El Peruano
Firmado por: Editora Peru
Fecha: 24/11/2026 00:48

CONVENIOS INTERNACIONALES

Acuerdo entre el Gobierno de la República Tunecina y el Gobierno de la República del Perú sobre Supresión de Visas para Titulares de Pasaportes Diplomáticos, Especiales o de Servicio **135**
Entrada en vigor del «Acuerdo entre el Gobierno de la República Tunecina y el Gobierno de la República del Perú sobre Supresión de Visas para Titulares de Pasaportes Diplomáticos, Especiales o de Servicio» **135**

SEPARATA ESPECIAL

SUPERINTENDENCIA DE BANCA, SEGUROS Y ADMINISTRADORAS PRIVADAS DE FONDOS DE PENSIONES

Res. SBS N° 02797-2026.- Aprueban los "Lineamientos sobre Buen Gobierno Corporativo para las Cajas Municipales de Ahorro y Crédito (CMAC)"

Diario Oficial El Peruano Electrónico (Ley N° 31649)

MUNICIPALIDAD DE ATE

Ordenanza N° 652-MDA.- Ordenanza que regula el proceso del Presupuesto Participativo Basado en Resultados en el distrito de Ate

MUNICIPALIDAD DE BREÑA

D.A. N° 011-026-MDB.- Prorrogan vigencia de beneficios tributarios establecidos en la Ordenanza N° 641-2026-MDB hasta el 30 de diciembre de 2026

MUNICIPALIDAD DE CHORRILLOS

Ordenanza N° 563-MDCH.- Ordenanza que regula la celebración de Matrimonio Civil Comunitario 2026

PODER EJECUTIVO

PRESIDENCIA DEL CONSEJO DE MINISTROS

Aprueban la Estrategia Nacional de Ciberseguridad 2026-2030

RESOLUCIÓN MINISTERIAL
N° 384-2026-PCM

Lima, 23 de noviembre de 2026

VISTOS: El Memorando N° D000828-2026-PCM-SGTD de la Secretaría de Gobierno y Transformación Digital; el Informe N° D000045-2026-PCM-SSTSD-ECV y el Informe N° D000018-2026-PCM-SSPRD-AZH, elaborados por la Subsecretaría de Tecnologías y Seguridad Digital y la Subsecretaría de Política y Regulación Digital, respectivamente; y,

CONSIDERANDO:

Que, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos; así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, en ese sentido, el artículo 8 del citado Decreto Legislativo establece que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), es el ente rector en materia de gobierno digital, la cual comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital, siendo responsable de dictar las normas, establecer los procedimientos en dicha materia, así como de garantizar su operación y correcto funcionamiento;

Que, el numeral 94.1 del artículo 94 del Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, aprobado mediante el Decreto Supremo N° 029-2021-PCM, dispone que el Marco de Seguridad Digital del Estado Peruano es dirigido, supervisado y evaluado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), en su calidad de ente rector de la seguridad digital, que emite lineamientos, especificaciones, guías, directivas, normas técnicas y estándares para su aplicación por parte de las entidades de la Administración Pública a fin de fortalecer la confianza de los ciudadanos, entidades públicas y personas en general en el entorno digital;

Que, por su parte, el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, tiene por objeto establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional;

Que, conforme al artículo 4 del citado Decreto de Urgencia N° 007-2020, el Marco de Confianza Digital se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, personas, empresas, entidades públicas, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital; y en concordancia con su artículo 5, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), es el ente rector en materia de Confianza Digital y el responsable de la articulación de cada uno de sus ámbitos: i) protección de datos personales y transparencia, ii) protección del consumidor y iii) seguridad digital;

Que, en esa misma línea, el literal h) del artículo 3 de la referida norma define a la ciberseguridad como la capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital; precisando expresamente que esta comprende la perspectiva técnica de la Seguridad Digital y constituye un ámbito del Marco de Seguridad Digital del país;

Que, el numeral 7.1 del artículo 7 del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, crea el Centro Nacional de Seguridad Digital (CNSD) como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

seguridad nacional, a fin de fortalecer la confianza digital; siendo responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos;

Que, en esa misma línea, el artículo 21 del Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, aprobado mediante el Decreto Supremo N° 157-2021-PCM, establece que las estrategias nacionales para la transformación digital son instrumentos activos, dinámicos y en constante actualización elaborados en el marco de la Política Nacional de Transformación Digital; las cuales comprenden, de manera no limitativa, a las estrategias nacionales sobre seguridad y confianza digital;

Que, la Política Nacional de Transformación Digital al 2030, aprobada mediante el Decreto Supremo N° 085-2023-PCM, establece como su Objetivo Prioritario 5 consolidar la seguridad y confianza digital en la sociedad. Para su efectivo cumplimiento, dispone la articulación de una estrategia nacional que provea la arquitectura y capacidades operativas necesarias para el monitoreo, identificación y respuesta ante incidentes de seguridad digital; garantice la protección y resiliencia de la infraestructura crítica; y fomente una cultura de ciberseguridad orientada a sensibilizar a la ciudadanía, fortaleciendo la confianza y asegurando el irrestricto respeto de los derechos humanos en el entorno digital;

Que, asimismo, en estricta concordancia con lo señalado, el Lineamiento 5.1 del Objetivo Prioritario 5 (OP5) de la citada Política Nacional de Transformación Digital exige asegurar el adecuado funcionamiento del Sistema Nacional de Transformación Digital mediante la elaboración y articulación de estrategias nacionales enfocadas en la seguridad y confianza digital, con el propósito ineludible de fortalecer las capacidades del país para mitigar riesgos cibernéticos y consolidar un entorno digital plenamente confiable para la sociedad;

Que, de conformidad con los artículos 82 y 83 del Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Resolución Ministerial N° 239-2026-PCM, la Secretaría de Gobierno y Transformación Digital (SGTD) es el órgano de línea con autoridad técnico-normativa a nivel nacional responsable de proponer, articular, implementar, supervisar y evaluar la Política Nacional de Transformación Digital y su estrategia, así como de formular y proponer estrategias y planes nacionales en las materias de su competencia; por lo que propone para su aprobación la Estrategia Nacional de Ciberseguridad 2026-2030 como instrumento orientador para la implementación de acciones en materia de ciberseguridad, en el marco de las competencias de la Presidencia del Consejo de Ministros;

Que, el Perú ha logrado avances significativos en la construcción de un sólido marco normativo e institucional en materia de ciberseguridad y confianza digital, impulsado por instrumentos como la Ley de Gobierno Digital y el Marco de Confianza Digital. Este ecosistema opera bajo la rectoría de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), y emplea al Centro Nacional de Seguridad Digital (CNSD) como la plataforma oficial encargada de gestionar, dirigir, articular y responder a los incidentes de seguridad digital a nivel nacional;

Que, no obstante, el principal desafío radica en una brecha estructural caracterizada por la insuficiente madurez técnico-operativa, tecnológica y de infraestructura del ecosistema nacional de ciberseguridad. Esta situación limita la implementación efectiva de los avances normativos alcanzados y compromete la capacidad del Estado para proteger los activos críticos nacionales, las actividades críticas y garantizar la continuidad de los servicios públicos esenciales frente a amenazas digitales;

Que, las buenas prácticas promovidas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Unión Internacional de Telecomunicaciones (UIT), la Organización de los Estados Americanos (OEA) y las Naciones Unidas recomiendan que los Estados cuenten con estrategias nacionales de ciberseguridad como instrumentos de política pública para fortalecer la gobernanza, desarrollar capacidades institucionales, gestionar los riesgos cibernéticos, promover la cooperación y mejorar la resiliencia frente a las amenazas en el entorno digital;

Que, la Estrategia Nacional de Ciberseguridad 2026-2030 constituye un instrumento de carácter estratégico que orienta y articula la actuación de las entidades competentes para el fortalecimiento de la ciberseguridad a nivel nacional, conforme al marco normativo vigente, sin alterar la distribución de competencias, funciones y responsabilidades establecidas en el ordenamiento jurídico ni crear obligaciones distintas de las previstas en la legislación aplicable;

Que, por su naturaleza técnica, dinámica y altamente especializada, la Estrategia Nacional de Ciberseguridad se configura como el instrumento estratégico orientado a desarrollar el componente de ciberseguridad dentro del Marco de Seguridad Digital del Estado y del Marco de Confianza Digital, mediante la definición de prioridades nacionales, estándares técnicos y mecanismos de coordinación para la protección de las redes, sistemas, activos e infraestructura tecnológica frente a riesgos y amenazas en el entorno digital;

Que, en atención al problema público previamente identificado, corresponde aprobar la Estrategia Nacional de Ciberseguridad 2026 - 2030 como un instrumento de política pública que permita ordenar, articular y orientar las medidas y acciones destinadas a fortalecer la seguridad digital, gestionar los riesgos en el entorno digital y proteger las redes, sistemas y activos digitales del país, en concordancia con las competencias institucionales y el marco normativo vigente; que tiene como objetivos estratégicos: fortalecer las capacidades nacionales de prevención, detección, respuesta y recuperación ante incidentes de seguridad digital en las entidades del ecosistema digital a nivel nacional; fortalecer la ciberseguridad de los activos críticos nacionales, las actividades críticas y los servicios públicos esenciales frente a amenazas de seguridad digital; desarrollar una cultura nacional de ciberseguridad y sólidas capacidades operativas en el talento humano del sector público y la ciudadanía; consolidar la cooperación internacional y el intercambio de información sobre amenazas de seguridad digital; fortalecer la gobernanza y el marco normativo en ciberseguridad en las entidades de la administración pública; y desarrollar capacidades nacionales de gestión de riesgos digitales e inteligencia en ciberseguridad en las entidades del Estado y sectores estratégicos;

Con el visado de la Secretaría de Gobierno y Transformación Digital, de la Oficina General de Planeamiento y Presupuesto y de la Oficina General de Asesoría Jurídica;

De conformidad con lo dispuesto en el numeral 8 del artículo 118 de la Constitución Política del Perú; la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; la Ley N° 30096, Ley de Delitos Informáticos; la Ley N° 29733, Ley de Protección de Datos Personales; el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; el Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital; el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento; y el Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por la Resolución Ministerial N° 239-2026-PCM;

SE RESUELVE:

Artículo 1.- Aprobación de la Estrategia Nacional de Ciberseguridad 2026-2030

1.1. Aprobar la Estrategia Nacional de Ciberseguridad 2026-2030, la misma que forma parte integrante de la presente Resolución Ministerial.

1.2. La Estrategia Nacional de Ciberseguridad 2026-2030 constituye un instrumento de carácter estratégico, orientador y articulador de las acciones en materia de

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

ciberseguridad, cuya implementación se desarrolla conforme a las competencias de cada entidad y al marco normativo vigente.

Artículo 2.- Ámbito de aplicación

2.1 La presente Resolución Ministerial y la Estrategia Nacional de Ciberseguridad 2026-2030 se aplican a:

a) Las entidades de la Administración Pública establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 006-2026-JUS, con excepción de las personas jurídicas señaladas en el numeral 8 del citado artículo.
b) Las empresas públicas de los gobiernos regionales y locales, y aquellas que se encuentran en el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE).
c) Aquellos que se encuentren obligados al cumplimiento de obligaciones de acuerdo a la normativa vigente del marco de confianza digital y de activos críticos nacionales.

2.2 Las organizaciones del sector privado pueden tomar como referencia lo establecido en la presente Resolución Ministerial y en la Estrategia Nacional de Ciberseguridad 2026-2030 en cuanto les genere valor.

Artículo 3.- Conducción, articulación, supervisión y evaluación de la Estrategia Nacional de Ciberseguridad 2026-2030

3.1. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), en ejercicio de la rectoría nacional en materia de gobierno digital, seguridad digital y confianza digital, conduce, articula, supervisa y evalúa la implementación de la Estrategia Nacional de Ciberseguridad 2026-2030.
3.2. Para el desarrollo de las acciones operativas vinculadas a la Estrategia Nacional de Ciberseguridad 2026-2030, la Secretaría de Gobierno y Transformación Digital (SGTD) actúa a través del Centro Nacional de Seguridad Digital (CNSD), el cual, de conformidad con el marco normativo vigente, gestiona, dirige, coordina y articula las acciones de prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital.

Artículo 4.- Responsabilidades institucionales del Sector Público

4.1. Para la implementación de la Estrategia Nacional de Ciberseguridad 2026-2030 las entidades públicas articulan sus objetivos, acciones e iniciativas institucionales con los objetivos de la referida Estrategia, en el marco de sus funciones, competencias, capacidades institucionales y disponibilidad presupuestal, considerando los instrumentos del Sistema Nacional de Planeamiento Estratégico, según corresponda.
4.2. Los Comités de Gobierno y Transformación Digital promueven el seguimiento de la implementación de la Estrategia Nacional de Ciberseguridad 2026-2030 en sus respectivas entidades. Para dicho efecto, las entidades adoptan las medidas necesarias, de acuerdo con sus competencias, capacidades institucionales y disponibilidad presupuestal, a fin de:

a) Incorporar objetivos, indicadores y metas vinculados a la ciberseguridad en sus instrumentos de planeamiento institucional, cuando corresponda.
b) Incorporar iniciativas orientadas a la gestión de riesgos, mitigación de vulnerabilidades y fortalecimiento de los controles de ciberseguridad en sus instrumentos de gestión de gobierno digital.
c) Fortalecer las capacidades institucionales para la gestión de la seguridad digital y promover el adecuado ejercicio de las funciones del Oficial de Seguridad y Confianza Digital (OSCD) y la consolidación de los Equipos de Respuesta ante Incidentes de Seguridad Digital (CSIRT), conforme al marco normativo vigente.

Artículo 5.- Oficial de Seguridad y Confianza Digital

5.1. El Oficial de Seguridad y Confianza Digital (OSCD) desempeña un rol estratégico en la gestión de la seguridad digital de la entidad pública. En el marco de sus funciones, coordina, promueve y articula las acciones necesarias para fortalecer la gestión de la seguridad digital, incluyendo la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), sin perjuicio de las competencias que correspondan a las unidades orgánicas responsables de las tecnologías de la información y demás órganos involucrados, conforme a la estructura orgánica y al marco normativo vigente.
5.2. Para garantizar su independencia funcional respecto de las áreas de tecnologías de la información, el Oficial de Seguridad y Confianza Digital (OSCD) ejerce sus funciones con autonomía técnica y reporta a la máxima autoridad administrativa de la entidad y al Comité de Gobierno y Transformación Digital, del cual forma parte, conforme a la normativa vigente.

Artículo 6.- Responsabilidad por incumplimiento de entidades públicas

El incumplimiento de las obligaciones previstas en la normativa vigente relacionadas con la implementación de la Estrategia Nacional de Ciberseguridad 2026-2030 genera las responsabilidades administrativas, civiles y penales que correspondan, de conformidad con el ordenamiento jurídico aplicable.

Artículo 7.- Seguimiento, Monitoreo y Evaluación

7.1. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), es la encargada de realizar el seguimiento, monitoreo y evaluación de la Estrategia Nacional de Ciberseguridad 2026-2030, en coordinación con el Centro Nacional de Seguridad Digital (CNSD) y las entidades responsables. Este proceso se ejecutará mediante:

a) Monitoreo semestral para verificar el avance de las acciones estratégicas.
b) Evaluación anual para determinar el cumplimiento de indicadores y metas.

7.2. Los resultados del seguimiento, monitoreo y evaluación constituyen insumos para la mejora continua de la Estrategia Nacional de Ciberseguridad 2026-2030 y sirven de base para la actualización de sus acciones, indicadores y metas, cuando corresponda, conforme a las competencias de la Secretaría de Gobierno y Transformación Digital (SGTD) y al marco normativo vigente.

Artículo 8.- Espacios de diálogo, articulación y participación

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), promueve mecanismos de diálogo, articulación y participación multisectorial para fortalecer la implementación, seguimiento, evaluación y mejora continua de la Estrategia Nacional de Ciberseguridad 2026-2030. Para tal efecto, puede convocar a las entidades públicas competentes, así como a representantes de la academia, el sector privado, la sociedad civil y organismos internacionales, conforme a sus competencias y al marco normativo vigente.

Artículo 9.- Financiamiento

9.1. La implementación de la Estrategia Nacional de Ciberseguridad 2026-2030 se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público y con cargo a los presupuestos institucionales autorizados.
9.2. Sin perjuicio de lo anterior, las entidades pueden gestionar recursos provenientes de la cooperación internacional no reembolsable y formular proyectos de inversión en el marco del Sistema Nacional de Programación Multianual y Gestión de Inversiones

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

(INVIERTE.PE) para el cierre de brechas en infraestructura de ciberseguridad.

Artículo 10.- Publicación
Disponer la publicación de la presente Resolución Ministerial y la Estrategia Nacional de Ciberseguridad 2026-2030, aprobada en el artículo 1, en la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano (www.gob.pe), así como en la sede digital de la Presidencia del Consejo de Ministros (www.gob.pe/pcm), el mismo día de la publicación de la presente Resolución Ministerial en el Diario Oficial "El Peruano".

