

Ley que establece la transición de las entidades públicas a la criptografía resistente a la computación cuántica y promueve la investigación en tecnologías cuánticas

Encarga a la Secretaría de Gobierno y Transformación Digital, a través del Centro Nacional de Seguridad Digital, una hoja de ruta nacional de migración a criptografía poscuántica con esquemas híbridos; obliga a las entidades del Poder Ejecutivo y descentralizadas a inventariar su criptografía (los inventarios de defensa e inteligencia quedan en el MINDEF y la DINI); pide al RENIEC un plan propio para el DNIe; incorpora la agilidad criptográfica en las compras, la preservación a largo plazo de documentos firmados y prioriza las tecnologías cuánticas en el Sinacti.

Comisión (Cámara de Diputados): Ciencia, Innovación Tecnológica y Sociedad Digital (+ Defensa Nacional y Orden Interno) ·

Revisora (Senado): En asuntos de Salud, Educación, Cultura, Mujer y Desarrollo Social y Digital · **Prioridad:** media · **Costo fiscal:** medio · **Plazo:** largo

Plan Perú 2050: Ciber Seguridad, Transformación Digital, Ciencia y Tecnología

I. Exposición de motivos

Los sistemas del Estado protegen información y firmas con criptografía de clave pública (RSA y curvas elípticas) que podría quedar vulnerable ante computadoras cuánticas suficientemente potentes; el riesgo es actual porque datos cifrados capturados hoy pueden descifrarse en el futuro ('capturar ahora, descifrar después'), lo que afecta información con valor de confidencialidad de largo plazo (salud, identidad, defensa, tributaria) y documentos firmados digitalmente que deben seguir siendo verificables por décadas. En agosto de 2024 el NIST de los Estados Unidos publicó los primeros estándares de criptografía poscuántica (FIPS 203 y FIPS 204, entre otros) y su borrador IR 8547 propone retirar progresivamente los algoritmos vulnerables; la Public Law 117-260 de los Estados Unidos obliga a las agencias federales a inventariar sus sistemas criptográficos. En el Perú, el Decreto Legislativo 1412 (Gobierno Digital), el Decreto de Urgencia 007-2020 (Marco de Confianza Digital) y la Ley 27269 (Firmas y Certificados Digitales) dan base institucional, pero no existe un inventario ni un plan de migración, y la migración de grandes sistemas toma años. El activo más difícil de migrar es el DNI electrónico, cuyos certificados residen en un chip con algoritmos RSA o de curvas elípticas y cuya sustitución sigue ciclos de renovación de varios años; por ello el RENIEC, como entidad de certificación del Estado, debe contar con un plan propio. Según la API del SPLEY, no hay proyectos de ley en 2021-2026 sobre tecnologías cuánticas o criptografía poscuántica.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY QUE ESTABLECE LA TRANSICIÓN DE LAS ENTIDADES PÚBLICAS A LA CRIPTOGRAFÍA RESISTENTE A LA COMPUTACIÓN CUÁNTICA Y PROMUEVE LA INVESTIGACIÓN EN TECNOLOGÍAS CUÁNTICAS

Artículo 1. Objeto

La presente ley tiene por objeto establecer la transición planificada de las entidades de la Administración Pública a algoritmos criptográficos resistentes a la computación cuántica y promover la investigación, el desarrollo y la formación en tecnologías cuánticas.

Artículo 2. Ámbito

2.1 La presente ley se aplica a las entidades del Poder Ejecutivo, a los gobiernos regionales y locales y a las demás entidades comprendidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, aprobado por el Decreto Supremo 006-2026-JUS, con excepción de las señaladas en el numeral 2.2. A los prestadores de servicios de certificación digital acreditados les es aplicable únicamente el artículo 8. 2.2 El Poder Legislativo, el Poder Judicial y los organismos constitucionalmente autónomos aprueban, conforme a su autonomía, su propio plan de migración tomando como referencia la hoja de ruta nacional, pueden adherirse a ella mediante convenio con la Presidencia del

Consejo de Ministros e informan anualmente a la Secretaría de Gobierno y Transformación Digital indicadores agregados de avance.

