complejidad en pagos

#	Reto	Implicación
1	Inventario distribuido	Las dependencias criptográficas viven en aplicaciones, HSM, certificados, redes, proveedores y contratos.
2	Compatibilidad	La coexistencia clásica/PQC puede prolongarse durante años; una negociación criptográfica más robusta pierde utilidad si un componente impide la interoperabilidad.
3	Ciclos asimétricos	Tarjetas, terminales, dispositivos especializados, software y servicios de nube tienen ritmos de renovación distintos.
4	Custodia y responsabilidad	Una organización puede ser responsable de gestionar un riesgo cuya dependencia técnica reside en un tercero.
5	Aseguramiento	Migrar sin reversión controlada, pruebas de regresión, monitoreo y retiro de componentes heredados puede introducir riesgo adicional.

PREGUNTA DE ARQUITECTURA

¿Qué dependencia criptográfica controla realmente la organización, cuál controla un tercero y qué evidencia contractual o técnica existe de que ambas migrarán en el orden correcto?

07 /

Priorización por horizonte de exposición

La priorización del riesgo no depende de predecir la fecha de disponibilidad de una computadora cuántica criptográficamente relevante; depende de relacionar longevidad, tiempo de migración y exposición.

Priorización por horizonte de exposición

El problema de priorización puede formularse con precisión: ¿durante cuánto tiempo debe permanecer confidencial o auténtico este activo, cuánto tardará en migrar y qué dependencias impiden ese cambio? Este marco de decisión permite separar urgencia material de formulaciones genéricas de riesgo.

Activo	Horizonte	Pregunta de transición
Identidad / población	Largo	¿Biometría o evidencia de identidad debe seguir protegida después del ciclo de renovación actual?
Salud	Largo	¿Qué expedientes o datos sensibles retienen valor durante décadas?
Finanzas / pagos	Variable	¿Qué datos, firmas o credenciales sobreviven más que el sistema que hoy los protege?
Infraestructura crítica	Largo / operativo	¿Qué secretos, firmware, certificados o canales tienen ciclos de vida extensos?
Sesiones efímeras	Corto	¿La prioridad real está en negociación criptográfica, disponibilidad y compatibilidad más que en confidencialidad de largo plazo?

El estudio no asigna probabilidades HNDL a organizaciones específicas a partir de evidencia pública. Utiliza la longevidad como una dimensión de priorización y como recordatorio de que la exposición criptográfica puede acumularse antes de que el cambio tecnológico sea visible externamente.

08 /

Del inventario criptográfico a la resiliencia operacional

En el ciclo 2027, la evidencia de mayor valor analítico será la que conecte inventario, priorización, diseño, prueba, despliegue, retiro y aseguramiento.

Del inventario criptográfico a la resiliencia operacional

Bajo este diseño, la transición post-cuántica se vuelve observable, en primera instancia, como una disciplina de arquitectura, inventario y gestión de dependencias; posteriormente, como despliegue y retiro controlado.

Etapa	Evidencia que aumenta la estimabilidad
1. Descubrir	Inventario criptográfico ligado a activos, propietarios, datos y terceros.
2. Priorizar	Longevidad del dato, criticidad, dependencia y horizonte de renovación.
3. Diseñar	Arquitectura objetivo, cryptoagilidad, estándares y estrategia híbrida/coexistencia.
4. Probar	Interoperabilidad, rendimiento, modos de fallo, reversión controlada y evidencia reproducible.
5. Desplegar	Producción en alcance definido con observabilidad y gestión de excepciones.
6. Retirar	Retirar algoritmos, raíces de confianza y componentes heredados vulnerables; demostrar que no quedaron rutas residuales.
7. Asegurar	Monitorear, medir, revalidar proveedores y ejercitar recuperación.

Evidencia prioritaria para el ciclo 2027

Si el registro público comienza a mostrar inventarios, hojas de ruta, pruebas, capacidades regionales, gobernanza de proveedores, retiro de componentes heredados y aseguramiento, el instrumento podrá medir cambio con mayor cobertura. El objetivo no es maximizar el número de puntajes, sino aumentar la capacidad del diseño para discriminar diferencias reales de evidencia sin sacrificar validez de constructo.