Artículo 11.- Vigencia
La presente Resolución entra en vigencia al día siguiente de su publicación en el Diario Oficial El Peruano.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- Articulación interinstitucional en materia de seguridad digital
La Secretaría de Gobierno y Transformación Digital (SGTD) de la Presidencia del Consejo de Ministros, a través del Centro Nacional de Seguridad Digital (CNSD), articula acciones con la Dirección Nacional de Inteligencia (DINI), el Comando Conjunto de las Fuerzas Armadas (CCFFAA), la Policía Nacional del Perú (PNP), la Autoridad Nacional de Protección de Datos Personales (ANPD), el Ministerio Público (MP), a través de sus órganos, y las demás entidades públicas competentes, con la finalidad de fortalecer las capacidades nacionales en materia de seguridad digital.
La articulación comprende el intercambio seguro de información, la cooperación técnica, el fortalecimiento de capacidades, la gestión de riesgos de seguridad digital, la adopción de medidas preventivas y de mitigación, la coordinación para la atención de incidentes de seguridad digital, la investigación y la persecución de delitos informáticos cuando corresponda, así como la promoción de buenas prácticas, conforme al marco normativo vigente en materia de gobierno digital, seguridad digital, confianza digital, protección de datos personales, delitos informáticos, defensa nacional e inteligencia.
La cooperación se desarrolla mediante mecanismos, protocolos y canales seguros de comunicación, en atención a la naturaleza y la clasificación de la información, así como a las obligaciones de confidencialidad, custodia y protección aplicables, con el fin de promover la complementariedad institucional y evitar la duplicidad de esfuerzos frente a riesgos, incidentes, delitos o amenazas que puedan comprometer la seguridad digital del Estado.

Segunda.- Adopción de estándares internacionales para la gestión de riesgos de seguridad digital en entornos industriales
Las entidades de la Administración Pública que administren, operen o sean responsables de gestionar sistemas de automatización y control industrial, y tecnología operativa (OT), adoptan e implementan normas técnicas y mejores prácticas globales en la gestión de riesgos en entornos industriales.
Para orientar y promover la seguridad de sistemas de automatización y control industrial, y tecnología operativa (OT) se puede considerar los siguientes estándares ISA/IEC 62443 (Seguridad de la información para sistemas de automatización y control industrial y la tecnología operativa), NIST SP 800-82 (Guía para la Seguridad de Tecnología Operativa), la norma ISO 22301 (Gestión de la continuidad del negocio), y otras de valor para el sector, industria o modelo de negocio. Estos estándares se implementan de manera complementaria a la normativa nacional vigente.

Regístrese, comuníquese y publíquese.

LUIS FERNANDO GALARRETA VELARDE
Presidente del Consejo de Ministros

2577750-1

COMERCIO EXTERIOR Y TURISMO

Designan miembro del Consejo Directivo de la Superintendencia Nacional de Migraciones - MIGRACIONES en representación del Sector Comercio Exterior y Turismo

RESOLUCIÓN SUPREMA
N° 008-2026-MINCETUR

Lima, 22 de noviembre de 2026

CONSIDERANDO:

Que, mediante el artículo 1 del Decreto Legislativo Nº 1130 se crea la Superintendencia Nacional de Migraciones - MIGRACIONES, como un Organismo Técnico Especializado adscrito al Ministerio del Interior, con personería jurídica de derecho público interno, con autonomía administrativa, funcional y económica en el ejercicio de sus atribuciones;
Que, el artículo 8 del citado Decreto Legislativo establece que el Consejo Directivo es el órgano máximo de MIGRACIONES, responsable de establecer las políticas institucionales y la dirección de MIGRACIONES y se encuentra integrado por cuatro (4) miembros designados por Resolución Suprema. El Sector Interior propondrá dos (2) miembros, uno de los cuales será el Superintendente Nacional. Los Sectores Comercio Exterior y Turismo, y Relaciones Exteriores propondrán un (01) miembro cada uno, que los representarán en el Consejo Directivo;
Que, mediante Resolución Suprema N° 002-2026-MINCETUR se designa a la señora Ysabel Angeles Ramos Yañez, como miembro del Consejo Directivo de MIGRACIONES en representación del Sector Comercio Exterior y Turismo;
Que, la señora Ysabel Angeles Ramos Yañez ha formulado su renuncia como miembro del Consejo Directivo de MIGRACIONES en representación del Sector Comercio Exterior y Turismo;
Que, estando a lo propuesto por el Ministerio de Comercio Exterior y Turismo, se ha visto por conveniente aceptar la renuncia formulada y designar al nuevo miembro del Consejo Directivo de MIGRACIONES en representación del Sector Comercio Exterior y Turismo;
De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; la Ley N° 31419, Ley que establece disposiciones para garantizar la idoneidad en el acceso y ejercicio de la función pública de funcionarios y directivos de libre designación y remoción; el Decreto Legislativo N° 1130, Decreto Legislativo que crea la Superintendencia Nacional de Migraciones - MIGRACIONES; la Ley N° 27790, Ley de Organización y Funciones del Ministerio de Comercio Exterior y Turismo; y, la Resolución Ministerial N° 216-2025-MINCETUR, que aprueba el Texto Integrado del Reglamento de Organización y Funciones del Ministerio de Comercio Exterior y Turismo;

SE RESUELVE:

Artículo 1.- Aceptar la renuncia formulada por la señora Ysabel Angeles Ramos Yañez, como miembro del Consejo Directivo de la Superintendencia Nacional de Migraciones – MIGRACIONES en representación del Sector Comercio Exterior y Turismo, dándosele las gracias por los servicios prestados.
Artículo 2.- Designar a la señora Carmen Rocío Arévalo Martos, como miembro del Consejo Directivo de la Superintendencia Nacional de Migraciones – MIGRACIONES en representación del Sector Comercio Exterior y Turismo.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2026-2030









SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONTROL DE VISADO Y FIRMADO

VISADO POR:	Subsecretaría de Política y Regulación Digital	
VISADO POR:	Subsecretaría de Tecnologías y Seguridad Digital	
VISADO POR:	Subsecretaría de Servicios e Innovación Digital	
FIRMADO POR:	Secretaría de Gobierno y Transformación Digital	

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

CONTENIDO

ÍNDICE DE FIGURAS 3
ÍNDICE DE TABLAS 4
ACRÓNIMOS 5
DEFINICIONES 6
RESUMEN EJECUTIVO 9
I. PANORAMA DE LA CIBERSEGURIDAD 10
1.1. Nuevas amenazas en el entorno digital 11
1.2. Contexto Nacional 13
1.3. Contexto institucional 20
II. ALINEACIÓN CON INSTRUMENTOS NACIONALES E INTERNACIONALES 24
2.1. Marco normativo en materia de ciberseguridad en el Perú 24
2.2. Alineación con instrumentos estratégicos nacionales 26
2.3 Alineación con instrumentos internacionales 31
III. GOBERNANZA Y COORDINACIÓN NACIONAL DE LA CIBERSEGURIDAD 34
3.1. ¿Por qué una Estrategia Nacional de Ciberseguridad? 34
3.2. Gobernanza institucional en el sector público 37
3.3 Corresponsabilidad del sector privado y proveedores de actividades críticas 38
IV. NECESIDAD ESTRATÉGICA Y PROYECCIÓN HACIA OBJETIVOS 39
4.1. Situación futura deseada 40
4.2. Alcance 40
4.3 Principios orientadores 40
V. DIAGNÓSTICO Y MARCO ESTRATÉGICO 42
5.1 Problema público 42
5.2 Objetivos y acciones estratégicas 45
VI. SEGUIMIENTO, MONITOREO Y EVALUACIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 82
ANEXOS 84
I. Matriz de alineación entre los Objetivos Prioritarios y Lineamientos de la PNTD con los Objetivos y Acciones Estratégicas de la ENC. 84
II. Matriz de Objetivos Estratégicos, Acciones Estratégica e Indicadores de la ENC 87

PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Gobierno y Transformación Digital
PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Tecnologías y Seguridad Digital
PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Servicios e Innovación Digital
PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Política y Regulación Digital

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

ÍNDICE DE FIGURAS

Figura 1 . Desempeño de Perú en el Índice Global de Ciberseguridad 2024, según los cinco pilares de evaluación 14
Figura 2. Evolución de Perú en el Índice Global de Ciberseguridad 2024 15
Figura 3. Evaluación de la madurez de la ciberseguridad de Perú por dimensiones, 2025 16
Figura 4. Dimensiones para la evaluación de la madurez de la ciberseguridad 18
Figura 5. Etapas de madurez del Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM) 19
Figura 6. Resultados consolidados por tipo de actividad del Centro Nacional de Seguridad Digital, 2024 – enero de 2026 20
Figura 7. Resultados 2024 (enero a diciembre) 21
Figura 8. Resultados 2025 (enero a diciembre) 22
Figura 9. Resultados 2026 (enero) 23
Figura 10. Coherencia y complementariedad estratégica entre la ENC y la PNTD 28
Figura 11. Principios de la Recomendación del Consejo sobre Gestión de Riesgos de Seguridad Digital (OECD/LEGAL/0479) 32
Figura 12. Actores de la Estrategia Nacional de Ciberseguridad 39

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

ÍNDICE DE TABLAS

Tabla 1. Alineación de las Políticas de Estado del Acuerdo Nacional con los Objetivos de la ENC ...28
Tabla 2. Alineación del PEDN al 2050 con los Objetivos de la ENC.....30
Tabla 3. Principales hallazgos sobre ciberseguridad en el Perú.....42

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

ACRÓNIMOS

- **ACN** - Activos Críticos Nacionales
- **CEPLAN** - Centro Nacional de Planeamiento Estratégico
- **CDEP** - Comité de Política de Economía Digital (OCDE)
- **CICTE** - Comité Interamericano contra el Terrorismo (OEA)
- **COSEDENA** - Consejo de Seguridad y Defensa Nacional
- **CNSD** - Centro Nacional de Seguridad Digital
- **CONCYTEC** - Consejo Nacional de Ciencia, Tecnología e Innovación
- **CSIRT:** Equipo de Respuesta ante Incidentes de Seguridad Digital
- **CVD** - Coordinated Vulnerability Disclosure
- **DINI** - Dirección Nacional de Inteligencia
- **ENC** - Estrategia Nacional de Ciberseguridad
- **GORE** - Gobierno Regional
- **IA** - Inteligencia Artificial
- **INACAL** – Instituto Nacional de Calidad
- **INDECOPI** – Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual
- **INEI** - Instituto Nacional de Estadística e Informática
- **ISO/IEC** - International Organization for Standardization / International Electrotechnical Commission
- **IoT** - Internet of Things (Internet de las Cosas)
- **MINDEF** – Ministerio de Defensa
- **MINEDU** - Ministerio de Educación
- **MINJUSDH** - Ministerio de Justicia y Derechos Humanos
- **OCDE** - Organización para la Cooperación y el Desarrollo Económicos
- **OEA** - Organización de los Estados Americanos
- **ONU** - Organización de las Naciones Unidas
- **OSCD** - Oficial de Seguridad y Confianza Digital
- **OT/IT** - Operational Technology / Information Technology
- **PCM** - Presidencia del Consejo de Ministros
- **PEI** - Plan Estratégico Institucional
- **POI** - Plan Operativo Institucional
- **PNTD** - Política Nacional de Transformación Digital
- **SERVIR** - Autoridad Nacional del Servicio Civil
- **SINA** - Sistema de Inteligencia Nacional
- **SGSI** - Sistema de Gestión de Seguridad de la Información
- **SGTD** - Secretaría de Gobierno y Transformación Digital
- **SOC** - Security Operations Center (Centro de Operaciones de Seguridad)
- **SOAR** - Security Orchestration, Automation and Response
- **SNTD** - Sistema Nacional de Transformación Digital
- **TIC** - Tecnologías de la Información y la Comunicación
- **UIT** - Unión Internacional de Telecomunicaciones

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

DEFINICIONES

1. **Ciberseguridad**: De acuerdo con el literal h) del artículo 3 del Decreto de Urgencia N.º 007-2020 que aprueba el Marco de Confianza Digital, la ciberseguridad se define como la capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos, y protegerlos ante amenazas y vulnerabilidades en el entorno digital.

2. **Activos Críticos Nacionales (ACN)**: Según lo dispuesto en el numeral 3.4 del artículo 3 del Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los ACN, aprobado por Decreto Supremo N.º 106-2017-PCM, son aquellos recursos, infraestructuras y sistemas que resultan esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales, o que están destinados a cumplir dicho fin. La afectación, perturbación o destrucción de dichos activos no permite soluciones alternativas inmediatas, generando grave perjuicio a la Nación.

3. **Actividades críticas**: El literal d) del artículo 3 del Decreto de Urgencia N.º 007-2020 que aprueba el Marco de Confianza Digital, las define como toda actividad económica y/o social cuya interrupción tiene graves consecuencias en la salud y seguridad de los ciudadanos, o en el funcionamiento efectivo de los servicios esenciales que mantienen la economía, sociedad y el gobierno, o afectan la prosperidad económica y social en general.

4. **CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Digital)**: Según lo tipificado en el artículo 104 del Reglamento de la Ley de Gobierno Digital, aprobado por Decreto Supremo N.º 029-2021-PCM, un CSIRT es el equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza.

5. **Oficial de Seguridad y Confianza Digital (OSCD)**: Conforme al artículo 11 del Reglamento de Confianza Digital, aprobado por Decreto Supremo N.º 126-2025-PCM, el OSCD es el rol estratégico responsable de coordinar la implementación y mantenimiento de acciones estratégicas y técnicas en materia de seguridad digital, así como los procesos del Sistema de Gestión de Seguridad de la Información (SGSI).

   Asimismo, es responsable de coordinar con el CSIRT institucional el registro y notificación obligatoria al CNSD de cualquier incidente de seguridad digital, e intercambio de información en materia de seguridad digital. Para el cumplimiento de sus responsabilidades, coordina con el Oficial de Datos Personales en las cuestiones relativas al diseño e implementación de controles para la protección de los datos personales a efectos de fortalecer la confianza en el entorno digital.

6. **Sistema de Gestión de Seguridad de la Información (SGSI)**: Conforme al artículo 109 del Reglamento de la Ley de Gobierno Digital (Decreto Supremo N.º 029-2021-PCM), el SGSI comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas que gestiona una entidad con el propósito de proteger sus activos de información, independientemente del soporte en que se encuentren.

   Para materializar esta obligación, la Resolución de Secretaría de Gobierno y Transformación Digital N.º 003-2023-PCM/SGTD impone que las entidades públicas deben usar obligatoriamente la Norma Técnica Peruana NTP ISO/IEC 27001 vigente para el análisis, diseño, implementación y mejora continua de este sistema, estableciendo como alcance mínimo e innegociable la protección de sus procesos misionales y servicios esenciales.

Amenaza de seguridad digital: El literal c) del artículo IV del Reglamento de la Ley de Ciberdefensa lo define como todo acto fuente, circunstancia o evento de origen externo o interno con la capacidad potencial de generar, a través del uso de sistemas o herramientas

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

cibernéticas, efectos adversos, daños o perjuicios a la seguridad nacional, soberanía, los intereses nacionales y los Activos Críticos Nacionales.

8. **Servicios digitales**: Conforme al numeral 3 del artículo 3 de la Ley de Gobierno Digital, Decreto Legislativo N.º 1412, son aquellos servicios provistos de forma total o parcial a través de Internet u otras redes equivalentes que se caracterizan por ser automáticos, no presenciales y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas.

9. **Transformación digital**: El artículo 3 del Decreto de Urgencia N.º 006-2020 que crea el Sistema Nacional de Transformación Digital la define como el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intensivo de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.

10. **Confianza digital**: De acuerdo con el literal a) del artículo 3 del Decreto de Urgencia N.º 007-2020, es el estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital.

11. **Recuperación y resiliencia digital:** El literal e) del numeral 5.1 del artículo V del Título Preliminar del Reglamento del Marco de Confianza Digital, aprobado por Decreto Supremo N.º 126-2025-PCM, la define como la capacidad por la cual se adoptan medidas a fin de anticipar, responder, recuperarse y aprender ante incidentes de seguridad digital.

12. **Entorno digital**: Conforme al numeral 2 del artículo 3 de la Ley de Gobierno Digital, Decreto Legislativo N.º 1412, y el literal c) del artículo 3 del Decreto de Urgencia N.º 007-2020, es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas.

Riesgo de seguridad digital: El literal g) del artículo 3 del Decreto de Urgencia N.º 007-2020 que aprueba el Marco de Confianza Digital, lo define como el efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad; y, resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan.

Incidente de seguridad digital: El literal e) del artículo 3 del Decreto de Urgencia N.º 007-2020 que aprueba el Marco de Confianza Digital lo define como aquel evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.

Ecosistema digital: El literal b) del artículo 3 del Reglamento de la Ley del Sistema Nacional de Transformación Digital, aprobado por Decreto Supremo N.º 157-2021-PCM, lo define como el sistema caracterizado por el despliegue y adopción masiva de las tecnologías digitales que conllevan a una transformación en la producción de bienes y servicios digitales de valor para las personas y el mercado. Se compone de la infraestructura de redes de banda ancha, dispositivos y plataformas digitales, personas, empresas, servicios y contenidos digitales,

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

capacidad de innovación y marco regulatorio, interrelacionados entre sí para promover la transformación digital de los procesos productivos y las actividades económicas y sociales para el desarrollo sostenible del país.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

RESUMEN EJECUTIVO

El Perú transita hoy por un proceso acelerado de transformación digital que ha reconfigurado la manera en que el Estado, el sector privado, la academia, sociedad civil y la ciudadanía interactúan, producen valor y ejercen derechos. El entorno digital ha dejado de ser un espacio accesorio para convertirse en una dimensión relevante y transversal, sobre la cual descansan servicios esenciales, flujos económicos y la propia gobernabilidad del país.

