

Ley que establece la subfamilia de puestos de ciberseguridad en el servicio civil y eleva a rango de ley la obligación de designar al oficial de seguridad y confianza digital en las entidades públicas

Encarga a SERVIR establecer, dentro de la familia de puestos de talento digital del servicio civil o la que haga sus veces, una subfamilia de ciberseguridad con perfiles por competencias, sin escala remunerativa nueva ni gasto adicional; eleva a rango de ley la obligación vigente de designar al oficial de seguridad y confianza digital con garantías de independencia y la posibilidad de compartirlo entre entidades pequeñas; y regula una reserva cívica de ciberseguridad con controles de acceso.

Comisión (Cámara de Diputados): Modernización de la Gestión del Estado y Contraloría (+ Ciencia, Innovación Tecnológica y Sociedad Digital) · **Revisora (Senado):** En asuntos de Gestión del Estado y Contraloría · **Prioridad:** media · **Costo fiscal:** nulo · **Plazo:** mediano

Plan Perú 2050: Ciber Seguridad, Reforma Del Estado, Capital Del Conocimiento

I. Exposición de motivos

Las entidades públicas compiten con el sector privado por un número reducido de especialistas en ciberseguridad y suelen cubrir la función con personal de tecnologías de la información sin especialización o mediante contratos temporales. El oficial de seguridad y confianza digital ya es obligatorio en las entidades públicas por norma reglamentaria (Decreto Supremo 029-2021-PCM, art. 111.3, y Decreto Supremo 126-2025-PCM, art. 11), y solo es facultativo en el sector privado (art. 15 del último); sin embargo, en muchas entidades, sobre todo municipalidades, el rol se asigna como función adicional, sin perfil, sin independencia respecto del área de tecnologías de la información y sin modelo para entidades pequeñas. No existe en el régimen de la Ley 30057 una agrupación de puestos de ciberseguridad con perfiles por competencias ni una ruta de formación. Estados Unidos estructura su fuerza laboral con el marco NICE del NIST, y la Ley 21.663 de Chile prevé encargados de ciberseguridad. No se dispone de un inventario oficial de profesionales de ciberseguridad en el Estado peruano. Por el artículo 79 de la Constitución, la mejora remunerativa no puede imponerse por iniciativa parlamentaria; esta propuesta se limita a ordenar perfiles, formación y garantías.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY QUE ESTABLECE LA SUBFAMILIA DE PUESTOS DE CIBERSEGURIDAD EN EL SERVICIO CIVIL Y ELEVA A RANGO DE LEY LA OBLIGACIÓN DE DESIGNAR AL OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL EN LAS ENTIDADES PÚBLICAS

Artículo 1. Objeto

La presente ley tiene por objeto fortalecer las capacidades de ciberseguridad del Estado mediante una subfamilia de puestos de ciberseguridad en el servicio civil y la designación obligatoria, con rango de ley, del oficial de seguridad y confianza digital en las entidades públicas.

Artículo 2. Subfamilia de puestos de ciberseguridad

2.1. La Autoridad Nacional del Servicio Civil (SERVIR), en coordinación con la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, establece en el régimen de la Ley 30057, Ley del Servicio Civil, una subfamilia de puestos de ciberseguridad dentro de la familia de puestos de talento digital o la que haga sus veces, con perfiles basados en un marco de competencias que comprenda, como mínimo, los roles de gobierno y riesgo, operación y monitoreo, respuesta a incidentes, arquitectura segura y auditoría.

2.2. Los puestos con acceso privilegiado a sistemas críticos se sujetan a verificación de antecedentes, compromisos de confidencialidad que subsisten tras el cese y revisión periódica de accesos.

2.3. La valorización de los puestos de la subfamilia se rige por las normas de compensación de la Ley 30057 y se sujeta a las leyes anuales de presupuesto y a la disponibilidad presupuestal de cada entidad. La presente ley no aprueba escalas, reajustes ni incrementos remunerativos.

Artículo 3. Oficial de seguridad y confianza digital

3.1. Toda entidad de la administración pública designa, entre su personal, un oficial de seguridad y confianza digital, con el perfil que apruebe SERVIR a propuesta de la Secretaría de Gobierno y Transformación Digital, dependencia funcional de la alta dirección y sin subordinación jerárquica al área de tecnologías de la información. La designación no implica la creación de plazas ni el incremento de remuneraciones.