Qué monitorear en el siguiente ciclo

- Publicación de inventarios o métodos de descubrimiento criptográfico.
- Hojas de ruta con responsables, alcance e hitos.
- Vínculos explícitos de atribución entre programas globales y operaciones mexicanas.
- Soporte regional de KMS/HSM/PKI/TLS y evidencia de producción.
- Pilotos con resultados, rendimiento e interoperabilidad documentados.
- Requisitos PQC en procesos de adquisición y contratos de terceros.
- Retiro de algoritmos vulnerables y controles de coexistencia.
- Métricas, excepciones, reversión controlada y resiliencia de la migración.

09 /

Panel analítico de 50 unidades / perfiles de evidencia

Todas las unidades permanecen como perfiles de evidencia; el orden de presentación es sectorial y no expresa una jerarquía de madurez.

Panel analítico de 50 unidades

Panel intencional de 50 unidades. Los conteos no deben extrapolarse como estimación poblacional para todas las organizaciones mexicanas.

Banca y autoridad monetaria

Unidad	Salida	Nota de evidencia
Santander México	Perfil de evidencia	Señal local PQC insuficiente para una dimensión estimable; contexto de grupo sin atribución local suficiente.
Banorte	Perfil de evidencia	Señal local insuficiente para adjudicar madurez.
BBVA México	Perfil de evidencia	Contexto de grupo/producto sin vínculo local suficiente de atribución.
Citi México	Perfil de evidencia	Contexto insuficiente para un ORS local.
HSBC México	Perfil de evidencia	Contexto insuficiente para un ORS local.
Scotiabank México	Perfil de evidencia	Contexto insuficiente para un ORS local.
Banco de México	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
Banamex	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
Banco Inbursa	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.

Pagos y fintech

Unidad	Salida	Nota de evidencia
Visa México	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
Mastercard México	Perfil de evidencia	Contexto global no equivale a madurez local.
Prosa	Perfil de evidencia	Las dependencias BCC no constituyen, por sí solas, evidencia de transición PQC.
Cecoban	Perfil de evidencia	Las dependencias BCC no constituyen, por sí solas, evidencia de transición PQC.
STP	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
Clip	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
Conekta	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
Nu México	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
E-Global	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
Mercado Pago Wallet México	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
Spin by OXXO	Perfil de evidencia	Señal/contexto insuficiente para una dimensión estimable bajo el protocolo.
Ualá México	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.

Telecomunicaciones

Unidad	Salida	Nota de evidencia
AT&T México	Perfil de evidencia	Contexto/BCC sin vínculo de atribución o detalle suficiente.
Telefónica Movistar México	Perfil de evidencia	Contexto global PQC sin vínculo mexicano de atribución suficiente.
América Móvil México	Perfil de evidencia	BCC/dependencias observables; sin transición local estimable.
Grupo Televisa / izzi	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
Megacable	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
Totalplay	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.

Nube e infraestructura de datos

Unidad	Salida	Nota de evidencia
AWS Mexico Central	Perfil de evidencia	D5=M4, D8=M4, EC=20%, MX-COMPONENT / DIRECT.
Google Cloud Querétaro	Perfil de evidencia	D5=M4, D8=M4, EC=20%, MX-COMPONENT / DIRECT.
Microsoft Azure Mexico Central	Perfil de evidencia	Contexto o capacidad de proveedor sin evidencia local suficiente para un ORS.
Oracle Cloud México	Perfil de evidencia	Contexto o capacidad de proveedor sin evidencia local suficiente para un ORS.
KIO Networks	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.

Seguros

Unidad	Salida	Nota de evidencia
BBVA Seguros México	Perfil de evidencia	Contexto insuficiente para un ORS local.
MetLife México	Perfil de evidencia	BCC/dependencias; sin transición PQC local estimable.
Quálitas	Perfil de evidencia	BCC/dependencias; sin transición PQC local estimable.
Seguros Banorte	Perfil de evidencia	BCC/dependencias; sin transición PQC local estimable.
GNP Seguros	Perfil de evidencia	BCC/dependencias; sin transición PQC local estimable.

Energía e infraestructura crítica

Unidad	Salida	Nota de evidencia
CENACE	Perfil de evidencia	Criticidad/BCC no autoriza inferencia de transición PQC.
CENAGAS	Perfil de evidencia	Criticidad/BCC no autoriza inferencia de transición PQC.

Unidad	Salida	Nota de evidencia
CNE	Perfil de evidencia	Sin dimensiones localmente estimables bajo el protocolo.
CFE	Perfil de evidencia	BCC/dependencias; sin transición PQC local estimable.
Pemex	Perfil de evidencia	BCC/dependencias; sin transición PQC local estimable.