Este nuevo entorno digital, caracterizado por su interconexión, dinamismo y alcance global, ofrece oportunidades sin precedentes para el desarrollo económico, la inclusión social y la transformación digital del Estado. Sin embargo, esta misma expansión ha traído consigo una creciente exposición a riesgos complejos, persistentes y cada vez más sofisticados, que desafían las capacidades tradicionales de gestión pública y exigen respuestas integrales, coordinadas y sostenibles.

En este contexto, la ciberseguridad deja de ser un asunto meramente técnico para posicionarse como un componente estratégico para la continuidad de los servicios públicos esenciales, servicios digitales, la protección de los derechos de las personas en el entorno digital y la confianza en el entorno digital. Las amenazas de seguridad digital actuales no solo comprometen sistemas informáticos, sino que pueden afectar directamente la estabilidad institucional, la economía y los derechos fundamentales de las personas.

El país ha avanzado significativamente en la construcción de un marco normativo e institucional sólido en materia de gobierno digital, confianza digital y protección de datos personales. No obstante, estos avances conviven con brechas relevantes en la implementación técnica, la madurez operativa y el desarrollo de capacidades especializadas, las cuales se manifiestan de manera diferenciada a nivel territorial, particularmente en los gobiernos regionales y locales, evidenciando una tensión estructural entre el desarrollo normativo y su aplicación efectiva.

En ese escenario, la presente Estrategia Nacional de Ciberseguridad se configura como un instrumento que busca precisamente combatir esa brecha. No se trata únicamente de fortalecer normas o la gobernanza institucional, sino de consolidar capacidades reales, medibles y sostenibles que permitan al país gestionar los riesgos del entorno digital de manera efectiva.

La Estrategia Nacional de Ciberseguridad propone una transición clara: de un enfoque centrado predominantemente en la generación de marcos normativos hacia un modelo de madurez operativa, donde la ciberseguridad se materialice en capacidades concretas de prevención, detección, respuesta y recuperación, articuladas bajo una gobernanza nacional coherente y con liderazgo.

Ello implica avanzar hacia una arquitectura nacional integrada, fortalecer el rol del Centro Nacional de Seguridad Digital como núcleo operativo, desarrollar capacidades descentralizadas en las entidades públicas, proteger las infraestructuras críticas y promover una cultura de ciberseguridad que involucre a todos los actores del Sistema Nacional de Transformación Digital. Asimismo, la Estrategia incorpora un enfoque territorial, orientado a adaptar las acciones y prioridades a las particularidades y niveles de madurez de los gobiernos regionales y locales, promoviendo el cierre progresivo de brechas y el desarrollo de capacidades en todo el territorio nacional.

En definitiva, la Estrategia Nacional de Ciberseguridad no solo responde a la necesidad de proteger sistemas y datos, sino a un objetivo mayor: garantizar que la consolidación de la transformación digital del país se desarrolle sobre bases seguras, confiables y resilientes, asegurando así la continuidad de los servicios públicos esenciales, la protección de los derechos fundamentales y el fortalecimiento de la confianza pública en el entorno digital.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

I. PANORAMA DE LA CIBERSEGURIDAD

El entorno digital se ha consolidado como un espacio común global, dinámico y de creciente relevancia estratégica para el Perú. Su carácter abierto, interconectado y transfronterizo ha transformado profundamente la forma en que los ciudadanos se comunican, las empresas desarrollan sus actividades y el Estado ejerce sus funciones y presta servicios.

Este entorno genera oportunidades significativas para el desarrollo económico y social, al ampliar la conectividad, facilitar el acceso a la información y mejorar la eficiencia de los servicios públicos y privados.

La adopción acelerada de tecnologías como la inteligencia artificial, el Internet de las Cosas (IoT) y la computación en la nube y la masificación de los *smartphones* (presentes en el 94,8% de hogares peruanos en 2024)[1] están redefiniendo los modelos productivos del país.

La consolidación de la transformación digital genera oportunidades significativas para el desarrollo económico y social. Conforme señala el Observatorio Nacional de Prospectiva, la transformación digital ha experimentado una aceleración sin precedentes: el acceso a internet alcanzó al 79,4 % de hogares en Lima Metropolitana en el 2024[2], el comercio electrónico generó US$ 13 000 millones en el 2023[3], y el uso de pagos digitales se disparó exponencialmente, pasando de 29 pagos digitales anuales per cápita en 2015 a 442 en 2024[4].

No obstante, esta creciente dependencia del entorno digital también introduce riesgos sustantivos para la seguridad, la economía y los derechos de las personas. El entorno digital se ha convertido en un complejo escenario donde la información estratégica, los datos personales y las infraestructuras digitales críticas constituyen activos de alto valor que se encuentran expuestos a amenazas cada vez más sofisticadas y persistentes.

La interconexión de sistemas, la expansión de servicios digitales y la proliferación de dispositivos conectados incrementan significativamente la superficie de ataque, lo que exige capacidades avanzadas de prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital.

De manera crítica, de la proporción de usuarios de Kaspersky, el Perú encabezó el ranking mundial de países con mayor proporción de usuarios afectados por phishing (19,06 % de los usuarios de Kaspersky en el país)[5]. A esto se suma que redes del crimen organizado

---

1 Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL. Encuesta Residencial de Servicios de Telecomunicaciones – ERESTEL 2024. https://sociedadtelecom.pe/wp-content/uploads/2025/09/ERESTEL-2024.pdf (p.7)

2 Instituto Nacional de Estadística e Informática (INEI), Informe Técnico N.° 1 – Marzo 2025. Trimestre: Octubre - Noviembre – Diciembre 2024. Disponible en: https://www.inei.gob.pe/media/MenuRecursivo/boletines/informe-tecnico_tics_oct-nov-dic24.pdf

3 Cámara Peruana de Comercio Electrónico – CAPECE, Reporte Oficial de la Industria Ecommerce en el Perú. Disponible en: https://biblioteca.bcrp.gob.pe/discovery/delivery/51BCDRDP_INST:51BCDRDP2/1225259470009006 (p. 61)

4 Banco Central de Reserva del Perú. Reporte del Sistema Nacional de Pagos y del Sector Fintech en Perú. Marzo 2025. https://www.bcrp.gob.pe/docs/Publicaciones/reporte-del-sistema-nacional-de-pagos/2025/marzo/rspf-marzo-2025.pdf (p. 7).

5 Observatorio CEPLAN, Incremento del ciberdelito, https://observatorio.ceplan.gob.pe/ficha/t85. Tomado originalmente de Kaspersky daily, EL spam y el phishing en 2024, 19 febrero 2025. https://securelist.lat/spam-and-phishing-report-2024/99599/

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

transnacional han adoptado la tecnología digital para blanquear capitales y cometer fraudes o extorsiones a nivel nacional[6].

En este contexto, el entorno digital se configura como un ámbito de operación relevante tanto para actores legítimos como para actores maliciosos, incluidos grupos criminales, organizaciones transnacionales y otros agentes que pueden afectar la estabilidad institucional, el desarrollo económico y la confianza pública. Las amenazas de seguridad digital actuales tienen el potencial de impactar de manera directa la continuidad de los servicios públicos esenciales, la protección de los datos personales, la integridad de la información y, en suma, en la seguridad digital del país.

1.1. Nuevas amenazas en el entorno digital

En el marco del proceso de transformación digital que atraviesa el país, el entorno global de amenazas de seguridad digital ha experimentado una evolución significativa, caracterizada por un aumento en la sofisticación, frecuencia y alcance de los ataques. Esta dinámica responde tanto al avance tecnológico como a la creciente profesionalización de los actores maliciosos, quienes emplean herramientas cada vez más complejas para explotar vulnerabilidades en sistemas, infraestructuras y usuarios.

En este contexto, la ampliación de la superficie de ataque (derivada de la masificación de servicios digitales, la adopción de tecnologías emergentes y la interconexión de dispositivos) incrementa la exposición a riesgos que pueden comprometer la continuidad de servicios públicos esenciales, la integridad, confidencialidad y disponibilidad de la información y la confianza en el ecosistema digital.

De acuerdo con el Observatorio Nacional de Prospectiva de CEPLAN[7], se estima que para el 2030 más de 7500 millones de personas usarán Internet a nivel mundial, ampliando masivamente esta "superficie de ataque".

Como consecuencia de ello, entre las principales tendencias que configuran el panorama actual de riesgos, destacan las siguientes:

- **Uso malicioso de la inteligencia artificial generativa**

  La incorporación de herramientas basadas en inteligencia artificial por parte de actores maliciosos ha transformado las modalidades de ataque, permitiendo ejecutar operaciones con mayor nivel de automatización, precisión y escalabilidad.

  La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) advierte que las redes del crimen organizado transnacional han convertido a la IA en una plataforma fundamental para cometer fraudes masivos y blanquear capitales[8]. Los ataques

---

6 United Nations Office on Drugs and crime - UNODC. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. October 2024. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

7 Observatorio CEPLAN. Incremento del ciberdelito. https://observatorio.ceplan.gob.pe/ficha/t85 Tomado originalmente de A. Vennela, R. B. Akarapu, B. L. Rakshith, L. G. Asirvatham y G. & Sunil, «Intelligent cybersecurity systems for phishing attack detection-An overview», publicado en la revista científica *Computers and Electrical Engineering*, vol. 130, en el año 2026.

Observatorio CEPLAN. Incremento del ciberdelito. https://observatorio.ceplan.gob.pe/ficha/t85 Tomado originalmente de UNODC, *"Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud,*

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

deterioran la reputación y la confianza de un país, además de afectar su competitividad y provocar inseguridad en el entorno digital[9].

- **Ataques de ransomware y persistencia de denegación de servicio distribuido**

El Observatorio Nacional de Prospectiva de CEPLAN evidencia que los ataques de *ransomware* (incidente que amenaza con bloquear el acceso a un sistema a datos informáticos) que tienen una dimensión política se han multiplicado por casi 40 veces desde 2016. De otro lado, para el año 2023, este tipo de ataque afectó al 64,1 % de las empresas a nivel mundial[10], posicionando a los gobiernos y sus instituciones públicas como blancos estratégicos debido a la información sensible que manejan y la frecuente carencia de recursos especializados.

Los ataques DDoS continúan representando una de las principales amenazas para la disponibilidad de servicios digitales. Mediante el uso de redes de dispositivos comprometidos (botnets), los atacantes generan volúmenes masivos de tráfico malicioso con el objetivo de saturar infraestructuras tecnológicas, provocando interrupciones en plataformas críticas tanto del sector público como privado[11].

- **Riesgos asociados a la computación cuántica**

Si bien la computación cuántica se encuentra en desarrollo progresivo, el impacto potencial que puede tener respecto de la ciberseguridad es significativo. En particular, la capacidad futura de estos sistemas para vulnerar los algoritmos criptográficos actualmente utilizados plantea un desafío para la protección de la información como activo estratégico de la era digital[12].

Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape", octubre de 2024. (Publicado por la Oficina de las Naciones Unidas contra la Droga y el Delito).

9 De acuerdo con el Informe de Riesgos Globales 2024 del Foro Económico Mundial (WEF), la información falsa y la desinformación (potenciada por tecnologías como la inteligencia artificial) representa el riesgo global más severo a corto plazo ocupando el primer lugar, mientras que la ciberinseguridad y los ciberataques se consolidan en el cuarto lugar (4°) entre los riesgos con mayor probabilidad de desencadenar una crisis a gran escala. Foro Económico Mundial (2024). *The Global Risks Report 2024*. Disponible en: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

10 Observatorio CEPLAN. Incremento de controles y riesgos en el ciberespacio. https://observatorio.ceplan.gob.pe/ficha/tg73
Tomado originalmente de European Repository of Cyber Incidents (EuRepoC), «Cyber Incident Dashboard», 2025.

11 Los incidentes cibernéticos del tipo "interrupción" (cuyo objetivo es precisamente dejar fuera de servicio un proceso o infraestructura tecnológica) han experimentado un crecimiento dramático, multiplicándose por 36 veces (pasando de 10 casos en 2008 a 363 en 2024). Observatorio Nacional de Prospectiva CEPLAN. Incremento de controles y riesgos en el ciberespacio. Tomado originalmente de European Repository of Cyber Incidents, «Cyber Incident Dashboard,» 2025. Disponible en: https://eurepoc.eu/dashboard/

12 Observatorio Nacional de Prospectiva CEPLAN. Ruptura de ciberseguridad por capacidades cuánticas. Disponible en: https://observatorio.ceplan.gob.pe/ficha/RD7. Tomado originalmente del World Economic Forum (WEF), específicamente de su informe «*Quantum Economy Blueprint*» (2024). Disponible en: https://www.weforum.org/publications/quantum-economy-blueprint/

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Este escenario introduce la necesidad de anticipar la transición hacia esquemas de criptografía postcuántica, a fin de garantizar la confidencialidad e integridad de la información, así como la autenticidad de las transacciones digitales en el largo plazo[13].

En conjunto, estas tendencias evidencian que el panorama de riesgos es cada vez más dinámico y complejo, lo que exige una respuesta integral basada en el fortalecimiento de capacidades técnicas, la adopción de tecnologías de protección avanzadas y la consolidación de mecanismos de coordinación interinstitucional. Resulta necesario evolucionar hacia un enfoque proactivo y resiliente de la ciberseguridad, que no solo permita responder eficazmente a incidentes, sino también anticipar amenazas, reducir vulnerabilidades y garantizar la continuidad y confianza en el ecosistema digital nacional.

1.2. Contexto Nacional

El Perú ha logrado avances significativos en su proceso de transformación digital, impulsado por un sólido marco normativo que incluye la Ley de Gobierno Digital aprobada por el Decreto Legislativo N.° 1412 y su Reglamento aprobado por el Decreto Supremo N.° 029-2021-PCM. Estas normas tienen como finalidad optimizar la prestación de servicios digitales centrados en la ciudadanía y fomentar el desarrollo de la confianza en el entorno digital.

En este contexto, corresponde considerar el Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, el cual posiciona a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), como el ente rector en dicha materia. Bajo este marco opera el Centro Nacional de Seguridad Digital (CNSD), creado como la plataforma encargada de gestionar, dirigir, articular y responder a los incidentes de seguridad digital a nivel nacional.

Este ecosistema se complementa de manera transversal con la Ley N.° 29733, Ley de Protección de Datos Personales y su Reglamento aprobado por Decreto Supremo N.° 016-2024-JUS, a efectos de garantizar la adecuada tutela del derecho fundamental de autodeterminación informativa frente a los riesgos del uso de nuevas tecnologías.

De acuerdo con el Observatorio de Ciberseguridad del BID-OEA (2020)[14], en lo relativo al 2020, el Perú presentó una madurez desagregada por dimensiones e indicadores[15] que fue calificada como en Estadio 2 Formativo, lo que evidencia la existencia de estructuras institucionales, políticas públicas y marcos regulatorios orientados a la gestión de riesgos en el entorno digital.

---

13 Pascale Davies, en su artículo *«¿Qué es la amenaza cuántica y qué tienen que ver unas simples matemáticas con la protección de la seguridad mundial?»* (Euronews, 2024). Disponible en: https://acortar.link/7HHu0T

14 Banco Interamericano de Desarrollo & Organización de los Estados Americanos (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*, p. 15, 142-145. Disponible en: https://doi.org/10.18235/0002513.

15 El *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe* utilizó el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés) a fin de poder medir el crecimiento y el desarrollo de las capacidades de los Estados Miembros para defenderse de las crecientes amenazas del espacio cibernético. El Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones, diseñado en 2013 por el Centro Global de Capacidad en Seguridad Cibernética (GCSCC, por sus siglas en inglés) de la Universidad de Oxford, fue la base de los estudios regionales de la OEA y el BID en 2016 y 2020 y sigue un enfoque integral que entiende la capacidad dentro de cinco dimensiones: (i) política y estrategia; (ii) cultura y sociedad; (iii) educación, capacitación y habilidades; (iv) marcos legales y regulatorios, y (v) estándares, organizaciones y tecnologías.

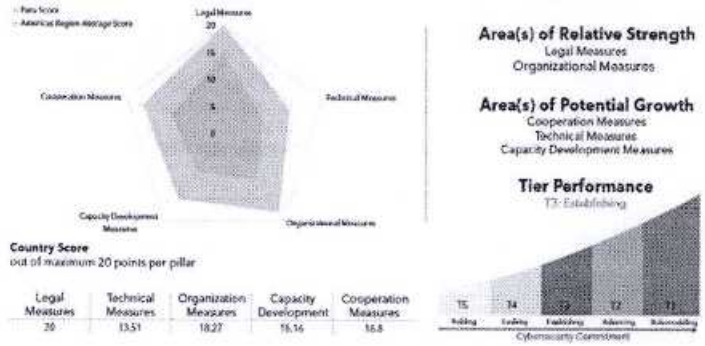
SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

El análisis anterior retomado en un estudio realizado por CEPAL[16] señaló que, respecto del Perú, como parte de la región América Latina y el Caribe, se observaba lo siguiente:

> *"una amplia necesidad en toda la región por hacer un esfuerzo extra para acompañar a las instituciones del ámbito tanto público como privado con normativas y leyes que sean actualizadas y oportunas, en las que se permita generar acciones preventivas tendientes a dificultar las actividades delictivas en el ciberespacio, donde también se favorezcan escenarios de rápida recuperación y protección de datos".*

Por su parte, el *Índice Global de Ciberseguridad 2024*[17] de la Unión Internacional de Telecomunicaciones (traducción libre del informe original en inglés) señala que el Perú obtuvo ubicación en el Nivel T3 – Establishing. Esta categoría comprende a los países que han alcanzado entre 55 y 85 puntos y que evidencian un compromiso básico con la ciberseguridad, mediante la evaluación, establecimiento o implementación de medidas generalmente aceptadas en un número moderado de pilares o indicadores.