3.2. El oficial no puede ejercer simultáneamente la jefatura de transformación digital ni la de tecnologías de la información de la entidad.

3.3. Las municipalidades y demás entidades de menor tamaño que determine el reglamento pueden designar un oficial compartido mediante convenio, o a través de la mancomunidad o del gobierno regional.

3.4. La acreditación del perfil la realiza SERVIR conforme al marco de competencias del artículo 2, reconociendo la formación de la Escuela Nacional de Administración Pública, universidades y certificaciones equivalentes, sin exigir una certificación comercial determinada.

3.5. La omisión de la designación en el plazo legal constituye falta disciplinaria del titular de la entidad o de quien haga sus veces, conforme a la Ley 30057.

Artículo 4. Formación

La Escuela Nacional de Administración Pública, en coordinación con universidades y con el Centro Nacional de Seguridad Digital, desarrolla, con cargo a su presupuesto institucional, programas de formación en ciberseguridad para servidores públicos, incluida una formación básica para directivos.

Artículo 5. Prácticas y jóvenes profesionales

Las entidades públicas pueden incorporar plazas de prácticas profesionales y preprofesionales en ciberseguridad dentro de sus programas vigentes, priorizando egresados de universidades e institutos de regiones, sujeto a su disponibilidad presupuestal.

Artículo 6. Reserva cívica de ciberseguridad

6.1. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, puede convocar mediante convenios a profesionales del sector privado y de la academia que integren voluntariamente, sin vínculo laboral ni retribución, una reserva cívica para apoyar la respuesta ante incidentes de gran escala.

6.2. Los integrantes son evaluados previamente en antecedentes e idoneidad, declaran conflictos de interés y actúan únicamente con mandato escrito de la entidad afectada, bajo coordinación del Centro Nacional de Seguridad Digital, que delimita alcance, sistemas y duración. Los accesos se otorgan con credenciales individuales, temporales y registradas.

6.3. Dichas actuaciones constituyen procedimientos autorizados para efectos del literal a) del artículo 12 de la Ley 30096, Ley de Delitos Informáticos. Los integrantes se consideran encargados de tratamiento conforme a la Ley 29733 y están sujetos a los deberes de confidencialidad de la Ley 27815, Ley del Código de Ética de la Función Pública. El convenio regula la responsabilidad por daños.

Artículo 7. Inventario de capacidades

SERVIR y la Presidencia del Consejo de Ministros levantan cada dos años un inventario de puestos y profesionales de ciberseguridad en el Estado y publican sus resultados agregados por nivel de gobierno y sector, sin identificar brechas por entidad.

Primera. Disposición Complementaria Final

Reglamentación. El Poder Ejecutivo, mediante decreto supremo refrendado por el presidente del Consejo de Ministros, reglamenta la presente ley en un plazo no mayor de ciento veinte días hábiles contados a partir del día siguiente de su publicación, y adecúa el artículo 111 del Decreto Supremo 029-2021-PCM y los artículos 11 y 15 del Decreto Supremo 126-2025-PCM.

Segunda. 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.

Tercera. Disposición Complementaria Final

Articulación con la familia de talento digital. Si a la entrada en vigencia de la presente ley no existiera la familia de puestos de talento digital, SERVIR establece la subfamilia de ciberseguridad dentro de la familia de puestos que corresponda según la normativa del servicio civil.

Única. Disposición Complementaria Transitoria

Implementación progresiva. La designación del oficial de seguridad y confianza digital con las garantías del artículo 3 es exigible a los seis meses para el Poder Ejecutivo, a los doce meses para los gobiernos regionales y a los veinticuatro meses para los gobiernos locales, contados desde la entrada en vigencia del reglamento.