Salud

Unidad	Salida	Nota de evidencia
IMSS	Perfil de evidencia	BCC/dependencias observables; sin transición PQC local estimable.
ISSSTE	Perfil de evidencia	BCC/dependencias observables; sin transición PQC local estimable.
IMSS-Bienestar	Perfil de evidencia	BCC/dependencias observables; sin transición PQC local estimable.
Secretaría de Salud / CCINSHAE	Perfil de evidencia	BCC/dependencias observables; sin transición PQC local estimable.

Gobierno digital

Unidad	Salida	Nota de evidencia
ATDT	Perfil de evidencia	BCC/dependencias; sin transición PQC local estimable.
RENAPO	Perfil de evidencia	BCC/dependencias; respuesta institucional formal: no se identificó fuente pública institucional de transición PQC; sin dimensión estimable.
SAT	Perfil de evidencia	BCC/dependencias; sin transición PQC local estimable.
ANAM	Perfil de evidencia	BCC/dependencias; sin transición PQC local estimable.

10 /

Validez, fuentes y trazabilidad

La solidez del resultado depende de las afirmaciones que la evidencia permite sostener, de las inferencias que el método excluye y de la capacidad de reconstruir cada adjudicación.

Validez, sesgos de observabilidad y límites inferenciales

- Panel intencional: los conteos describen las 50 unidades codificadas; no son estimaciones poblacionales ni permiten inferir prevalencias para todas las organizaciones mexicanas.
- Validez temporal: las fuentes pueden cambiar, desaparecer o actualizarse. El corte principal de evidencia es el 2 de septiembre de 2026.
- Datos no observados: NE no es M0; una dimensión no estimable permanece sin valor y no reduce artificialmente un puntaje.
- Separación de constructos: la evidencia de criptografía convencional se conserva como BCC, pero no se transforma en transición PQC sin vínculo explícito.
- Atribución local: programas de grupo, capacidades de proveedor y productos globales requieren evidencia separada de aplicabilidad cuando la afirmación se refiere a México.
- Precisión factual: únicamente una corrección factual o una nueva fuente pública verificable podía modificar una adjudicación; la metodología permaneció congelada.
- Alcance de validación: el estudio evalúa evidencia pública de transición PQC; configuraciones internas, eficacia de controles y cumplimiento quedan fuera del objeto de estimación.

Amenazas a la validez y salvaguardas de diseño

Amenaza	Riesgo de inferencia	Salvaguarda
Sesgo de divulgación	La visibilidad pública puede diferir por sector y régimen institucional.	EC separado de madurez; NE no se imputa; no se publica una clasificación ordinal sectorial.
Error de atribución	Evidencia de grupo o proveedor puede atribuirse indebidamente a México.	Locus explícito, reglas de herencia y vínculo de atribución obligatorio.
Datos faltantes no aleatorios	El silencio documental puede correlacionarse con sensibilidad operativa o práctica de divulgación.	NE como no observación; sin M0 implícito ni promedios con celdas faltantes.
Deriva de fuentes	Contenido web puede cambiar después de la codificación.	Fecha de corte, estado de fuente, revalidación y retención de fuentes cambiadas.
Grados de libertad del investigador	Cambios ex post en pesos, puertas o umbrales podrían favorecer resultados.	Codebook congelado, enmiendas documentadas y adjudicación separada.
Validez temporal	La transición PQC es dinámica.	Resultados fechados; replicación futura debe aplicar el mismo protocolo o documentar versión nueva.

Referencias metodológicas

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods* (4th ed.). SAGE. Krippendorff, K. (2018). *Content Analysis: An Introduction to Its Methodology* (4th ed.). SAGE. Little, R. J. A., & Rubin, D. B. (2019). *Statistical Analysis with Missing Data* (3rd ed.). Wiley.

Referencias primarias - estándares, políticas y migración

National Institute of Standards and Technology (2024). *FIPS 203, 204 y 205*: [Fuente oficial](#)

NCCoE / NIST. *Migration to Post-Quantum Cryptography*: [Fuente oficial](#)

The White House (2026, 22 junio). *Executive Order 14412 - Securing the Nation Against Advanced Cryptographic Attacks*: [Fuente oficial](#)

Canadian Centre for Cyber Security. *Roadmap for the migration to post-quantum cryptography for the Government of Canada*: [Fuente oficial](#)

UK National Cyber Security Centre. *Timelines for migration to post-quantum cryptography*: [Fuente oficial](#)