Figura 1 . Desempeño de Perú en el Índice Global de Ciberseguridad 2024, según los cinco pilares de evaluación



Fuente: *Unión Internacional de Telecomunicaciones (UIT). (2024). Índice Global de Ciberseguridad 2024 (5.ª edición).*

El nivel Nivel T3 – Establishing para el Perú refleja un estado de **madurez intermedia**, en el cual el país ha logrado establecer bases institucionales y regulatorias relevantes, pero aún no alcanza un nivel avanzado de desarrollo técnico y operativo.

El análisis desagregado por pilares permite identificar con mayor precisión las fortalezas y brechas estructurales a nivel nacional. El Perú alcanza el puntaje máximo en el pilar de Medidas Legales (20/20), lo que evidencia la existencia de un marco normativo robusto y

---

16 Mariano, R. & Nuñez, G. (2023). *"Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe"*, Documentos de Proyectos (LC/TS.2023/93), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), p. 10, 21 y 22. https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

17 Unión Internacional de Telecomunicaciones (UIT). (2024). *Índice Global de Ciberseguridad 2024 (5ª Edición)*. Ginebra: ITU Publications. ISBN 978-92-61-38751-8 (Versión electrónica). https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

El Índice Global de Ciberseguridad (GCI) 2024 de la Unión Internacional de Telecomunicaciones - UIT es el instrumento que mide el compromiso de los países con la ciberseguridad a través de cinco pilares de acción (Medidas Legales, Medidas Técnicas, Medidas Organizacionales, Medidas de Desarrollo de Capacidad y Medidas de Cooperación). Cada pilar se evalúa con un máximo de 20 puntos.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

alineado con estándares internacionales, así como un alto desempeño en Medidas Organizacionales (18.27/20), lo que confirma la existencia de estructuras institucionales orientadas a la gestión de la ciberseguridad.

Por otro lado, el país presenta niveles intermedios en los pilares de Medidas de Cooperación (16.8/20) y las Medidas de Desarrollo de Capacidad (15.16/20), lo que refleja avances en la articulación interinstitucional y en la formación de capacidades, aunque aún resultan insuficientes para alcanzar un nivel de madurez avanzado.

La principal brecha estructural se observa en el pilar de **Medidas Técnicas**, donde el Perú obtiene un puntaje de 13.51/20, **el más bajo entre los cinco pilares evaluados**, lo que evidencia limitaciones en la implementación efectiva de controles técnicos, capacidades de detección, respuesta y resiliencia frente a incidentes de seguridad digital.

De acuerdo a la información del estudio de la ITU, la diferencia entre el alto desempeño en el pilar legal y el menor resultado en el pilar técnico evidencia una brecha estructural entre el desarrollo normativo y la capacidad operativa en el país. Esto refleja que, aunque el Perú ha avanzado en la adopción de marcos regulatorios, persisten limitaciones técnicas e institucionales para su implementación efectiva, situación característica de países en proceso de consolidación digital.

En línea con lo anterior, mediante el reporte Resultados Índice Global de Ciberseguridad 2024 (diciembre de 2024), la Secretaría de Gobierno y Transformación Digital de la PCM analizó el desempeño del Perú en comparación con el 2020[18], identificando avances regulatorios, pero también persistentes deficiencias en la implementación de medidas técnicas de defensa en materia de seguridad digital, como se muestra en la siguiente figura:

Figura 2. Evolución de Perú en el Índice Global de Ciberseguridad 2024

Al comparar los resultados de 2024 con los de 2020, edición anterior a la del 2024, **se observa una mejora en todos los criterios evaluados**: Legal, técnico, organizacional, desarrollo de capacidades y cooperación.

CRITERIO	2024		2020		Variación en puntos 2024 - 2020	Variación en posición 2024 - 2020
	Puntos	Posición regional	Puntos	Posición regional		
Legal	20	2	20	2	0	0
Técnico	13.51	10	11.58	7	+1.93	↘ -3
Organizacional	18.27	5	5.63	15	+12.64	↗ +10
Desarrollo de capacidades	15.16	5	5.32	14	+9.84	↗ +9
Cooperación	16.8	4	13.15	6	+3.65	↗ +2



Fuente: *Secretaría de Gobierno y Transformación Digital (SGTD-PCM). (2024). Resultados del Índice Global de Ciberseguridad 2024, p. 14.*

De acuerdo con los resultados mostrados en la Figura II, la SGTD de la PCM concluyó que el Perú mantiene una brecha relevante en infraestructura tecnológica y capacidades operativas, lo que limita su capacidad para detectar, prevenir y mitigar amenazas de manera eficaz, especialmente en el ámbito de la resiliencia técnica y la infraestructura especializada.

En esa lógica, el reporte de la SGTD recomendó aumentar la inversión en tecnologías de protección, monitoreo de amenazas y respuesta a incidentes; realizar un esfuerzo más

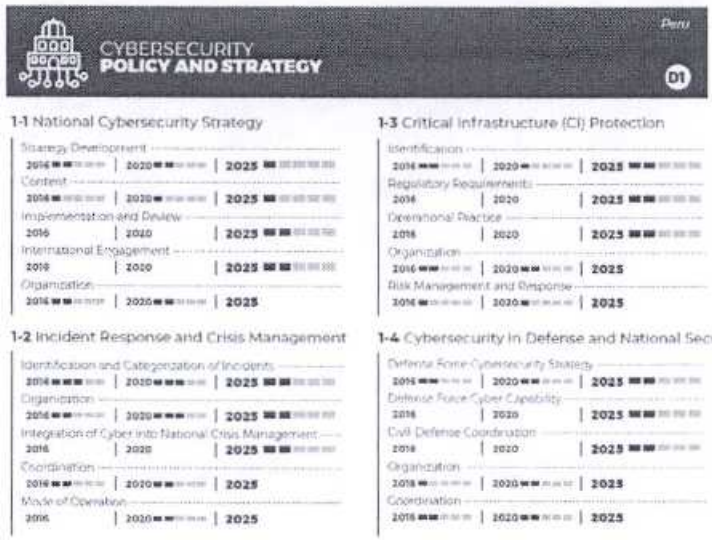
18 Secretaría de Gobierno y Transformación Digital (SGTD-PCM) – Presidencia del Consejo de Ministros. Reporte Resultados índice Global de Ciberseguridad 2024. Secretaría de Gobierno y Transformación Digital. Disponible en: https://www.gob.pe/institucion/pcm/informes-publicaciones/6283830-peru-en-el-indice-global-de-ciberseguridad-2024-retos-y-oportunidades

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

coordinado para fortalecer los pilares de capacidades técnicas y cooperación interinstitucional; fortalecer participación del país en iniciativas de cooperación internacional; priorizar la creación de infraestructura más robusta; consolidar redes robustas de colaboración internacional, entre otros aspectos.

Finalmente, conviene tomar en cuenta la información del Reporte de Ciberseguridad 2025: Desafíos de Vulnerabilidad y Madurez para Cerrar las Brechas en América Latina y el Caribe[19], que señala que el Perú presentó una madurez que fue calificada predominantemente entre el Estadio 2 (Formativo), evidenciando la existencia de estructuras institucionales, políticas públicas y marcos normativos orientados a la gestión de riesgos digitales y destacando la creación del Centro Nacional de Seguridad Digital (CNSD), la labor operativa del PeCERT y la adhesión a convenios internacionales contra el cibercrimen, operando activamente en el marco de la Política Nacional de Transformación Digital.

Figura 3. Evaluación de la madurez de la ciberseguridad de Perú por dimensiones, 2025.



Porrúa, Miguel, Guillermo Moncayo, Santiago Paz, Ariel Nowersztern, Jorge Fernando Bejarano, Maria Florencia Baudino, Maria Paula Bordese, et al. 2025. *2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean.* https://doi.org/10.18235/0013872 . Disponible en: https://publications.iadb.org/en/2025-cybersecurity-report-vulnerability-and-maturity-challenges-bridging-gaps-latin-america-and

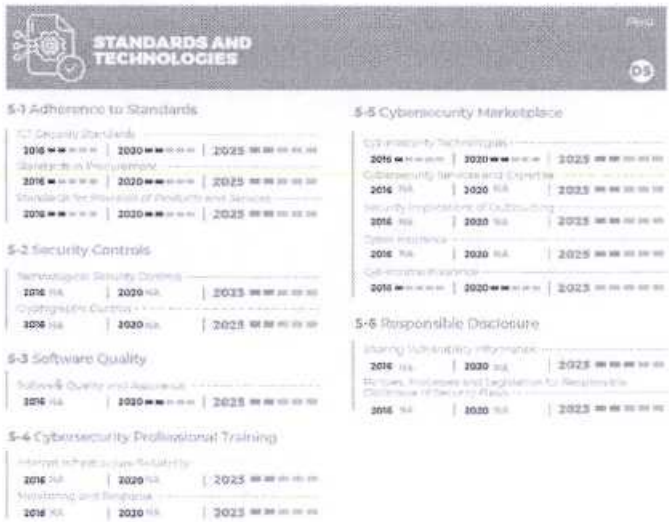
SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ



PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Gobierno y Transformación Digital
PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Tecnologías y Servicios
PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Gobierno y Transformación Digital

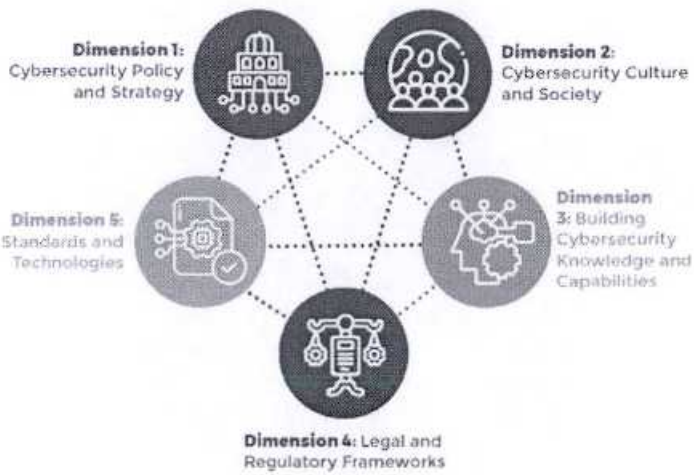
SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe



Fuente: *Porrúa, M. et al. (2025), 2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean, pp. 144-146.*

De las figuras anteriores, es posible apreciar que, para evaluar el nivel de madurez de la capacidad de ciberseguridad del Perú, el Reporte de Ciberseguridad 2025 analizó 5 dimensiones claramente determinadas:

Figura 4. Dimensiones para la evaluación de la madurez de la ciberseguridad



Fuente: *Porrúa, M. et al. (2025). 2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean, p. 37.*

Conforme al Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM), se evalúa el nivel de madurez de las capacidades de ciberseguridad de un país, asignando una etapa específica que corresponde a su grado de logro en ciberseguridad. Las 5 (cinco) etapas de madurez, que se asignan mediante una evaluación, van desde la más básica (Inicio) hasta la más avanzada (Dinámica), como se aprecia en la figura siguiente:

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Figura 5. Etapas de madurez del Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM)



Fuente: *Porrúa, M. et al. (2025). 2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean, p. 30.*

De la revisión de las 5 dimensiones analizadas, para el 2025, el Perú se encuentra prioritariamente en un **nivel de madurez 2 (Formativo)**, lo cual, conforme a los términos del estudio precitado, implica una situación en la que algunas características han comenzado a desarrollarse y formularse y ello puede demostrarse claramente, sin embargo, esto se ha dado de forma desorganizada, mal definida o simplemente nueva.

No obstante, es posible identificar que, en las dimensiones 2, 4 y 5, se puede encontrar 3 indicadores que lograron una calificación en nivel de madurez de 3 (Establecido)[20] estos son: "Conciencia de los riesgos" en la Dimensión 2; "Legislación sobre protección de datos" en la Dimensión 4, "Compartir información sobre vulnerabilidades" en la dimensión 5.

Finalmente, resulta indispensable comentar que, en la dimensión 4, hay que destacar el caso de los indicadores "Evaluación del impacto en los derechos humanos" y "Legislación sobre propiedad intelectual", los cuales tienen un **nivel 1 (Puesta en marcha)**[21].

De acuerdo con el Estudio de Ciberseguridad 2025, el Perú se encuentra en una etapa de institucionalización y consolidación caracterizada por avances significativos en gobernanza y marco normativo, siendo indispensable impulsar la implementación práctica, a través del desarrollo de capacidades técnicas, operativas e institucionales en ciberseguridad.

---

20 La calificación de nivel de madurez 3 (Establecido) involucra lo siguiente: *"Los indicadores del Aspecto están en marcha, y la evidencia demuestra que funcionan. Sin embargo, no se ha considerado detenidamente la asignación relativa de recursos. Se han tomado pocas decisiones que evalúen las compensaciones en relación con la inversión relativa en los diversos elementos del Aspecto. Pero el Aspecto es funcional y está definido".*

21 *"En esta etapa, o bien no existe madurez en ciberseguridad, o bien esta se encuentra en una fase muy incipiente. Puede que se estén llevando a cabo conversaciones iniciales sobre el desarrollo de capacidades en ciberseguridad, pero no se han tomado medidas concretas. Es posible que no haya evidencia observable en esta etapa".*

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

1.3. Contexto institucional

El Centro Nacional de Seguridad Digital (CNSD) de la Secretaría de Gobierno y Transformación Digital ha sido creado en virtud del artículo 7 del Decreto de Urgencia N.° 007-2020 como la plataforma oficial encargada legalmente de gestionar, dirigir, articular y supervisar la operación de la seguridad digital a nivel nacional.

El CNSD gestiona los reportes del Registro Nacional de Incidentes de Seguridad Digital y centraliza la información a escala país, dado que el numeral 9.1 del artículo 9 del citado Decreto de Urgencia en concordancia con el artículo 18.1 de su Reglamento, aprobado por Decreto Supremo N.° 126-2025-PCM, impone a las entidades de la administración pública, así como a los proveedores de servicios digitales del sector financiero, servicios básicos, salud, transporte y actividades críticas, la obligación legal e ineludible de notificar al CNSD todo incidente de seguridad digital en sus organizaciones.

De este modo, la información que custodia y procesa el CNSD no representa una muestra sectorial, sino que constituye evidencia oficial de alcance nacional sobre el panorama general de la ciberseguridad en el Estado Peruano.

Ahora bien, según información remitida por el CNSD[22], del 2024 a enero 2026, es posible observar una actividad sostenida y prioritariamente enfocada en asistencia técnica, capacitación ciudadana, gestión de incidentes y alertas de ciberseguridad.

La mayor carga operativa se concentra en acciones de capacitación ciudadana, seguida de asistencia técnica y emisión de alertas/comunicados, lo que evidencia que el CNSD ha tenido un enfoque mixto entre fortalecimiento preventivo y respuesta operativa.

En términos acumulados, y en resultados consolidados por tipo de actividad (2024 a enero 2026) se registran los siguientes resultados:

- Capacitación ciudadana: 20,150 acciones
- Asistencia técnica: 2,653 intervenciones
- Alertas / comunicados emitidos: 2,376
- Incidentes reportados: 1,094
- Informes de vulnerabilidades: 628
- Eventos (Simulacros de ataques): 2

Figura 6. Resultados consolidados por tipo de actividad del Centro Nacional de Seguridad Digital, 2024 – enero de 2026



Fuente: *Elaboración propia con base en información remitida por el Centro Nacional de Seguridad Digital (CNSD), 2026. Elaborado con apoyo de herramientas de inteligencia artificial.*

22 CALIZAYA, Gabriel. 2026, Coordinador General del Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la PCM. [Cooperación Digital] Estrategia Nacional de Seguridad Digital. Correo electrónico del 26 de febrero de 2026 a la Subsecretaría de Políticas y Regulación de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Como se puede apreciar, del 2024 a enero de 2026, la capacitación ciudadana representa la principal línea de intervención, concentrando el mayor volumen de acciones del período analizado. Asimismo, al revisar la información por cada año, los resultados son los siguientes:

En el año 2024:

En términos anuales, el año **2024 (enero a diciembre)** muestra una actividad equilibrada entre prevención (capacitaciones y alertas) y gestión operativa (incidentes y vulnerabilidades) presentando los siguientes datos:

- Asistencia técnica: 1,030
- Capacitación ciudadana: 4,269
- Incidentes reportados: 505
- Informes de vulnerabilidades: 396
- Alertas/comunicados: 1,206
- Simulacros: 1

Figura 7. Resultados 2024 (enero a diciembre)



Fuente: *Elaboración propia con base en información remitida por el Centro Nacional de Seguridad Digital (CNSD), 2026. Elaborado con apoyo de herramientas de inteligencia artificial.*

En el año 2025:

Por su parte, durante el año **2025 (enero a diciembre)** se evidencia un incremento significativo en capacitación ciudadana (más de tres veces respecto de 2024), lo que sugiere una priorización estratégica del fortalecimiento de capacidades y cultura de ciberseguridad. Asimismo, la asistencia técnica aumenta en aproximadamente 45% respecto al año anterior. En contraste, los informes de vulnerabilidades disminuyen.