Artículo 3. Hoja de ruta nacional de migración

3.1 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, en su calidad de ente rector de la seguridad digital conforme al Decreto de Urgencia 007-2020, su reglamento aprobado por el Decreto Supremo 126-2025-PCM, y el Decreto Legislativo 1412, y por medio del Centro Nacional de Seguridad Digital, aprueba la Hoja de Ruta Nacional de Migración a Criptografía Poscuántica, en coordinación con el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), en su calidad de Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Electrónica; con el Registro Nacional de Identificación y Estado Civil (RENIEC), en su calidad de entidad de certificación del Estado; y con el Ministerio de Defensa. 3.2 La hoja de ruta establece, con base en estándares internacionales abiertos, tales como los publicados por el NIST, la ISO/IEC y el IETF: a) los algoritmos de establecimiento de claves y de firma resistentes a la computación cuántica; b) el uso de esquemas híbridos, que combinan algoritmos clásicos y poscuánticos, durante la transición, cuando corresponda; c) las longitudes mínimas de claves simétricas y de funciones resumen; y d) las fases, los criterios de priorización y los mecanismos de seguimiento. Prioriza algoritmos estandarizados y evaluados públicamente y no recomienda algoritmos propietarios o no publicados. Se actualiza cada dos años.

Artículo 4. Inventario criptográfico

4.1 Cada entidad comprendida en el numeral 2.1 elabora y mantiene actualizado un inventario de los sistemas, servicios, certificados y dispositivos que emplean criptografía, con énfasis en la de clave pública, identificando los algoritmos, su función, el tiempo durante el cual la información protegida debe mantenerse confidencial y la dependencia de proveedores. 4.2 El inventario se remite a la Secretaría de Gobierno y Transformación Digital por canales cifrados dentro de los dieciocho meses siguientes a la aprobación de la hoja de ruta y, en adelante, con periodicidad anual. 4.3 La información del inventario cuya divulgación permita identificar vulnerabilidades explotables de los sistemas constituye excepción al derecho de acceso a la información pública conforme al numeral 6 del artículo 17 del Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado por el Decreto Supremo 021-2019-JUS, mientras subsista dicho riesgo y por un plazo máximo de cinco años renovable. La Secretaría custodia los inventarios con control de acceso por necesidad de conocer, cifrado y registro de accesos, y publica únicamente indicadores agregados de avance. 4.4 Los inventarios de los sistemas de defensa nacional y del Sistema de Inteligencia Nacional se elaboran y custodian por el Ministerio de Defensa y por la Dirección Nacional de Inteligencia, respectivamente, conforme a la Ley 30999, Ley de Ciberdefensa, y al Decreto Legislativo 1141, que remiten a la Secretaría de Gobierno y Transformación Digital únicamente indicadores agregados de avance.

Artículo 5. Priorización

Las entidades priorizan la migración de: a) sistemas que protegen información con necesidad de confidencialidad por más de diez años, incluida la información crítica para la continuidad del Estado conforme a la clasificación prevista en la ley que establece el marco de nube del Estado, o la que haga sus veces; b) sistemas de identidad digital, firma digital y sellado de tiempo; c) servicios digitales que soporten infraestructuras críticas, conforme a la normativa vigente sobre activos críticos nacionales; y d) comunicaciones de seguridad y defensa nacional.

Artículo 6. Agilidad criptográfica en las contrataciones

6.1 En las contrataciones de bienes y servicios de tecnología que incorporen funciones criptográficas, las entidades incluyen en los requerimientos la capacidad de actualizar los algoritmos sin sustitución integral del sistema y la compatibilidad con los estándares recomendados en la hoja de ruta, conforme a la Ley 32069, Ley General de Contrataciones Públicas, y su reglamento. 6.2 La Secretaría de Gobierno y Transformación Digital publica especificaciones de referencia para dicho fin, que el Organismo Especializado para las Contrataciones Públicas Eficientes puede incorporar en sus documentos estándar.

Artículo 7. Metas indicativas

La hoja de ruta establece como meta indicativa que las entidades completen la migración de los sistemas comprendidos en los literales a) y b) del artículo 5 al año 2032 y del resto de sistemas priorizados al año 2035,

sujeta a la programación multianual y a la disponibilidad presupuestal de cada entidad, aprovechando los ciclos ordinarios de renovación tecnológica. La hoja de ruta prioriza la habilitación del establecimiento de claves híbrido o poscuántico en los servicios web públicos, en la medida en que el software disponible lo permita.