III. Análisis costo-beneficio

No genera gasto adicional: la ley no aprueba escalas ni reajustes remunerativos, el oficial se designa entre el personal existente, la formación de ENAP y los perfiles de SERVIR se elaboran con su presupuesto institucional, y la reserva cívica no es retribuida. Conforme al artículo 79 de la Constitución y a la STC 00018-2023-PI/TC, cualquier mejora remunerativa futura queda sujeta a las normas de compensación de la Ley 30057 y a las leyes anuales de presupuesto, a iniciativa del Poder Ejecutivo. El beneficio es ordenar perfiles y rutas de formación, dar independencia al oficial respecto del área de tecnologías de la información y ofrecer un modelo compartido viable para municipalidades pequeñas. La reserva cívica aporta capacidad de respuesta sin costo laboral, con controles de acceso. El inventario bienal permitirá medir brechas hoy desconocidas.

Normas que modifica

- Ley 30057, Ley del Servicio Civil, familia/subfamilia de puestos; compensación sin cambios — *complementa*
- Decreto Supremo 126-2025-PCM, arts. 11 y 15 (oficial de seguridad y confianza digital) — *eleva_rango*
- Decreto Supremo 029-2021-PCM, art. 111.3 — *eleva_rango*
- Ley 30096, Ley de Delitos Informáticos, art. 12, literal a) (reserva cívica) — *complementa*

Entidades implicadas (quién hace qué)

- **SERVIR** (rectora): Establece la subfamilia de puestos, aprueba y acredita el perfil del oficial y levanta el inventario (arts. 2, 3 y 7).
- **PCM-SGTD / CNSD** (consultiva): Propone el perfil del oficial, coordina la reserva cívica y la formación (arts. 3.1, 4 y 6).
- **ENAP** (ejecutora): Desarrolla programas de formación con su presupuesto (art. 4).
- **Entidades** (regulada): Designan al oficial con independencia, o lo comparten, en los plazos de la DCT Única (art. 3).
- **MEF** (financiadora): Mantiene la competencia sobre compensaciones conforme a la Ley 30057 y las leyes de presupuesto (art. 2.3).

Sujetos obligados: Todas las entidades de la administración pública de los tres niveles de gobierno; integrantes de la reserva cívica respecto de sus deberes de confidencialidad.

Beneficiarios: Entidades públicas y ciudadanos que dependen de sus servicios digitales; servidores que acceden a una ruta de formación. No cuantificable: no existe inventario oficial.

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

Tipo: neutro

Costo para el Estado: S/ 0 adicional (absorbido en presupuestos institucionales)

Horizonte: 2027-2031

Financiamiento: Presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público. Cualquier mejora remunerativa requiere iniciativa del Poder Ejecutivo conforme a la Ley 30057 y a las leyes anuales de presupuesto.

Supuestos: El oficial se designa entre el personal existente (art. 3.1); SERVIR y ENAP elaboran perfiles y formación con su presupuesto; la reserva cívica no es retribuida; no se aprueban escalas. El costo de oportunidad del tiempo del personal designado no se cuantifica.

Beneficio para el Estado: Menor improvisación en la gestión de incidentes, independencia del oficial y modelo compartido para municipalidades pequeñas. No cuantificable con información pública.

Beneficio para la sociedad: Mayor protección de los datos y servicios digitales públicos. No cuantificable con información pública.

Inversión privada: No aplica.

Costo para privados: No aplica, salvo el tiempo voluntario de los integrantes de la reserva cívica.

Riesgos: Sin mejora remunerativa, la rotación de especialistas hacia el sector privado puede persistir; sobrecarga del personal designado; dependencia de que exista la familia de talento digital (mitigado por la DCF Tercera).