Los datos reportados para el 2025 (enero a diciembre) son los siguientes:

- Asistencia técnica: 1,501
- Capacitación ciudadana: 15,334
- Incidentes reportados: 536
- Informes de vulnerabilidades: 220
- Alertas/comunicados: 1,092
- Simulacros: 1

Es importante resaltar que en julio de 2025 se realizó el *Simulacro de Ataques Cibernéticos 2025* en el que participaron 392 entidades públicas y privadas para poner a prueba sus

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

protocolos de defensa y respuesta ante incidentes críticos. Este ejercicio estratégico permitió identificar brechas y fortalecer las capacidades nacionales, reafirmando el compromiso del Estado con la protección de la soberanía y la confianza digital[23].

Figura 8. Resultados 2025 (enero a diciembre)



Fuente: *Elaboración propia con base en información remitida por el Centro Nacional de Seguridad Digital (CNSD), 2026. Elaborado con apoyo de herramientas de inteligencia artificial.*

<u>En el año 2026</u>:

En lo relativo al año **2026**, al tratarse de información correspondiente únicamente al mes de enero, los valores no son comparables en términos anuales, pero permiten advertir continuidad operativa en todas las líneas de acción. Los datos son los siguientes:

- Asistencia técnica: 122
- Capacitación ciudadana: 547
- Incidentes reportados: 53
- Informes de vulnerabilidades: 12
- Alertas/comunicados: 78
- Simulacros: 0

[23] Presidencia del Consejo de Ministros. (2025). *PCM realizó el Segundo Simulacro Internacional de Ataques Cibernéticos 2025.* Plataforma digital única del Estado Peruano. https://www.gob.pe/institucion/pcm/noticias/1207704-pcm-realizo-el-segundo-simulacro-internacional-de-ataques-ciberneticos-2025

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Figura 9. Resultados 2026 (enero)



***Fuente**: Elaboración propia con base en información remitida por el Centro Nacional de Seguridad Digital (CNSD), 2026. Elaborado con apoyo de herramientas de inteligencia artificial.*

1.4. Tendencias identificadas

El análisis de la evolución de los indicadores durante el período evaluado permite identificar tendencias relevantes para la toma de decisiones estratégicas.

En primer lugar, se observa una expansión significativa de las acciones de capacitación ciudadana durante el año 2025, consolidándose esta línea de intervención como uno de los ejes centrales de la gestión. El incremento sustancial respecto de 2024 refleja una apuesta institucional por el fortalecimiento de la cultura de ciberseguridad y la sensibilización ciudadana como mecanismo preventivo frente a los riesgos digitales.

En segundo término, se evidencia un crecimiento sostenido en la asistencia técnica brindada a entidades, lo que sugiere una mayor demanda institucional de acompañamiento especializado. Este comportamiento puede interpretarse como un indicador de mayor confianza en el soporte técnico disponible, pero también como señal de que persisten brechas en capacidades internas que requieren ser atendidas.

Por otro lado, el número de incidentes reportados se mantiene relativamente estable en el período analizado. Esta estabilidad podría responder, por un lado, al mantenimiento del nivel de exposición frente a amenazas de seguridad digital o, por otro, a una mejora en los mecanismos de detección y reporte, lo que permitiría una visibilización más consistente de los eventos de seguridad.

En contraste, se aprecia una reducción en los informes de vulnerabilidades durante 2025, lo que amerita un análisis técnico más detallado para determinar la causa.

Finalmente, se constata una baja frecuencia de ejercicios de simulación, con la realización de un solo simulacro anual. Este aspecto revela una oportunidad clara de fortalecimiento en materia de preparación operativa y resiliencia institucional, considerando que los ejercicios periódicos constituyen un componente esencial para evaluar la capacidad de respuesta ante escenarios de crisis de seguridad digital.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

En complemento con lo anterior, es importante considerar los Indicadores de Transformación Digital, Reporte de avances en gobierno y transformación digital[24], en lo relativo al componente de Seguridad y Confianza Digital, los cuales presentan la información, a nivel de gobierno nacional y regional, sobre el despliegue de equipos de respuesta ante incidentes a nivel regional, así como las alertas de incidentes reportados.

Así, en dicho reporte se indica que, en el ámbito de Ministerios, el 89.47% implementó el Equipo de Respuesta ante Incidentes de Seguridad Digital, mientras que el 100% implementó el Sistema de Gestión de Seguridad de la Información.

A diferencia de lo anterior, en lo referido a gobiernos regionales, se aprecia que el 65.38% implementaron el Equipo de Respuesta ante Incidentes de Seguridad Digital, mientras que el 26.92% implementó el Sistema de Gestión de Seguridad de la Información.

En suma, el período analizado evidencia una consolidación progresiva de capacidades institucionales en materia de sensibilización y acompañamiento técnico, destacando la expansión significativa de la capacitación ciudadana durante 2025 como eje preventivo de la gestión. Este comportamiento refleja una priorización estratégica orientada a fortalecer la cultura y reducir riesgos asociados al factor humano.

Sin embargo, el análisis integral de los indicadores también revela la necesidad de robustecer la dimensión técnico-operativa del sistema nacional. En particular, resulta imprescindible intensificar la realización de ejercicios de simulación y fortalecer los mecanismos sistemáticos de identificación, análisis y gestión de vulnerabilidades. Ello permitirá transitar de un enfoque predominantemente formativo y reactivo hacia un modelo más integral de resiliencia, basado en capacidades de detección temprana, respuesta coordinada y mejora continua.

II. ALINEACIÓN CON INSTRUMENTOS NACIONALES E INTERNACIONALES

2.1. Marco normativo en materia de ciberseguridad en el Perú

El desarrollo de la ciberseguridad en el Perú se sustenta en un conjunto articulado de normas y gobernanza institucional que se estructura sobre 3 (tres) regímenes especializados y complementarios que operan sobre objetos distintos y se articulan mediante instrumentos de coordinación.

En primer lugar, el Marco de Confianza Digital y el Marco de Seguridad Digital del Estado Peruano, orientados a garantizar la continuidad de los servicios digitales y salvaguardar los derechos de las personas en el entorno digital. Uno de los instrumentos centrales es el Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. Esta norma define la ciberseguridad como la capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos frente a amenazas y vulnerabilidades en el entorno digital, y la determina como la perspectiva técnica de la seguridad digital[25].

---

[24] Información disponible en: https://indicadores.digital.gob.pe/
Revisado el 25 de febrero de 2026.

[25] Literal h) del artículo 3 del Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital
"Artículo 3. Definiciones
Para la aplicación del presente Decreto de Urgencia se establece las siguientes definiciones:
(...) h) Ciberseguridad.- Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país".

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Asimismo, establece la gobernanza institucional para la gestión de incidentes de seguridad digital, creando el Centro Nacional de Seguridad Digital (CNSD)[26] y el Equipo de Respuesta a Incidentes de Seguridad Digital Nacional (CSIRT Nacional) como instancias operativas responsables de la coordinación, gestión y respuesta ante incidentes de seguridad digital a nivel país[27]. Se desarrolla mediante el Decreto Supremo N.° 126-2025-PCM, que aprueba el Reglamento del Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

Complementariamente, el Decreto Legislativo N.° 1412, Ley de Gobierno Digital, y su Reglamento aprobado por Decreto Supremo N.° 029-2021-PCM, establecen el marco de gobernanza del gobierno digital en el país y el Marco de Seguridad Digital. En este marco, se dispone la obligación de las entidades públicas de implementar Sistemas de Gestión de Seguridad de la Información (SGSI)[28], designar al Oficial de Seguridad y Confianza Digital (OSCD)[29] y establecer capacidades institucionales de respuesta a incidentes de seguridad digital mediante equipos CSIRT institucionales[30].

En segundo lugar, el régimen vinculado a los activos críticos nacionales, el cual regula la identificación, evaluación, gestión de riesgos, protección y continuidad de los Activos Críticos Nacionales, entendidos como recursos, infraestructuras y sistemas indispensables para mantener o desarrollar capacidades nacionales. Su afectación, perturbación o destrucción no permite soluciones alternativas inmediatas y puede generar grave perjuicio a la Nación[31].

La Dirección Nacional de Inteligencia (DINI) interviene como autoridad técnica normativa estrictamente en el ámbito de su competencia, de conformidad con el artículo 17.8 del Decreto Legislativo N.° 1141. Con respecto a los Activos Críticos Nacionales (ACN), si bien la identificación y evaluación de sus riesgos recae legalmente sobre cada operador bajo la supervisión del sector responsable, la DINI ejerce el rol de Coordinador General de dicho

---

26 Numeral 7.1 del artículo 7 del Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital.

27 Numeral 7.4 del artículo 7 del Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y el numeral 27.1 del artículo 27 del Reglamento del Decreto de Urgencia N.° 007-2020 aprobado por Decreto Supremo N.° 126-2025-PCM.

28 Literal a) del Artículo 105 y numeral 109.3 del artículo 109 del Reglamento de la Ley de Gobierno Digital, aprobado por Decreto Supremo N.° 029-2021-PCM.

29 Numeral 111.3 del artículo 111 del Reglamento de la Ley de Gobierno Digital, aprobado por Decreto Supremo N.° 029-2021-PCM.

30 Numeral 104.2 del artículo 104 del Reglamento de la Ley de Gobierno Digital, aprobado por Decreto Supremo N.° 029-2021-PCM.

31 Cfr. Decreto Supremo N.° 106-2017-PCM, Reglamento para la Identificación, Evaluación y Gestión del Riesgo de los Activos Críticos Nacionales; Ley N.° 30618, Ley que modifica el Decreto Legislativo N.° 1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI, a fin de regular la seguridad digital; Decreto Legislativo N.° 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI; Decreto Legislativo N.° 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional; Ley N.° 30535, Ley que modifica el Decreto Legislativo 1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia – DINI.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

proceso, validando las propuestas sectoriales y administrando el Inventario Nacional (Artículo 9 del Decreto Supremo N.° 106-2017-PCM).

Finalmente, en estricta aplicación del numeral 8.5 del Decreto Supremo N.° 106-2017-PCM, el Consejo de Seguridad y Defensa Nacional (COSEDENA) es la máxima instancia con competencia para aprobar y actualizar el Inventario Nacional de Activos Críticos Nacionales (INACN) propuesto por la DINI.

Los sectores responsables previstos en el Anexo 4 del Decreto Supremo N° 106-2017-PCM participan en la identificación, evaluación de criticidad, propuesta sectorial al Inventario Nacional y seguimiento de medidas aplicables a los operadores. Asimismo, los operadores de Activos Críticos Nacionales ejecutan las medidas de protección, continuidad, gestión de riesgos y seguridad digital que correspondan conforme a su responsabilidad sobre el activo[32].

Según información brindada por la DINI[33], al cierre del 2025, el Inventario Nacional registra cincuenta Activos Críticos Nacionales y aproximadamente ochenta y tres operadores conforme a la depuración institucional vigente, distribuidos en diez de los trece sectores responsables previstos en el Anexo 4 del Decreto Supremo N° 106-2017-PCM.

Finalmente, dada su vinculación con la ciberseguridad, corresponde referenciar la Ley N.° 30999, Ley de Ciberdefensa. Esta norma tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.

Asimismo, mediante Decreto Supremo N.° 017-2024-PCM se aprueba el Reglamento de la Ley 30999, Ley de Ciberdefensa, el cual tiene por objeto establecer las disposiciones normativas para regular las capacidades de ciberdefensa, operaciones militares, y uso de la fuerza en y mediante el ciberespacio, entre otras disposiciones para preservar la seguridad nacional, a cargo de los órganos ejecutores del Ministerio de Defensa, dentro de su ámbito de competencia, en el marco de la Ley N.° 30999, Ley de Ciberdefensa.

2.2. Alineación con instrumentos estratégicos nacionales

- **Política Nacional de Transformación Digital**

La Estrategia Nacional de Ciberseguridad (ENC) y la Política Nacional de Transformación Digital (PNTD) guardan una relación de coherencia y complementariedad estratégica, en la medida en que ambas se enmarcan en el proceso de consolidación de un entorno digital seguro, confiable y resiliente para el país.

---

32 Cfr. Norma Técnica N.° 001-DINI-01 (06 de enero de 2022) que desarrolla el procedimiento técnico de identificación, evaluación anual de riesgos, canal seguro de comunicación operativa y designación de Funcionarios Responsables Sectoriales; Resolución de la Dirección de Inteligencia Nacional N° 087-2020-DINI-01, Directiva de Identificación y Validación de los Activos Críticos Nacionales; Resolución de la Dirección de Inteligencia Nacional N° 096-2021-DINI-01, Guía Metodológica para la Identificación, Análisis y Evaluación de Riesgos de los Activos Críticos Nacionales; Decreto Supremo N° 007-2019-DE, Directiva Nacional de Seguridad y Defensa Nacional para la protección de los Activos Críticos Nacionales.

33 Borda, Erick. Dirección Nacional de Inteligencia de la PCM. Correo electrónico del 29 de mayo de 2026 a la Subsecretaría de Políticas y Regulación de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

A nivel nacional, la Estrategia Nacional de Ciberseguridad operativiza los objetivos estratégicos de la Política Nacional de Transformación Digital, específicamente, tiene vinculación con el **Objetivo Prioritario 5** (Consolidar la seguridad y confianza digital en la sociedad); el **Objetivo Prioritario 4** (Fortalecer el talento digital en todas las personas); el **Objetivo Prioritario 6** (Garantizar el uso ético y adopción de las tecnologías exponenciales y la innovación en la sociedad) y el **Objetivo Prioritario 3** (Garantizar la disponibilidad de servicios públicos digitales inclusivos, predictivos y empáticos con la ciudadanía).

En ese marco, la PNTD constituye el instrumento de política pública que orienta la transformación digital a nivel nacional, definiendo objetivos, lineamientos y prioridades para el desarrollo del ecosistema digital. Por su parte, la ENC se configura como un instrumento estratégico que desarrolla, profundiza y operativiza el aspecto de la ciberseguridad, incorporando objetivos y acciones técnicas, organizacionales y de gobernanza que resultan necesarias para asegurar la continuidad, integridad, disponibilidad y resiliencia de los entornos digitales.

Desde esta perspectiva, la ENC se articula a la PNTD al traducir sus orientaciones generales en acciones específicas para la prevención, detección, respuesta y recuperación frente a incidentes y amenazas de seguridad digital.

- **Gestión de riesgos**
  Mientras la PNTD promueve la generación de confianza en el entorno digital y la adopción de enfoques de gestión de riesgos, la ENC debe desarrollar esa orientación desde una lógica operativa y especializada, mediante el fortalecimiento de capacidades nacionales de prevención, monitoreo, respuesta y recuperación. Ello comprende, entre otros aspectos, el impulso de arquitecturas técnicas, mecanismos de articulación operativa y medidas orientadas a la protección frente a amenazas digitales.

- **Desarrollo de talento y cultura de ciberseguridad**
  Ambos instrumentos reconocen la centralidad del factor humano en la transformación digital. En línea con la PNTD, la ENC debe priorizar el desarrollo de competencias digitales y habilidades para la ciudadanía en general, complementando dicho enfoque con el fortalecimiento de capacidades especializadas en ciberseguridad, incluyendo formación técnica, certificación en ámbitos críticos para la seguridad digital del país.

- **Gobernanza y sostenibilidad del gobierno digital**
  La PNTD impulsa la consolidación de servicios públicos digitales, interoperables, inclusivos y centrados en las personas. De acuerdo con ello, corresponde que la ENC incorpore la ciberseguridad como condición habilitante y transversal para la sostenibilidad de dichos servicios, proponiendo el fortalecimiento de la rectoría, la clarificación de roles y responsabilidades y la consolidación del marco normativo a efectos de implementación efectiva de las obligaciones en la materia.

- **Cooperación internacional y articulación externa.**
  La PNTD reconoce el valor de la cooperación internacional para acelerar la innovación, la adopción tecnológica y el desarrollo del ecosistema digital. En línea con ello, la ENC debe aterrizar esta dimensión en el ámbito específico de la ciberseguridad, promoviendo la integración del país en redes de cooperación técnica, la adopción de estándares y buenas prácticas internacionales, así como el intercambio de información e inteligencia sobre amenazas digitales.

PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Gobierno y Transformación Digital
PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Tecnologías Digitales
PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Servicios e Innovación Digital
PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Gobierno y Transformación Digital

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Figura 10. Coherencia y complementariedad estratégica entre la ENC y la PNTD



Fuente: *Elaboración propia con base en la Política Nacional de Transformación Digital y la Estrategia Nacional de Ciberseguridad. Elaborado con apoyo de herramientas de inteligencia artificial.*

En consecuencia, la ENC debe entenderse como un instrumento de desarrollo estratégico especializado que fortalece la implementación de la PNTD en el componente de ciberseguridad, permitiendo cerrar brechas técnicas, institucionales y operativas que no pueden ser abordadas únicamente desde una política general de transformación digital.

El detalle de esta alineación se desarrolla en el Anexo I.

Asimismo, refuerza su visión a largo plazo al alinearse con:

- **Las Políticas de Estado del Acuerdo Nacional:**

  La Política 35, relativa a la sociedad de la información y del conocimiento, dispone que el Estado promueva las condiciones para que la población se desenvuelva de manera segura en el entorno digital, garantizando simultáneamente un internet libre y abierto con adecuado resguardo de la seguridad de la información.