Artículo 8. Infraestructura Oficial de Firma Electrónica y DNI electrónico

8.1 El INDECOPI, en su calidad de Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Electrónica conforme a la Ley 27269, Ley de Firmas y Certificados Digitales, y su reglamento, aprobado por el Decreto Supremo 052-2008-PCM, actualiza los requisitos de acreditación de las entidades de certificación y de los prestadores de servicios de valor añadido para incorporar algoritmos resistentes a la computación cuántica, una vez adoptados en la hoja de ruta, con periodos de transición que no afecten la validez de los certificados vigentes. 8.2 Los documentos firmados digitalmente conservan su validez jurídica. Las entidades que custodian documentos firmados de conservación prolongada aplican, antes de que los algoritmos empleados sean declarados inseguros en la hoja de ruta, sellos de tiempo o registros de evidencia con algoritmos vigentes, conforme a los estándares técnicos de preservación de firmas que apruebe el INDECOPI. 8.3 El RENIEC, en el marco de su autonomía y de la Ley 27269, aprueba y publica un plan de migración de los certificados del documento nacional de identidad electrónico, del documento nacional de identidad digital y de su infraestructura de certificación, compatible con la hoja de ruta, que prevea la emisión de nuevos documentos con capacidad criptográfica poscuántica o híbrida en sus ciclos ordinarios de renovación.

Artículo 9. Investigación y formación en tecnologías cuánticas

El Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica (CONCYTEC) incorpora las tecnologías cuánticas (computación, comunicaciones, sensores y criptografía) entre las áreas priorizadas del Sinacti y promueve la cooperación internacional, la formación de posgrado y el acceso de investigadores nacionales a infraestructura de cómputo cuántico, en articulación con la red nacional de cómputo avanzado para la investigación o la que haga sus veces, con cargo a los instrumentos existentes. La investigación en distribución cuántica de claves no sustituye la migración a algoritmos poscuánticos prevista en la presente ley.

Artículo 10. Informe anual

La Secretaría de Gobierno y Transformación Digital publica anualmente un informe con indicadores agregados de avance del inventario y de la migración, y lo remite a la Comisión de Ciencia, Innovación Tecnológica y Sociedad Digital de la Cámara de Diputados y a la comisión competente del Senado.

Primera. Disposición Complementaria Final

Reglamentación. El Poder Ejecutivo reglamenta la presente ley en un plazo de ciento veinte días hábiles contados a partir del día siguiente de su publicación, mediante decreto supremo refrendado por el Presidente del Consejo de Ministros y el Ministro de Defensa.

Segunda. Disposición Complementaria Final

Hoja de ruta. La Hoja de Ruta Nacional de Migración a Criptografía Poscuántica se aprueba mediante resolución de la Secretaría de Gobierno y Transformación Digital en un plazo de doce meses contados a partir del día siguiente de la publicación de la presente ley.

Tercera. Disposición Complementaria Final

Activos críticos privados. Los reguladores sectoriales promueven, en el marco de sus competencias, que los operadores de activos críticos nacionales adopten planes de migración compatibles con la hoja de ruta.

Cuarta. Disposición Complementaria Final

Financiamiento. La implementación de la presente ley se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público y sujeta a disponibilidad presupuestal.

III. Análisis costo-beneficio

La ley ordena planificar y no impone un plazo cerrado de gasto: la migración se integra a los ciclos ordinarios de renovación tecnológica y las metas son indicativas, sujetas a disponibilidad presupuestal. El costo identificable de corto plazo es el inventario criptográfico y la hoja de ruta (estimado S/ 3–9 millones en total). El

componente más costoso es la sustitución del DNle y de lectores; acoplada al ciclo ordinario de renovación, el sobre costo se limita a la diferencia de chip. El costo de la migración no es cuantificable con información pública; postergarlo lo eleva, y el mayor costo evitable es reemplazar equipos sin agilidad criptográfica comprados después de la ley. Habilitar el intercambio de claves híbrido en servicios web públicos tiene costo marginal. Requiere coordinación con el Poder Ejecutivo, fuente de financiamiento identificada e informe previo de sostenibilidad fiscal del MEF antes del dictamen.