European Commission / NIS Cooperation Group (2025). *Coordinated Implementation Roadmap for the Transition to PQC*: [Fuente oficial](#)

Australian Signals Directorate. *Planning for post-quantum cryptography*: [Fuente oficial](#)

Cyber Security Agency of Singapore (2026, 16 julio). *Quantum-Safe Migration Handbook and Quantum Readiness Index*: [Fuente oficial](#)

Japan National Cybersecurity Office (2025). *Cybersecurity Strategy 2025*: [Fuente oficial](#)

KISA (2026). Post-quantum cryptography pilot transition programme: [Fuente oficial](#)

Instituto Nacional de Tecnologia da Informação (Brasil). Portaria ITI nº 38 — GTT-PQC/ICP-Brasil: [Fuente oficial](#)

Referencias primarias - México e infraestructura de nube

CIC-IPN (2026). Desarrollo de una infraestructura de clave pública (PKI) postcuántica para aplicaciones en el IPN: Fuente oficial

INAOE. Línea de investigación en criptografía post-cuántica: Fuente oficial

AWS Key Management Service. Hybrid post-quantum TLS: Fuente oficial

AWS (2025, 14 de enero). AWS Mexico (Central) Region, mx-central-1: Fuente oficial

Google Cloud (2026, 11 de agosto). Post-quantum cryptography roadmap: Fuente oficial

Google Cloud KMS (2026, 28 de julio). Quantum-safe digital signatures and ML-KEM: Fuente oficial

Google Cloud. Cloud KMS locations / Compute Engine regions and zones — northamerica-south1 (México/Querétaro): Fuente oficial

Trazabilidad del estudio

El registro de trazabilidad conserva las 500 decisiones entidad-dimensión con dimensión, peso, estimabilidad, madurez, puntos, locus de alcance, modo de dependencia, clase S/F/T, identificadores de evidencia, estado de fuente, ECS, URL y justificación de adjudicación. El perímetro final y el Codebook v1.0 quedaron bajo control de versión. La revisión final de validez verificó consistencia de atribución, alcance, lenguaje causal, tratamiento de evidencia no observable y congruencia entre el registro de trazabilidad y las conclusiones reportadas.

REPRODUCIBILIDAD

La reproducibilidad depende de que cada adjudicación pueda reconstruirse desde la fuente, el alcance, la regla aplicada y la justificación. El diseño privilegia esa trazabilidad sobre la densidad de puntajes.

Protocolo mínimo de replicación

Paso	Requisito reproducible
1	Fijar versión del Codebook y fecha de corte antes de adjudicar.
2	Recolectar evidencia por unidad-dimensión y registrar fuente, locus y estado.
3	Resolver elegibilidad antes de asignar M1-M5; conservar NE sin imputación.
4	Aplicar codificación independiente/adjudicación y documentar desacuerdos.
5	Calcular EC y sólo después determinar si el ORS puede publicarse.



Implicaciones estratégicas

Bajo este diseño, la transición post-cuántica se vuelve observable como una disciplina de arquitectura, inventario y gestión de dependencias y, después, como despliegue y retiro controlado.

Cierre

Esta primera edición no encuentra fundamento empírico suficiente para sostener una clasificación ordinal entre las unidades del panel. Su contribución principal es identificar y caracterizar la brecha entre la observabilidad de las dependencias criptográficas y la observabilidad de una transición post-cuántica localmente atribuible.

Ese contraste orienta la agenda del siguiente ciclo. En 2027, el indicador metodológicamente más relevante será si se reduce mediante evidencia de inventarios, hojas de ruta, pruebas, capacidades regionales, gobernanza de terceros, retiro y aseguramiento. Si la cobertura supera los umbrales predefinidos, el ORS podrá discriminar diferencias organizacionales sin sustituir evidencia por inferencia.

PREGUNTA DE GOBIERNO CRIPTOGRÁFICO

¿Qué componentes concentran funciones críticas de confianza criptográfica y en qué medida la organización puede identificarlos, gobernarlos, sustituirlos y demostrar su capacidad de migración?

Implicaciones estratégicas

La cuestión estratégica no consiste en declarar la adopción de PQC, sino en demostrar qué dependencias criptográficas deben modificarse, quién ejerce control sobre ellas, qué datos y mecanismos de confianza están expuestos a horizontes prolongados y mediante qué arquitectura de migración pueden sustituirse sin degradar la seguridad, la interoperabilidad ni la continuidad.

ZERO TRUST CONSULTING

<https://zerotrust.consulting>