  De esta forma se proporciona el fundamento estratégico para fortalecer las capacidades nacionales de prevención, protección y respuesta frente a riesgos y amenazas de seguridad en el entorno digital, reduciendo vulnerabilidades y asegurando la continuidad de los servicios esenciales, la generación segura de contenidos, servicios y bienes digitales; la protección de la información y la estabilidad del país en el entorno digital.

Tabla 1. Alineación de las Políticas de Estado del Acuerdo Nacional con los Objetivos de la ENC

Política de Estado del Acuerdo Nacional	Objetivo Estratégico de la ENC	Sustento de la alineación
Política de Estado N.° 35: Sociedad de la información y sociedad del conocimiento.	**OE1.** Fortalecer las capacidades nacionales de prevención, detección, respuesta y recuperación ante incidentes de seguridad digital en las entidades del ecosistema digital a nivel nacional.	La Política 35 establece que el desarrollo de la sociedad de la información debe permitir que las personas se desempeñen de manera segura en el entorno digital y dispone el adecuado resguardo de la seguridad de la información. La ENC contribuye a esta finalidad mediante mecanismos nacionales para prevenir,

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

		detectar, responder y recuperarse frente a incidentes de seguridad digital.
	OE2. Fortalecer la ciberseguridad de los activos críticos nacionales, las actividades críticas y los servicios públicos esenciales frente a amenazas de seguridad digital.	La Política 35 promueve el uso transversal de las TIC en ámbitos como la educación, salud, conservación del ambiente, seguridad ciudadana, prevención de riesgo de desastres, gobierno abierto, defensa nacional, innovación, investigación, transferencia de conocimiento y sectores productivos y sociales, junto con el adecuado resguardo de la seguridad de la información. La ENC genera condiciones de protección y resiliencia para los activos y servicios que sustentan ese uso intensivo de tecnologías digitales.
	OE3. Desarrollar una cultura nacional de ciberseguridad y sólidas capacidades operativas en el talento humano del sector público y la ciudadanía.	La Política 35 promueve la inclusión y alfabetización digital para reducir las brechas existentes y generar igualdad de oportunidades. La ENC desarrolla esta orientación mediante educación, capacitación, especialización, certificación, asistencia técnica e investigación en ciberseguridad, fortaleciendo las capacidades necesarias para una participación segura en la sociedad digital y reducir la brecha de alfabetización digital.
	OE5. Fortalecer la gobernanza y el marco normativo en ciberseguridad en las entidades de la administración pública.	La Política 35 plantea el uso de las TIC para fortalecer la gobernabilidad democrática y promover un servicio moderno, transparente, eficiente y descentralizado. La ENC operacionaliza esta orientación mediante el fortalecimiento de la gobernanza, rectoría, supervisión y marco normativo de ciberseguridad, incorporando además la seguridad en la planificación del gobierno digital.

Fuente: *Elaboración propia, sobre la base de las Políticas de Estado del Acuerdo Nacional y la ENC.*

- **El Plan Estratégico de Desarrollo Nacional al 2050:**

En el Plan Estratégico de Desarrollo Nacional al 2050, la ciberseguridad se configura como un eje transversal imprescindible para la protección de la ciudadanía, la estabilidad institucional, la economía y la soberanía del país, integrándose de manera directa en 3 (tres) objetivos nacionales.

En el **Objetivo Nacional 2** (Territorio Sostenible), se reconoce la ciberseguridad como componente de la defensa nacional y de la gestión de amenazas, a través de la Acción Estratégica 2.8.3, orientada a garantizar el uso, desarrollo y gestión del ciberespacio frente a riesgos que afecten la seguridad y la confianza de las personas, la prosperidad económica y social y los intereses nacionales, cuyo cumplimiento se monitorea mediante indicadores internacionales como el Índice Global de Ciberseguridad.

Por su parte, en el **Objetivo Nacional 3** (Competitividad e Innovación), la seguridad y la confianza digital se conciben como condiciones habilitantes para el desarrollo económico basado en tecnologías, el comercio electrónico, los datos abiertos y la innovación productiva.

Asimismo, en el **Objetivo Nacional 4** (Democracia y Paz), la ciberseguridad es la herramienta clave para asegurar un Estado efectivo y proteger a la sociedad. Esto se evidencia en acciones orientadas a reducir la victimización ciudadana mediante el uso de la ciberinteligencia en todos los componentes del Sistema Nacional de Seguridad Ciudadana frente al crimen organizado.

En conjunto, estas disposiciones evidencian que la ciberseguridad constituye el soporte estructural que permite al Estado peruano defender su soberanía en el ciberespacio, prevenir y neutralizar el cibercrimen y consolidar un entorno confiable para la transformación digital y el crecimiento económico sostenible.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Tabla 2. Alineación del PEDN al 2050 con los Objetivos de la ENC

Objetivo Nacional / Objetivo específico del PEDN al 2050	Objetivo Estratégico de la ENC vinculada	Sustento de la alineación
ON2. Gestionar el territorio de manera sostenible a fin de prevenir y reducir los riesgos y amenazas que afectan a las personas y sus medios de vida, con el uso intensivo del conocimiento y las comunicaciones, reconociendo la diversidad geográfica y cultural, en un contexto de cambio climático. **OE 2.8.** Garantizar la defensa de los intereses nacionales destinados a la paz y seguridad internacional.	**OE1.** Fortalecer las capacidades nacionales de prevención, detección, respuesta y recuperación ante incidentes de seguridad digital en las entidades del ecosistema digital a nivel nacional. **OE2.** Fortalecer la ciberseguridad de los activos críticos nacionales, las actividades críticas y los servicios públicos esenciales frente a amenazas de seguridad digital. **OE6.** Desarrollar capacidades nacionales de gestión de riesgos digitales e inteligencia en ciberseguridad en las entidades del estado y sectores estratégicos.	La AE 2.8.3 del PEDN incorpora expresamente la seguridad y confianza digital y la gestión del ciberespacio frente a riesgos que puedan afectar a las personas, la prosperidad y la seguridad nacional. La ENC operacionaliza esta orientación mediante capacidades de prevención, monitoreo, detección, respuesta y recuperación, protección de activos críticos nacionales y servicios esenciales, gestión de riesgos para evitar desestabilizar la seguridad nacional o la prosperidad económica y social.
ON3. Elevar los niveles de competitividad y productividad con empleo decente y en base al aprovechamiento sostenible de los recursos, el capital humano, el uso intensivo de la ciencia y tecnología, y la transformación digital del país. **OE 3.5.** Elevar la capacidad científica y de innovación tecnológica del país, en base a la investigación, creación, adaptación y transferencia tecnológica y científica, y el impulso al proceso nacional de transformación digital; favoreciendo la articulación entre la academia, el Estado, los sectores productivos y la Sociedad civil.	**OE3.** Desarrollar una cultura nacional de ciberseguridad y sólidas capacidades operativas en el talento humano del sector público y la ciudadanía. **OE6.** Desarrollar capacidades nacionales de gestión de riesgos digitales e inteligencia en ciberseguridad en las entidades del estado y sectores estratégicos.	El PEDN orienta el ON3 al fortalecimiento de la competitividad mediante ciencia, tecnología, innovación y transformación digital. La ENC contribuye generando capacidades humanas especializadas, investigación e innovación en ciberseguridad y capacidades de analítica avanzada e inteligencia artificial, que permiten que los procesos de innovación y transformación digital se desarrollen en condiciones de mayor seguridad y resiliencia.
ON4. Garantizar una sociedad justa, democrática, pacífica y un Estado efectivo al servicio de las personas, en base al diálogo, la concertación nacional y el fortalecimiento de las instituciones. **OE 4.4.** Garantizar un adecuado funcionamiento de la institucionalidad política-jurídica-social en el país, mediante el uso intensivo de las tecnologías digitales y datos.	**OE6.** Desarrollar capacidades nacionales de gestión de riesgos digitales e inteligencia en ciberseguridad en las entidades del estado y sectores estratégicos	El PEDN incorpora expresamente la cyber-inteligencia como herramienta para reducir la victimización y fortalecer la seguridad ciudadana. La ENC desarrolla capacidades nacionales de inteligencia de amenazas, intercambio de información, análisis de riesgos y analítica avanzada, contribuyendo a fortalecer la generación de información para la prevención y toma de decisiones frente a amenazas en el entorno digital.
ON4. Garantizar una sociedad justa, democrática, pacífica y un Estado efectivo al servicio de las personas, en base al diálogo, la concertación nacional y el fortalecimiento de las instituciones. **OE 4.5.** Garantizar intervenciones públicas de calidad que respondan de manera oportuna a las necesidades y expectativas de las personas, tomando en cuenta la heterogeneidad territorial, social, económica, cultural e intergeneracional del país, con énfasis en el fortalecimiento de la	**OE1.** Fortalecer las capacidades nacionales de prevención, detección, respuesta y recuperación ante incidentes de seguridad digital en las entidades del ecosistema digital a nivel nacional. **OE5.** Fortalecer la gobernanza y el marco normativo en ciberseguridad en las entidades de la administración pública.	El PEDN impulsa un Estado efectivo mediante gobierno y transformación digital. La ENC incorpora la ciberseguridad como condición transversal para la continuidad, integridad y resiliencia de esta transformación, fortaleciendo la gobernanza, planificación, supervisión y capacidad de respuesta de las entidades públicas.

PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Gobierno y Transformación Digital de Política y Regulación
PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Gobierno y Transformación Digital de Tecnología y Seguridad
PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Gobierno y Transformación Digital de Servicios e Innovación
PRESIDENCIA DEL CONSEJO DE MINISTROS Secretaría de Gobierno y Transformación Digital

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

cultura de integridad y de lucha contra la corrupción, y la transformación digital.		

Fuente: *Elaboración propia, sobre la base de PEDN al 2050 y la ENC.*

2.3 Alineación con instrumentos internacionales

Marco de la Organización para la Cooperación y el Desarrollo Económicos - OCDE

En el marco del proceso de adhesión del Perú a la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el país viene recibiendo recomendaciones orientadas a fortalecer su marco de seguridad digital y la gestión del riesgo en el entorno digital.

Estas recomendaciones promueven un enfoque integral de la ciberseguridad, orientado a consolidar la confianza digital, fortalecer la resiliencia de los sistemas y proteger los activos digitales, en armonía con estándares internacionales.

En el marco del proceso de adhesión del Perú a la OCDE, la Estrategia incorpora los instrumentos vigentes del Comité de Política de Economía Digital (CDEP):

- Recomendación del Consejo sobre la Seguridad Digital de Actividades Críticas (OECD/LEGAL/0479, 2019), que orienta la protección de operadores de infraestructura crítica y sus cadenas de suministro[34].
- Recomendación del Consejo sobre las Directrices para la Política de Criptografía (OECD/LEGAL/0289)[35]
- Recomendación del Consejo sobre la Seguridad Digital de Productos y Servicios (OECD/LEGAL/0481, 2022)[36].
- Recomendación del Consejo sobre Tratamiento de Vulnerabilidades en Seguridad Digital (OECD/LEGAL/0482, 2022), que promueve programas de divulgación coordinada de vulnerabilidades (CVD) y de recompensa por errores[37].

Al respecto, corresponde desarrollar lo referido a la Recomendación del Consejo sobre Gestión de Riesgos de Seguridad Digital (OECD/LEGAL/0479) y a la Recomendación del Consejo sobre las Directrices para la Política de Criptografía (OECD/LEGAL/0289):

Recomendación del Consejo sobre Gestión de Riesgos de Seguridad Digital (OECD/LEGAL/0479)

La Recomendación del Consejo sobre Gestión de Riesgos de Seguridad Digital establece que los Estados deben adoptar un enfoque basado en principios que permitan integrar la seguridad digital en la toma de decisiones públicas y privadas.

---

34 Disponible en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479

35 Disponible en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289

36 Disponible en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481

37 Disponible en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Entre estos principios destacan la promoción de una cultura de seguridad digital mediante la concienciación y el desarrollo de capacidades; la responsabilidad compartida de los actores en la gestión del riesgo; el respeto de los derechos humanos y de los valores fundamentales; y la cooperación a nivel nacional e internacional. Este enfoque refleja que la seguridad digital no debe abordarse únicamente desde una dimensión técnica, sino también desde sus implicancias institucionales, económicas y sociales.

Asimismo, la OCDE plantea principios operativos dirigidos a los responsables de la toma de decisiones, orientados a incorporar la gestión del riesgo de seguridad digital en la estrategia organizacional, implementar procesos continuos de identificación, evaluación y tratamiento de riesgos, adoptar medidas de seguridad apropiadas y proporcionales, y fortalecer la preparación, respuesta, recuperación y continuidad frente a incidentes.

La Estrategia Nacional de Ciberseguridad se alinea con el enfoque promovido por la OCDE, en tanto incorpora principios orientadores, mecanismos de articulación institucional, fortalecimiento de capacidades y medidas dirigidas a la prevención, detección, respuesta, recuperación frente a incidentes de seguridad digital, contribuyendo así al fortalecimiento de la confianza en el entorno digital.

Figura 11. Principios de la Recomendación del Consejo sobre Gestión de Riesgos de Seguridad Digital (OECD/LEGAL/0479)



Fuente: *Elaboración propia con base en la Recomendación del Consejo sobre Gestión de Riesgos de Seguridad Digital (OECD/LEGAL/0479), OCDE. Elaborado con apoyo de herramientas de inteligencia artificial.*

Recomendación del Consejo sobre las Directrices para la Política de Criptografía (OECD/LEGAL/0289)

Esta recomendación reconoce que el uso de la criptografía es un componente esencial para asegurar la confidencialidad, integridad y disponibilidad de los datos, al proporcionar mecanismos irrefutables de autenticación y no repudio. Su incorporación en la ENC permitirá al país promover la aprobación de lineamientos técnicos, garantizando así un equilibrio que fortalezca la protección de la privacidad, los intereses económicos y la seguridad nacional, sin generar obstáculos injustificados al desarrollo de las redes y el comercio digital.

Conforme a lo expuesto, la ENC busca alinearse con los lineamientos establecidos por la OCDE, en tanto se configura como un instrumento técnico-estratégico orientado a articular actores, desarrollar capacidades, fortalecer la resiliencia digital y establecer un marco integral de actuación frente a los riesgos en el entorno digital, en concordancia con estándares internacionales y con una visión de implementación progresiva y coordinada.

La presente Estrategia considera otros documentos de referencia internacional, tales como:

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Ámbito de la Organización de Estados Americanos - OEA:

- Estrategia Interamericana Integral de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética (AG/RES. 2004 XXXIV-O/04)[38] y la Declaración "Fortalecimiento de la Cooperación en Ciberseguridad en las Américas"[39].

- Ambos instrumentos encomiendan a los Estados de la OEA crear CSIRT nacionales y participar en una red hemisférica de equipos de respuesta, lo cual se materializó en la red CSIRTAmericas gestionada por la Secretaría Ejecutiva del CICTE (de la cual el Perú forma parte)[40].

Ámbito de la Organización de las Naciones Unidas - ONU:

- Resoluciones de la Asamblea General de las Naciones Unidas sobre comportamiento responsable de los Estados en el ciberespacio (A/RES/70/237[41], A/RES/73/27[42], A/RES/75/240[43]).

- En conjunto, las resoluciones 70/237, 73/27 y 75/240 de la Asamblea General de la ONU constituyen la base que permite consolidar un marco común de normas voluntarias para un comportamiento responsable de los Estados en el ciberespacio, las cuales sirven de referencia para que países como el Perú adapten sus políticas y legislación en consonancia con estas normas voluntarias.

Ámbito de la Unión Internacional de Telecomunicaciones - ITU

- La Agenda Global de Ciberseguridad[44] y el Índice Global de Ciberseguridad (GCI)[45], este último, el principal instrumento de medición comparada del desarrollo nacional en la materia.

---

38 Disponible en: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Estrategia-seguridad-cibernetica-resolucion.pdf

39 Disponible en: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Declaracion%20del%20Fortalecimiento%20de%20la%20Seguridad%20en%20las%20Americas.pdf

40 Disponible en: https://csirtamericas.org/es

41 Disponible en: https://digitallibrary.un.org/record/815989/files/A_RES_70_237-EN.pdf

42 Disponible en: https://docs.un.org/en/a/res/73/27

43 Disponible en: https://docs.un.org/en/A/Res/75/240

44 Disponible en: https://www.itu.int/en/action/cybersecurity/pages/gca.aspx

45 Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

III. GOBERNANZA Y COORDINACIÓN NACIONAL DE LA CIBERSEGURIDAD

La gobernanza de la ciberseguridad en el Perú se organiza bajo un modelo que distribuye responsabilidades entre distintos niveles y roles del Estado.

En el nivel político-estratégico, el Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo constituye la máxima instancia de coordinación, articulación y supervisión entre el sector público, el sector privado, la academia, la sociedad civil y la ciudadanía. Este enfoque parte del reconocimiento de que la ciberseguridad no es únicamente un asunto tecnológico, sino que involucra dimensiones operativas, estratégicas y de seguridad nacional, por lo que requiere la participación coordinada de múltiples actores del Sistema Nacional de Transformación Digital[46].

En el ámbito rector e institucional, la Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital (SGTD), ejerce la rectoría del Sistema Nacional de Transformación Digital y, de manera específica, en materia de gobierno digital, confianza digital y seguridad digital. En tal condición, le corresponde formular políticas, estrategias, lineamientos y estándares técnicos orientados a fortalecer la seguridad digital, así como promover su implementación en las entidades públicas y la articulación con el sector privado y la comunidad internacional.