Normas que modifica

- Decreto Legislativo 1412, Ley de Gobierno Digital, concordancia (rectoría) — *complementa*
- Decreto de Urgencia 007-2020, Marco de Confianza Digital, concordancia (seguridad digital) — *complementa*
- Ley 27269, Ley de Firmas y Certificados Digitales, concordancia (art. 7 de la propuesta) — *complementa*
- Ley 32069, Ley General de Contrataciones Públicas, requerimientos (art. 6 de la propuesta) — *complementa*
- Decreto Supremo 052-2008-PCM, Reglamento de la Ley 27269, requisitos de acreditación (art. 8.1) — *complementa*
- TUO de la Ley 27806, Decreto Supremo 021-2019-JUS, art. 17, numeral 6 (excepción por ley, art. 4.3) — *complementa*
- Ley 30999, Ley de Ciberdefensa, y Decreto Legislativo 1141, concordancia (art. 4.4) — *complementa*
- Ley 26497, Ley Orgánica del RENIEC, concordancia, no se modifica (art. 8.3) — *complementa*

Entidades implicadas (quién hace qué)

- **PCM-SGTD** (rectora): Aprueba y actualiza la hoja de ruta por medio del CNSD (art. 3), recibe y custodia inventarios (art. 4.2-4.3), publica especificaciones (art. 6) e informa anualmente (art. 10).
- **INDECOPI** (reglamentadora): Actualiza requisitos de acreditación de la IOFE (art. 8.1) y aprueba estándares de preservación de firmas (art. 8.2).
- **MINDEF** (ejecutora): Coordina la hoja de ruta (art. 3.1), elabora y custodia el inventario de sistemas de defensa y remite solo indicadores agregados (art. 4.4); refrenda el reglamento.
- **CONCYTEC** (ejecutora): Prioriza tecnologías cuánticas en el Sinacti (art. 9).
- — (regulada): Elaboran inventarios y migran sistemas priorizados (arts. 4, 5 y 8).
- **RENIEC** (ejecutora): Coordina la hoja de ruta y aprueba su plan de migración del DNle, DNI digital y su infraestructura de certificación (arts. 3.1 y 8.3).
- **DINI** (ejecutora): Elaborar y custodia el inventario del Sistema de Inteligencia Nacional y remite solo indicadores agregados (art. 4.4).
- **OECE** (consultiva): Puede incorporar especificaciones de agilidad criptográfica en documentos estándar (art. 6.2).
- — (regulada): Aprueban su propio plan conforme a su autonomía e informan indicadores agregados (art. 2.2).

Sujetos obligados: Entidades del Poder Ejecutivo, gobiernos regionales y locales y demás entidades del art. I del TUO de la Ley 27444, salvo Poderes Legislativo y Judicial y organismos constitucionalmente autónomos (plan propio e informe agregado); prestadores de certificación acreditados solo respecto del art. 8.

Beneficiarios: Ciudadanos y empresas cuya información y documentos firmados custodia el Estado; comunidad científica en tecnologías cuánticas.

Impacto económico estimado (confianza baja; referencial, no oficial)

Tipo: gasto

Costo para el Estado: S/ 3–9 millones (único, inventario y hoja de ruta); migración no cuantificable con información pública

Horizonte: 2027-2031

Financiamiento: Presupuesto institucional de los pliegos involucrados, sin demandar recursos adicionales al Tesoro Público y sujeto a disponibilidad presupuestal; requiere coordinación con el Poder Ejecutivo, fuente de financiamiento identificada e informe previo de sostenibilidad fiscal del MEF antes del dictamen (art. 79 de la Constitución; STC 00018-2023-PI/TC).

Supuestos: Estimación del editor: 300–600 entidades con sistemas relevantes (no existe cifra oficial verificada) y un costo medio de S/ 10–15 mil por inventario con personal propio y herramientas de descubrimiento; hoja de ruta con equipo de la SGTD. La migración se asume dentro de ciclos de renovación (5–8 años), por lo que su costo incremental depende del estado de cada sistema.