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

- **Constitucional** — Observaciones graves: Profesionalizar la ciberseguridad en el Estado es legítimo y la designación del oficial puede imponerse por ley a todos los niveles de gobierno. Sin embargo, la escala remunerativa diferenciada, con financiamiento solo para 'el primer año', constituye iniciativa de gasto con impacto futuro, vedada a los congresistas según el art. 79 y la STC 00018-2023-PI/TC.
- **Técnica legislativa** — Observaciones graves: Profesionalizar la ciberseguridad en el Estado es pertinente, pero ordenar una escala remunerativa diferenciada y nuevos puestos genera gasto público que la propia propuesta reconoce («costo fiscal medio», «sin recursos adicionales en el primer año»), lo que choca con el art. 79 de la Constitución y con las reglas de las leyes anuales de presupuesto.
- **Concordancia normativa** — Con observaciones: El oficial de seguridad ya es un rol obligatorio en las entidades públicas: el D.S. 029-2021-PCM (arts. 96.2 lit. d y 111.3) y el D.S. 126-2025-PCM (art. 11) lo regulan; solo es facultativo en el sector privado (art. 15). La propuesta presenta como facultativo lo que ya es obligatorio en el sector público y omite que las escalas diferenciadas chocan con las prohibiciones de reajuste de las leyes anuales de presupuesto.
- **Seguridad** — Con observaciones: Atiende la brecha de talento, que es el principal cuello de botella de la ciberseguridad pública, con un diseño correcto (independencia del oficial respecto de TI, oficial compartido para municipios pequeños). La reserva cívica requiere un marco de autorización, verificación de antecedentes y gestión de conflictos de interés, y los puestos con accesos privilegiados necesitan controles de riesgo interno.
- **Derecho tecnológico** — Con observaciones: La familia de puestos basada en un marco de competencias (NICE de NIST) y el oficial compartido para municipalidades pequeñas son medidas realistas. El OSCD de entidades públicas ya está regulado por el art. 11 del DS 126-2025-PCM, de modo que la ley debe presentarse como elevación de rango y fijación de perfil e independencia. La escala diferenciada choca con las restricciones anuales de las leyes de presupuesto y con el art. 79; la reserva cívica requiere protección jurídica y controles de acceso.

IV. Efecto de la vigencia de la norma

Complementa la Ley 30057 y su reglamento general (D.S. 040-2014-PCM); eleva a rango de ley la obligación del art. 11 del D.S. 126-2025-PCM y del art. 111.3 del D.S. 029-2021-PCM, que se adecúan; complementa la Ley 30096 (art. 12, literal a), la Ley 29733 y la Ley 27815. Se articula como subfamilia dentro de la familia de puestos de talento digital del servicio civil. No exceptúa las prohibiciones de las leyes anuales de presupuesto. No requiere votación de ley orgánica.

V. Indicador de éxito al 2031

A 2031, 100 % de entidades del Poder Ejecutivo y gobiernos regionales con oficial de seguridad y confianza digital designado con las garantías del art. 3, subfamilia de puestos de ciberseguridad aprobada por SERVIR e inventario bienal publicado.

Normas relacionadas

- Ley 30057, Ley del Servicio Civil — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/30057.pdf>
- Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento — https://www3.congreso.gob.pe/Docs/comisiones2020/ConstitucionReglamento/files/du_interregno_2020/du-007-2020.pdf
- Decreto Supremo 126-2025-PCM, Reglamento del Decreto de Urgencia 007-2020 (Marco de Confianza Digital) — <https://busquedas.elperuano.pe/dispositivo/EX/2455024-1>

- Decreto Supremo 029-2021-PCM, Reglamento del Decreto Legislativo 1412 — <https://busquedas.elperuano.pe/dispositivo/NL/1929103-3>
- Decreto Supremo 085-2023-PCM, Política Nacional de Transformación Digital al 2030 — <https://busquedas.elperuano.pe/dispositivo/NL/2200457-5>

Antecedentes

Según verificación en SPLEY del revisor normativo, no se identificaron proyectos del periodo 2021-2026 sobre carrera de ciberseguridad en el servicio civil.

Referencias internacionales

- Estados Unidos: NIST NICE Framework (marco de competencias de la fuerza laboral en ciberseguridad) — <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center>
- Chile: Ley 21.663, Ley Marco de Ciberseguridad (crea la Agencia Nacional de Ciberseguridad y CSIRT) — <https://www.bcn.cl/leychile/navegar?idNorma=1202434>

Fuentes

- Apaxi (07-09-2026): Normas de ciberseguridad para empresas en el Perú — <https://apaxi.info/2026/09/07/normas-ciberseguridad-empresas-peru/>
- gob.pe: Autoridad Nacional del Servicio Civil — <https://www.gob.pe/servir>
- EY Perú: Reglamento del Marco de Confianza Digital (DS 126-2025-PCM) — https://www.ey.com/es_pe/technical/tax-alert/reglamento-ley-marco-confianza-digital-medidas-fortalecimiento

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/CIB-12.html>