Esta rectoría se proyecta en el plano operativo a través del Centro Nacional de Seguridad Digital (CNSD), que constituye la plataforma y la instancia nacional encargada de gestionar, dirigir, coordinar y articular la respuesta frente a incidentes de seguridad digital. El CNSD actúa como el único punto de contacto oficial del Estado, concentrando capacidades de alerta, análisis, coordinación y gestión de incidentes, además de administrar el Registro Nacional de Incidentes de Seguridad Digital[47].

Como componente técnico-operativo del CNSD, el Equipo de Respuesta a Incidentes de Seguridad Digital Nacional (CSIRT Nacional) cumple funciones de monitoreo continuo, análisis de amenazas, alerta temprana, contención y respuesta ante incidentes de seguridad digital. Asimismo, brinda soporte especializado a los equipos institucionales y sectoriales, facilita el intercambio de información y promueve la adopción de buenas prácticas.

3.1. ¿Por qué una Estrategia Nacional de Ciberseguridad?

La formulación de una Estrategia Nacional de Ciberseguridad como instrumento estratégico responde a la necesidad de desarrollar, de manera sistemática y coordinada, las capacidades técnicas, operativas e institucionales requeridas para proteger el entorno digital nacional, en el marco de la Seguridad Digital establecido por el ordenamiento jurídico peruano. En ese sentido, busca promover la transición desde un enfoque predominantemente normativo y neutral frente a la tecnología hacia un modelo orientado al fortalecimiento efectivo de las capacidades operativas, técnicas e institucionales del país.

El Decreto Legislativo N.° 1412, Ley de Gobierno Digital, en su artículo 31, establece el Marco de Seguridad Digital del Estado Peruano como el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos orientados a preservar la

---

46 Artículo 10 del Decreto de Urgencia N.° 006-2020 (Ley del Sistema Nacional de Transformación Digital) y el Artículo 8 (numeral 8.1) del Reglamento del Sistema Nacional de Transformación Digital aprobado por Decreto Supremo N.° 157-2021-PCM.

47 Numerales 7.1 y 7.2 del artículo 7 y en el numeral 8.2 del artículo 8 del Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital; así como en el artículo 20 del Reglamento del Decreto de Urgencia N.° 007-2020 aprobado por Decreto Supremo N.° 126-2025-PCM.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

confidencialidad, integridad y disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.

Asimismo, en articulación con el Decreto de Urgencia N.° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, la seguridad digital se consolida como un ámbito fundamental para generar y preservar la confianza en el entorno digital[48]. Este modelo integral comprende dimensiones normativas, institucionales, organizacionales y tecnológicas, cuyo desarrollo requiere instrumentos diferenciados que permitan abordar cada dimensión con el nivel de especialización correspondiente[49].

En ese marco, el Decreto Legislativo N.° 1412, Ley de Gobierno Digital, en su artículo 30, define la seguridad digital como el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Esta definición evidencia que la seguridad digital constituye un concepto de alcance sistémico, que integra dimensiones regulatorias, organizacionales y técnicas.

Por su parte, el Decreto de Urgencia N.° 007-2020 delimita expresamente la ciberseguridad como la capacidad tecnológica orientada a preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos, y protegerlos frente a amenazas y vulnerabilidades en el entorno digital, precisando que esta constituye la perspectiva técnica de la seguridad digital[50].

En consecuencia, el ordenamiento jurídico peruano establece una distinción funcional entre:

- Seguridad Digital, como marco integral que comprende dimensiones normativas, institucionales y organizacionales para la gestión de riesgos en el entorno digital; y
- Ciberseguridad, como el componente técnico y operativo orientado a preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos.

Esta diferenciación no solo es conceptual, sino también operativa.

El Reglamento del Decreto Legislativo N.° 1412, aprobado mediante Decreto Supremo N.° 029-2021-PCM, así como el Reglamento del Decreto de Urgencia N.° 007-2020, aprobado mediante Decreto Supremo N.° 126-2025-PCM, establecen obligaciones concretas vinculadas a la gestión técnica de la seguridad digital, tales como:

- la implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital (CSIRT)[51];
- la gestión y notificación oportuna de incidentes de seguridad digital[52];

---

48 Artículo 4, numeral 4.2, literal c) del Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

49 Artículo 31 del Decreto Legislativo N.° 1412, Ley de Gobierno Digital.

50 Artículo 3, literal h) del Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

51 Artículo 104, numeral 104.2 del Reglamento de la Ley de Gobierno Digital, aprobado por Decreto Supremo N.° 029-2021-PCM.

52 Artículo 32 y 34 del Reglamento del Marco de Confianza Digital, aprobado por Decreto Supremo N.° 126-2025-PCM.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

- la protección y resiliencia de las actividades críticas y de los Activos Críticos Nacionales (ACN) [53];
- el fortalecimiento de capacidades técnicas especializadas en las entidades públicas[54].

La implementación efectiva de estas obligaciones requiere capacidades operativas avanzadas, incluyendo mecanismos de detección temprana de amenazas, monitoreo continuo, análisis de vulnerabilidades, respuesta coordinada ante incidentes de seguridad digital y recuperación de servicios digitales. Asimismo, exige la adopción de estándares técnicos internacionales (ISO 27001, NIST CSF, CIS Controls, GSMA NESAS, GSMA MCKB, 3GPP SCAS, etc.) y el fomento continuo del talento digital especializado.

El desarrollo de dichas capacidades no puede lograrse únicamente mediante disposiciones normativas generales. Por su naturaleza técnica, dinámica y altamente especializada, la ciberseguridad requiere un instrumento estratégico específico que permita definir prioridades nacionales, objetivos operativos, estándares técnicos, mecanismos de articulación institucional y líneas de acción.

En este contexto, la Estrategia Nacional de Ciberseguridad constituye el instrumento técnico-estratégico idóneo para operativizar el componente tecnológico del marco de Seguridad Digital, estableciendo acciones para el desarrollo progresivo de capacidades de prevención, detección, respuesta y recuperación frente a riesgos e incidentes en el entorno digital.

Asimismo, la formulación de este instrumento se encuentra habilitada por el marco institucional vigente. El Decreto Legislativo N.° 1412, Ley de Gobierno Digital, junto con el Decreto de Urgencia N.° 006-2020, que crea el Sistema Nacional de Transformación Digital, y el Decreto de Urgencia N.° 007-2020, atribuyen a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, la rectoría nacional en materia de gobierno digital, confianza digital y seguridad digital, incluyendo la formulación de políticas, estrategias, lineamientos y demás instrumentos necesarios para su implementación.

De este modo, la Estrategia Nacional de Ciberseguridad constituye un instrumento jurídicamente habilitado, institucionalmente coherente y estratégicamente necesario para desarrollar las capacidades tecnológicas nacionales requeridas para la protección de las redes, activos y sistemas informáticos, en concordancia con el modelo institucional del Sistema Nacional de Transformación Digital.

Asimismo, la Estrategia adopta un enfoque de capacidad de respuesta nacional en ciberseguridad, orientado a fortalecer la capacidad del Estado, los operadores de servicios esenciales y las entidades para anticipar, responder, recuperarse frente a incidentes y amenazas, garantizando la continuidad operativa y la prestación de servicios para la ciudadanía.

La implementación de la Estrategia promoverá mecanismos permanentes de colaboración entre el Estado, el sector privado, la academia y la sociedad civil o comunidad técnica, fomentando el intercambio de información sobre amenazas, el desarrollo de capacidades, la gestión coordinada de incidentes y el fortalecimiento de la resiliencia del ecosistema digital nacional.

---

53 Artículos 8, 13 y 30 (numeral 30.4) del Reglamento del Marco de Confianza Digital, aprobado por Decreto Supremo N.° 126-2025-PCM.

54 Artículo 112, numeral 112.1 del Reglamento de la Ley de Gobierno Digital, aprobado por Decreto Supremo N.° 029-2021-PCM y el artículo 21, literal h) del Reglamento del Marco de Confianza Digital, aprobado por Decreto Supremo N.° 126-2025-PCM.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

3.2. Gobernanza institucional en el sector público

En cada entidad pública, la ciberseguridad se integra al funcionamiento institucional mediante estructuras de gobernanza que permiten planificar, ejecutar y supervisar las medidas de ciberseguridad, así como gestionar los riesgos asociados al uso de tecnologías digitales.

El Comité de Gobierno y Transformación Digital cumple el rol de definir la orientación estratégica en materia de transformación y seguridad digital, aprobar políticas institucionales, asignar recursos y supervisar la gestión de riesgos y el cumplimiento de los objetivos establecidos.

En este esquema, el Líder de Gobierno y Transformación Digital actúa como el articulador principal y nexo estratégico. Este rol, que recae en un funcionario o asesor de la Alta Dirección o en un director de un órgano de línea[55], es el responsable de articular la implementación operativa de las iniciativas y proyectos priorizados por el Comité con los dueños de procesos y las diferentes unidades de organización de la entidad[56].

Específicamente, el Líder tiene como acción prioritaria gestionar la asignación de recursos destinados al fortalecimiento de las capacidades del personal en materia de seguridad digital, interoperabilidad, firma digital y gestión de datos[57]; además, es el encargado de comunicar los objetivos, medidas y avances institucionales al Líder Nacional de Gobierno y Transformación Digital (la Secretaría de Gobierno y Transformación Digital)[58].

Por su parte, el Oficial de Seguridad y Confianza Digital (OSCD) lidera la implementación operativa de las medidas de seguridad digital dentro de la entidad, gestionando riesgos y vulnerabilidades, coordinando acciones preventivas y asegurando el reporte oportuno de incidentes al CNSD, conforme a los lineamientos nacionales. El Oficial de Seguridad y Confianza Digital (OSCD) desempeña un rol estratégico para la gestión digital en la entidad pública y ejerce sus funciones con autonomía técnica reportando a la máxima autoridad administrativa y al Comité de Gobierno y Transformación Digital del cual es miembro. También, coordina con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en todas las cuestiones relativas a la implementación de controles de seguridad de la información relacionados con las materias de gestión de datos y protección de datos personales en la entidad, respectivamente.

El rol recae en un funcionario o servidor civil de la entidad pública que cuente con el conocimiento, experiencia profesional y formación especializada para coordinar la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad pública, en el marco de lo dispuesto por la Directiva N.° 001-2023-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital o norma que la sustituya[59].

---

55 Artículo 9 del Decreto de Urgencia N.° 006-2020.

56 Artículo 14.2. del Reglamento del Decreto de Urgencia N.° 006-2020.

57 "Lineamientos del Líder de Gobierno Digital" aprobado por Resolución de Secretaría de Gobierno Digital N.° 004-2018-PCM-SEGDI del 10 de diciembre de 2018.

58 Artículo 9 del Decreto de Urgencia N.° 006-2020.

59 Disponible en: https://www.gob.pe/institucion/pcm/normas-legales/4616729-001-2023-pcm-sgtd

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Complementariamente, los Equipos de Respuesta ante Incidentes (CSIRT institucionales) constituyen la capacidad técnica especializada encargada de detectar, analizar, contener y remediar incidentes de seguridad digital que afecten los sistemas y redes institucionales[60].

Cuando la magnitud o el impacto del incidente supera la capacidad de respuesta de la entidad, estos equipos coordinan con el CNSD para una atención articulada. Su actuación resulta esencial para preservar la continuidad operativa y restablecer los servicios.

3.3 Corresponsabilidad del sector privado y proveedores de actividades críticas

En la estructura de gobernanza en materia de ciberseguridad, el ámbito de responsabilidad puede trascender el ámbito estatal.

En este contexto, los proveedores de servicios digitales (PSD) y los proveedores de actividades críticas desempeñan un papel fundamental debido a su impacto en la economía, la prestación de servicios esenciales y la vida cotidiana de la población[61].

Entre los sectores prioritarios se encuentran, entre otros, el financiero, salud, energía eléctrica, agua y gas, transporte, telecomunicaciones y servicios educativos, cuya interrupción podría generar impactos significativos en la seguridad, el bienestar o la estabilidad del país[62].

Estas organizaciones deben gestionar de manera proactiva sus riesgos, implementar controles técnicos y organizativos adecuados, asegurar la continuidad de sus operaciones y notificar al CNSD los incidentes de seguridad digital que puedan comprometer sus servicios, infraestructuras o los datos bajo su responsabilidad[63].

---

60 Artículo 28 (literales a y c) y numeral 35.1 del artículo 35 del Reglamento del Decreto de Urgencia N.° 007-2020 aprobado por Decreto Supremo N.° 126-2025-PCM. Asimismo, el artículo 105 (literal e) del Reglamento de la Ley de Gobierno Digital, aprobado por Decreto Supremo N.° 029-2021-PCM.

61 Artículo 3 (literales d y j) del Decreto de Urgencia N.° 007-2020, Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital.

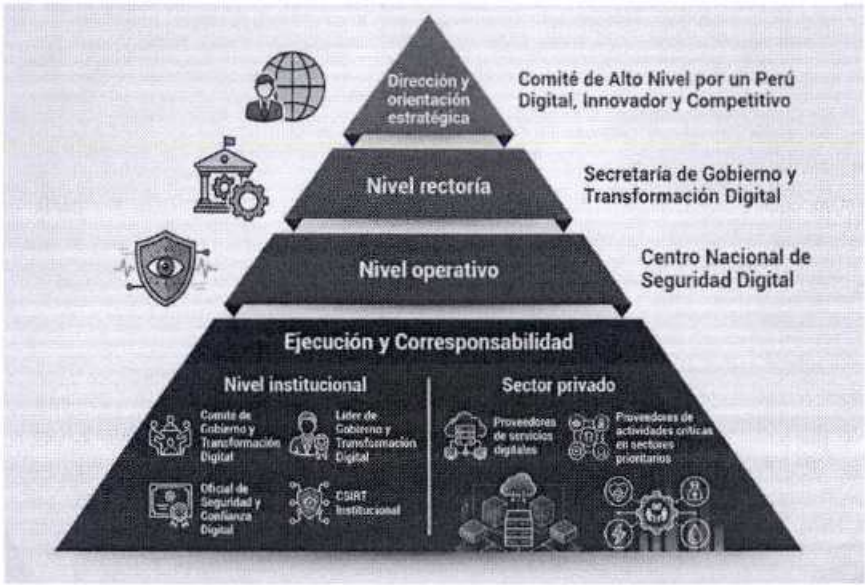
62 Artículo 9 (numeral 9.1) y Artículo 4, numeral 4.2 (literal a) del Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital.

63 Artículo 9 (numeral 9.1, literales a, b y c) del Decreto de Urgencia N.° 007-2020, Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital. Asimismo, el artículo 8 (numeral 8.3) y en el artículo 1 (numeral 1.2) del Reglamento del Decreto de Urgencia N.° 007-2020 aprobado por Decreto Supremo N.° 126-2025-PCM.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Figura 12. Actores de la Estrategia Nacional de Ciberseguridad



Fuente: *Elaboración propia con base en el marco de gobernanza y coordinación nacional de la ciberseguridad. Elaborado con apoyo de herramientas de inteligencia artificial.*

IV. NECESIDAD ESTRATÉGICA Y PROYECCIÓN HACIA OBJETIVOS

El Perú ha consolidado, durante los últimos años, importantes avances normativos e institucionales en materia de gobierno digital, confianza y ciberseguridad. No obstante, el principal desafío actual consiste en transformar ese marco regulatorio en capacidades operativas efectivas, sostenibles y homogéneas a nivel nacional, considerando las brechas existentes entre los distintos niveles de gobierno y sectores.

En este contexto, la siguiente etapa de desarrollo debe orientarse a asegurar la implementación efectiva, articulada y medible de las políticas, normas y mecanismos existentes, mediante el fortalecimiento de capacidades institucionales, la reducción de brechas técnicas y territoriales, y la consolidación de capacidades operativas que permitan gestionar los riesgos digitales de manera continua y resiliente.

Este tránsito desde una fase de construcción normativa hacia una etapa de madurez operativa constituye el eje central de la Estrategia Nacional de Ciberseguridad, cuyos objetivos y acciones estratégicas buscan consolidar un ecosistema digital seguro, resiliente, confiable e integrado en todo el territorio nacional.

Para el diseño e implementación de los objetivos y acciones estratégicas de la Estrategia, resulta necesario priorizar los siguientes ámbitos de intervención:

1. Fortalecer el desarrollo de talento especializado mediante programas de formación, certificación y especialización en ciberseguridad.
2. Robustecer las capacidades tecnológicas y operativas para la prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital.
3. Incrementar la realización de ejercicios, simulaciones y pruebas de ciberseguridad que permitan evaluar y mejorar la preparación nacional.
4. Fortalecer la protección y resiliencia de las infraestructuras, servicios y capacidades críticas que sustentan el funcionamiento del país.
5. Reducir las brechas territoriales e institucionales en materia de ciberseguridad, promoviendo capacidades descentralizadas y sostenibles.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

6. Intensificar la cooperación público-privada, académica e internacional para el intercambio de información, conocimientos y buenas prácticas.
7. Consolidar una cultura nacional de ciberseguridad que promueva la gestión responsable de los riesgos digitales en todos los sectores de la sociedad.

4.1. Situación futura deseada

Al 2030, el Perú habrá fortalecido progresivamente sus capacidades nacionales de ciberseguridad, avanzando hacia un entorno digital más seguro, resiliente y confiable para el desarrollo de las actividades del Estado, el sector privado y la ciudadanía.

Este avance se sustentará en el fortalecimiento de capacidades tecnológicas, operativas e institucionales para la prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital, así como en una mayor incorporación de prácticas de gestión de riesgos y de una cultura de ciberseguridad en los distintos actores del ecosistema digital.