Beneficio para el Estado: Menor riesgo de exposición de información de largo plazo y continuidad de la validez de la firma digital; evita migraciones de emergencia más costosas. No cuantificable.

Beneficio para la sociedad: Protección de datos personales y de documentos firmados de los ciudadanos. No cuantificable.

Inversión privada: Demanda de servicios de ciberseguridad y actualización tecnológica; monto no estimable.

Costo para privados: Prestadores de certificación digital: actualización de infraestructura de clave pública en los periodos de transición.

Riesgos: Estándares aún en evolución (mitigado con actualización bienal y esquemas híbridos); baja capacidad técnica en entidades pequeñas; concentración del mapa de vulnerabilidades (mitigado: inventarios de defensa e inteligencia fuera de la SGTD, custodia cifrada y excepción de acceso del art. 4.3); retraso del DNle si el RENIEC no acopla la migración a su ciclo de renovación.

Revisión especializada (asistida por IA, sobre la versión anterior)

- **Constitucional** — Conforme: Propuesta constitucionalmente conforme: las metas son indicativas y sujetas a disponibilidad presupuestal (compatible con el art. 79 y la STC 00018-2023-PI/TC), no crea órganos y respeta la autonomía de los organismos constitucionales. Se sugiere extender la cláusula de autonomía a los poderes Legislativo y Judicial y precisar el fundamento legal de la reserva del inventario.
- **Técnica legislativa** — Con observaciones: Ley de planificación correcta: metas indicativas sujetas a disponibilidad presupuestal, sin organismos nuevos y con reglamentación del Poder Ejecutivo. Falta precisar qué obligaciones alcanzan a los prestadores privados de certificación, incluir al RENIEC como entidad de certificación del Estado y fundar la reserva del inventario en una excepción legal precisa.
- **Concordancia normativa** — Con observaciones: Sin duplicidad legal (no hay norma ni proyecto sobre criptografía poscuántica en SPLEY ni en data/antecedentes.json). Las normas citadas existen (D.Leg. 1412, D.U. 007-2020, Ley 27269, Ley 32069, Ley 31250). Faltan el reglamento del D.U. 007-2020 (D.S. 126-2025-PCM) y el reglamento de la Ley 27269 (D.S. 052-2008-PCM); el ámbito es internamente contradictorio respecto de los organismos autónomos; la reglamentación no tiene inicio de plazo y debe coordinarse con CIB-01, CIB-08, CIB-09 y GOB-13.
- **Seguridad** — Con observaciones: Propuesta técnicamente acertada (inventario, priorización por confidencialidad de largo plazo, agilidad criptográfica, metas alineadas con referentes internacionales). Debe evitar que el inventario de sistemas de defensa e inteligencia se concentre en una secretaría civil, en contra de la Ley 30999 y del régimen de inteligencia, reforzar la clasificación y custodia del inventario agregado y prever una transición híbrida y la adhesión efectiva de RENIEC como emisor de la PKI del DNle.
- **Derecho tecnológico** — Observaciones graves: Técnicamente bien fundada (FIPS 203/204, NIST IR 8547, Public Law 117-260) y con metas razonables (2032/2035, coherentes con el calendario NIST de desaprobación 2030 y retiro 2035). Omite a RENIEC como ECERNEP y emisor del DNle, cuyo chip es el activo criptográfico más difícil de migrar; debe exigir agilidad e hibridación, cubrir la criptografía simétrica y la preservación a largo plazo con estándares precisos, y evitar que la promoción de comunicaciones cuánticas se lea como sustituto de la PQC.

IV. Efecto de la vigencia de la norma

Complementa el Decreto Legislativo 1412, el Decreto de Urgencia 007-2020 y su reglamento (Decreto Supremo 126-2025-PCM), la Ley 27269 y su reglamento (Decreto Supremo 052-2008-PCM, que se adecuó), la Ley 32069, la Ley 31250 y el TUO de la Ley 27806 (excepción del art. 17.6). Se concuerda con la Ley 30999 y el Decreto Legislativo 1141 (inventarios de defensa e inteligencia). El art. 8.3 se formula dentro de las competencias del RENIEC como entidad de certificación del Estado conforme a la Ley 27269, sin modificar la Ley 26497; si en el dictamen se estimara que incide en las funciones de su ley orgánica, se tramita con votación de ley orgánica. Se coordina con las propuestas sobre el Centro Nacional de Seguridad Digital (CIB-01), DNI digital (CIB-08) y firma digital (CIB-09). No deroga normas.

V. Indicador de éxito al 2031

A 2031, la hoja de ruta está aprobada y actualizada; al menos el 80% de entidades del Poder Ejecutivo ha remitido su inventario criptográfico; el RENIEC ha publicado su plan de migración del DNle; los principales servicios web gov.pe admiten intercambio de claves híbrido; y la Infraestructura Oficial de Firma Electrónica cuenta con requisitos de acreditación que incorporan algoritmos poscuánticos.

Normas relacionadas

- Decreto Legislativo 1412, Ley de Gobierno Digital — <https://busquedas.elperuano.pe/dispositivo/NL/1691026-1>
- Decreto de Urgencia 007-2020, Marco de Confianza Digital — <https://busquedas.elperuano.pe/dispositivo/NL/1844001-2>
- Ley 27269, Ley de Firmas y Certificados Digitales — <https://leyes.congreso.gob.pe/Documentos/Leyes/27269.pdf>
- Ley 32069, Ley General de Contrataciones Públicas — https://leyes.congreso.gob.pe/Documentos/2021_2026/ADLP/Texto_Consolidado/32069-TXM.pdf
- Ley 31250, Ley del Sistema Nacional de Ciencia, Tecnología e Innovación — https://leyes.congreso.gob.pe/Documentos/2016_2021/ADLP/Normas_Legales/31250-LEY.pdf
- Ley 30999, Ley de Ciberdefensa — https://leyes.congreso.gob.pe/Documentos/2016_2021/ADLP/Normas_Legales/30999-LEY.pdf
- Decreto Legislativo 1141, de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional y de la DINI — <https://www.leyes.congreso.gob.pe/Documentos/DecretosLegislativos/01141.pdf>
- Decreto Supremo 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales — <https://www.gob.pe/institucion/pcm/normas-legales/292462-052-2008-pcm>

Antecedentes

No se identificaron en la API pública del SPLEY (consulta del 22-oct-2026) proyectos de ley con los términos 'cuántica', 'criptografía' o 'poscuántica' en el título (Congreso 2021-2026 y Cámara de Diputados 2026-2031) ni en data/antecedentes.json. Relacionados con la firma digital, sin tratar la migración criptográfica: PL 14841/2025-CR (eficacia plena de la firma digital; en comisión) y PL 10065/2024-CR (fecha cierta de documentos con firma digital; en comisión), verificados en la API SPLEY.

Referencias internacionales

- Estados Unidos: Public Law 117-260, Quantum Computing Cybersecurity Preparedness Act — <https://www.govinfo.gov/app/details/PLAW-117publ260>
- Estados Unidos: NIST FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard — <https://csrc.nist.gov/pubs/fips/203/final>
- Estados Unidos: NIST FIPS 204, Module-Lattice-Based Digital Signature Standard — <https://csrc.nist.gov/pubs/fips/204/final>
- Estados Unidos: NIST IR 8547 (borrador), Transition to Post-Quantum Cryptography Standards — <https://csrc.nist.gov/pubs/ir/8547/ipd>
- Internacional (IETF): RFC 4998, Evidence Record Syntax (preservación a largo plazo de firmas) — <https://www.rfc-editor.org/rfc/rfc4998>

Fuentes

- NIST IR 8547 (borrador), Transition to Post-Quantum Cryptography Standards — <https://csrc.nist.gov/pubs/ir/8547/ipd>
- NIST FIPS 203 — <https://csrc.nist.gov/pubs/fips/203/final>
- GovInfo: Public Law 117-260, Quantum Computing Cybersecurity Preparedness Act — <https://www.govinfo.gov/app/details/PLAW-117publ260>
- Plan Perú 2050, Comisión Perú en la Era Digital — <https://planperu2050.pe/c/peru-en-la-era-digital.html>

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/SOB-06.html>