Asimismo, se espera consolidar mecanismos de coordinación y cooperación entre entidades públicas, sector privado, academia y socios internacionales, promoviendo el intercambio de información, el desarrollo de capacidades especializadas y la adopción de buenas prácticas en materia de ciberseguridad.

Bajo un enfoque territorial, orientado a la reducción de brechas y al fortalecimiento gradual de capacidades en los gobiernos regionales y locales, el país buscará mejorar sus niveles de preparación y resiliencia frente a las amenazas digitales, contribuyendo al fortalecimiento de la confianza digital y a la continuidad de los servicios y actividades esenciales para la sociedad.

4.2. Alcance

La Estrategia Nacional de Ciberseguridad es de aplicación obligatoria para:

a) Las entidades de la Administración Pública establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N.° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N.° 006-2026-JUS, con excepción de las personas jurídicas señaladas en el numeral 8 del citado artículo.
b) Las empresas públicas de los gobiernos regionales y locales, y aquellas que se encuentran en el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE).
c) Los sujetos públicos o privados que, conforme a la normativa vigente sobre confianza digital, seguridad digital y activos críticos nacionales, se encuentren obligados al cumplimiento de disposiciones vinculadas a dichas materias.

Las organizaciones del sector privado que no se encuentren comprendidas en las obligaciones previstas en la normativa vigente pueden tomar como referencia lo establecido en la presente Resolución Ministerial y en la Estrategia Nacional de Ciberseguridad 2026-2030 en aquello que resulte compatible con la naturaleza de sus actividades, riesgos y obligaciones aplicables.

4.3 Principios orientadores

- **Liderazgo y responsabilidad compartida**
  La ciberseguridad constituye una responsabilidad compartida entre el Estado, el sector privado, la academia, la sociedad civil y la ciudadanía. En este marco, el Estado ejerce un liderazgo estratégico para promover políticas, estándares y mecanismos de coordinación que fortalezcan la protección del entorno digital nacional, fomentando la articulación y participación activa de todos los actores en la prevención, detección y respuesta frente a riesgos e incidentes de seguridad digital.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

- **Garantía de derechos en el entorno digital**
  El diseño, implementación y mantenimiento de medidas y controles de seguridad digital deben desarrollarse respetando y protegiendo los derechos fundamentales de las personas en el entorno digital. En particular, las medidas de seguridad deben salvaguardar la privacidad, la protección de datos personales, la libertad de expresión, el acceso a la información y otros derechos vinculados al uso de tecnologías digitales, contribuyendo al fortalecimiento de la confianza digital y al desarrollo de un entorno seguro y respetuoso de los derechos.

- **Resiliencia y continuidad frente a incidentes de seguridad digital**
  El país debe fortalecer su capacidad para prevenir, detectar, resistir, responder y recuperarse de incidentes de seguridad digital que puedan afectar las actividades críticas, las cadenas de suministro, los activos de información y los datos como activos estratégicos del Estado y del sector privado, así como la estabilidad económica y social.

  Para ello, se promueve el desarrollo de capacidades de gestión de riesgos de seguridad digital, monitoreo permanente, continuidad operativa, respuesta coordinada y recuperación ante incidentes de seguridad digital, con el fin de asegurar la disponibilidad, integridad y confidencialidad de la información, los sistemas y los servicios digitales.

- **Enfoque basado en la gestión de riesgos**
  Las medidas y controles de ciberseguridad deben sustentarse en un enfoque sistemático de gestión de riesgos que permita identificar, analizar, valorar, tratar y monitorear los riesgos que puedan afectar los activos de información, los datos como activos estratégicos, los sistemas y los servicios digitales.

  Este enfoque promueve la adopción de medidas preventivas, así como la implementación de herramientas como evaluaciones de impacto, auditorías de seguridad y mecanismos continuos de gestión de riesgos que fortalezcan la resiliencia en el entorno digital.

- **Protección de datos personales y seguridad de la información**
  La protección de datos personales y la seguridad digital constituyen ámbitos esenciales para el fortalecimiento de la confianza digital y la protección de los derechos de las personas.

  En ese sentido, las políticas y medidas de ciberseguridad deben garantizar que el tratamiento de datos personales se realice conforme al marco normativo vigente, respetando los principios y obligaciones establecidos en la legislación sobre protección de datos personales, a fin de salvaguardar la privacidad y los derechos de las personas en el entorno digital.

- **Cooperación público-privada, multisectorial e internacional**

  La seguridad del ecosistema digital requiere cooperación efectiva entre el Estado, el sector privado, la academia, la sociedad civil, la comunidad técnica y los socios internacionales.

  Se promoverán mecanismos de colaboración, intercambio seguro de información, desarrollo conjunto de capacidades, notificación de incidentes y respuesta operativa articulada.

  Asimismo, se impulsará la cooperación internacional para enfrentar el carácter transnacional de los riesgos e incidentes de seguridad digital, mediante el intercambio de información, buenas prácticas y asistencia técnica.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

V. DIAGNÓSTICO Y MARCO ESTRATÉGICO

5.1 Problema público

El entorno digital se ha consolidado como un espacio común global de alta relevancia estratégica para el desarrollo económico, social e institucional del país. La acelerada digitalización de servicios públicos, actividades críticas, procesos productivos y sistemas de información ha ampliado exponencialmente la superficie de exposición frente a amenazas de seguridad digital cada vez más sofisticadas.

El Perú ha logrado avances importantes en ciberseguridad mediante la consolidación de un marco normativo robusto (como la Ley de Gobierno Digital, el Marco de Confianza Digital, entre otros) y del sistema institucional articulado bajo la rectoría de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital y con el Centro Nacional de Seguridad Digital (CNSD) como plataforma operativa.

Sin embargo, el principal desafío estructural del país no radica en la ausencia de normas, sino en la brecha significativa entre el desarrollo normativo y su implementación efectiva. En particular, subsisten desafíos relacionados con el fortalecimiento de capacidades técnicas, operativas e institucionales que permitan materializar los avances normativos alcanzados.

En términos prácticos, el país cuenta con un marco normativo, una institucionalidad rectora y estructuras organizacionales definidas; no obstante, aún requiere consolidar capacidades técnicas para prevenir, detectar, responder y recuperarse de manera eficaz frente a incidentes de ciberseguridad.

En este contexto, el Perú se encuentra en una etapa de consolidación intermedia de la ciberseguridad, predominantemente formativa, caracterizada por avances en materia de gobernanza, marco legal, organización institucional, capacitación y cooperación. Sin perjuicio de ello, persisten limitaciones en las capacidades técnicas, operativas y de resiliencia, cuya atención resulta indispensable para alcanzar niveles más avanzados de madurez.

Tabla 3. Principales hallazgos sobre ciberseguridad en el Perú

Instrumento	Hallazgo	Observaciones
Reporte de Ciberseguridad 2025 (BID-OEA)	Predominantemente Estadio 2 – Formativo	Con algunos indicadores en Estadio 3 – Establecido, como conciencia de riesgos, legislación de protección de datos y reporte/compartición de vulnerabilidades.
Índice Global de Ciberseguridad 2024	T3 – Establishing	La principal brecha en el pilar de Medidas Técnicas, donde obtiene su calificación más baja (13.51/20)
Centro Nacional de Seguridad Digital - CNSD	Principal línea de intervención es la capacitación ciudadana	
	Baja frecuencia en ejercicios de simulación	
Indicadores de Transformación Digital, "Reporte de avances en gobierno y transformación digital"	89.47% de los ministerios implementó un Equipo de Respuesta ante Incidentes de Seguridad Digital	65.38% de los gobiernos regionales implementó con un Equipo de Respuesta ante Incidentes de Seguridad Digital
	100% de los ministerios implementó el Sistema de Gestión de Seguridad de la Información.	26.92% de los gobiernos regionales implementó el Sistema de Gestión de Seguridad de la Información.

Fuente: *Elaboración propia con base en información del BID-OEA, UIT, CNSD e Indicadores de Transformación Digital.*

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

La principal tensión se presenta entre los avances alcanzados en materia normativa e institucional y las limitaciones existentes en las capacidades técnicas y operativas del país. Esta situación se refleja en una limitada realización de ejercicios de simulación, debilidades en la gestión sistemática de vulnerabilidades y niveles de madurez heterogéneos entre las entidades públicas.

En ese contexto, el problema público puede definirse como la insuficiente madurez técnico-operativa, tecnológica y de infraestructura del ecosistema nacional de ciberseguridad, lo que dificulta la implementación efectiva de los avances normativos alcanzados. Esta situación incrementa la exposición del país frente a amenazas digitales y compromete la protección de los activos críticos nacionales, las actividades críticas y la continuidad de los servicios públicos esenciales.

Frente a ello, resulta necesario que el Estado impulse una transición desde un enfoque predominantemente formativo y reactivo hacia un modelo integral de resiliencia en ciberseguridad, basado en el fortalecimiento de las capacidades de detección temprana, la respuesta coordinada ante incidentes, la formación de talento humano especializado, el desarrollo de infraestructura tecnológica y la mejora continua de las capacidades nacionales.

Brechas identificadas

- **Brecha en capacidad de respuesta operativa**

  La capacidad operativa para gestionar incidentes de manera coordinada presenta niveles heterogéneos. Las asimetrías de despliegue antes mencionadas son evidentes: mientras el 89.47 % de los ministerios cuenta con un Equipo de Respuesta ante Incidentes de Seguridad Digital implementado, esta cifra desciende al 65.38 % en los gobiernos regionales.

  Asimismo, se constata una baja frecuencia de ejercicios de simulación, con la realización de un solo simulacro anual, como el Simulacro de Ataques Cibernéticos efectuado en julio de 2025.

  Este escenario revela una clara oportunidad de mejora para fortalecer la preparación operativa y la resiliencia institucional frente a escenarios de crisis.

- **Brecha en infraestructura tecnológica**

  Persisten limitaciones significativas en la disponibilidad y modernización de infraestructura tecnológica y de resiliencia técnica, lo cual ha sido identificado por la propia Secretaría de Gobierno y Transformación Digital (SGTD) como una limitante directa para detectar, prevenir y mitigar amenazas de manera eficaz.

  Esta situación es respaldada por el Índice Global de Ciberseguridad 2024, donde la principal brecha estructural se observa en el pilar de Medidas Técnicas (13.51/20, el puntaje más bajo del país), evidenciando falencias en la implementación de controles técnicos y de respuesta.

- **Brecha en la protección de activos críticos nacionales y actividades críticas**

  La creciente dependencia de los sistemas digitales y la interconexión de infraestructuras han ampliado exponencialmente la superficie de exposición a ataques en los sectores estratégicos del país. De acuerdo con el análisis del Foro Económico Mundial (WEF

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

2024)[64], los ciberataques dirigidos contra las infraestructuras críticas representan uno de los riesgos globales con probabilidad de desencadenar una crisis a nivel nacional. Ante este escenario, resulta indispensable fortalecer la protección de los pilares tecnológicos y operativos que sostienen al país. Para ello, el Estado Peruano reconoce jurídicamente la necesidad de blindar estos sectores a través de dos dimensiones regulatorias especializadas y complementarias:

- **Las Actividades Críticas y Servicios Públicos Esenciales:** Comprenden aquellas actividades económicas o sociales (como el sector financiero, salud, energía y telecomunicaciones) cuya interrupción genera graves consecuencias en la salud, la seguridad ciudadana y la prosperidad económica del país. Su protección se rige bajo el Marco de Confianza Digital, con la rectoría de la Secretaría de Gobierno y Transformación Digital (SGTD) de la PCM.

- **Los Activos Críticos Nacionales (ACN):** Comprenden los recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales, o que están destinados a cumplir dicho fin. Su identificación, evaluación, y gestión de riesgos se rigen por el marco de la Seguridad y Defensa Nacional. Resulta ineludible fortalecer la protección de los activos críticos nacionales y actividades críticas que sostienen al país, en tanto su afectación puede comprometer gravemente la continuidad de los servicios públicos esenciales y la estabilidad económica nacional.

- **Brecha en talento especializado**

El talento humano especializado en ciberseguridad constituye un activo estratégico para la resiliencia digital del Estado, cuya disponibilidad, desarrollo y retención son esenciales para garantizar la continuidad de los servicios digitales, la protección de la información y la respuesta eficaz frente a amenazas cibernéticas.

Desde una perspectiva técnica y de gestión de riesgos los estándares internacionales como el ISO/IEC 27001:2022, ISO/IEC 27002:2022, NIST CSF 2.0 y NIST NICE; reconocen que las personas, sus competencias y los roles especializados son componentes esenciales para el éxito de la Estrategia Nacional de Ciberseguridad.

Existe necesidad de invertir en la formación de profesionales especializados en ciberseguridad. Las evaluaciones internacionales reflejan que, si bien existen avances, las medidas de desarrollo de capacidades aún resultan insuficientes para que el país alcance un nivel de madurez consolidado, obteniendo 15.16 sobre 20 en este pilar en el Índice Global de Ciberseguridad 2024.

Asimismo, en el Reporte de Ciberseguridad 2025, se aprecia que respecto de los indicadores "Educación en ciberseguridad", "Formación profesional en ciberseguridad" e "Investigación e innovación en ciberseguridad" de la dimensión 3 denominada "Desarrollando conocimientos y capacidades en ciberseguridad", Perú ha logrado un nivel de madurez 2, es decir, se encuentra aún en un nivel formativo.

Esta limitación en lo referido al talento especializado restringe la consolidación de capacidades técnicas y dificulta la implementación efectiva de los marcos normativos,

64 Foro Económico Mundial (2024). *The Global Risks Report 2024*. Disponible en: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

convirtiendo en un asunto muy relevante las capacidades del talento humano para prevenir, detectar y responder a incidentes de manera oportuna y eficaz.

- **Brecha en cultura de ciberseguridad**

  Las cifras consolidadas del Centro Nacional de Seguridad Digital, correspondientes al periodo 2024 a enero de 2026, muestran que la capacitación ciudadana constituye la principal línea de intervención, con 20,150 acciones, equivalentes al 74.9 % del total de acciones registradas.

  Esta priorización evidencia una orientación institucional hacia el fortalecimiento preventivo de la cultura de ciberseguridad y la reducción de riesgos asociados al factor humano. Sin embargo, el volumen de capacitaciones no garantiza, por sí solo, la adopción efectiva y sostenida de buenas prácticas.

  Por ello, persiste el desafío de avanzar desde la sensibilización hacia el desarrollo verificable de capacidades, hábitos seguros y competencias especializadas que fortalezcan integralmente el ecosistema nacional de ciberseguridad.

5.2 Objetivos y acciones estratégicas

La Estrategia Nacional de Ciberseguridad se estructura sobre la base de 6 (seis) objetivos estratégicos principales:

OBJETIVO ESTRATÉGICO N.° 1:

FORTALECER LAS CAPACIDADES NACIONALES DE PREVENCIÓN, DETECCIÓN, RESPUESTA Y RECUPERACIÓN ANTE INCIDENTES DE SEGURIDAD DIGITAL EN LAS ENTIDADES DEL ECOSISTEMA DIGITAL A NIVEL NACIONAL

El objetivo estratégico se orienta a fortalecer las capacidades nacionales de prevención, detección, respuesta y recuperación ante incidentes de seguridad digital, mediante el desarrollo de una arquitectura operativa integrada que articula capacidades de gobernanza, operación tecnología e intercambio de información, bajo la coordinación del Centro Nacional de Seguridad Digital, a efectos de garantizar una respuesta coordinada y oportuna.

ACCIONES ESTRATÉGICAS:

<u>Acción estratégica 1.1</u>: Consolidar una arquitectura nacional de ciberseguridad basada en un modelo SOC de SOCs e iSOC para redes OT (Redes Industriales), articulando entidades públicas, sectores estratégicos y el Centro Nacional de Seguridad Digital.

La finalidad de esta acción es integrar los Centros de Operaciones de Seguridad (SOC) sectoriales en un modelo integrado de monitoreo coordinado, bajo el liderazgo del Centro Nacional de Seguridad Digital, que permita la correlación de eventos y el intercambio de información en tiempo real en el Estado.

Esta integración tiene como propósito superar la fragmentación de la información y la limitada visibilidad de las amenazas identificadas, fortaleciendo la capacidad de detección temprana y respuesta coordinada frente a incidentes de seguridad digital.

Responsables:
Secretaría de Gobierno y Transformación Digital – PCM.
Centro Nacional de Seguridad Digital.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Corresponsables:
Entidades públicas.
Operadores de actividades críticas y operadores de servicios esenciales.

Indicador:
Número de entidades públicas priorizadas integradas al sistema de monitoreo del Centro Nacional de Seguridad Digital.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de entidades públicas priorizadas[65] conforme a criterios de criticidad definidos por el ente rector en materia de seguridad digital.

En segundo lugar, se contabilizan aquellas entidades que se encuentran integradas operativamente al sistema de monitoreo del Centro Nacional de Seguridad Digital, entendiéndose como tal la conexión activa y el intercambio continuo de información de seguridad, incluyendo el envío de registros de eventos y el reporte de incidentes, conforme a protocolos y estándares definidos.

Finalmente, el valor del indicador corresponde al número de entidades públicas priorizadas que se encuentran integradas operativamente al sistema de monitoreo del Centro Nacional de Seguridad Digital.

Logro esperado:
2026: 0 (Período de preparación)
2027: 5
2028: 15
2029: 20
2030: 50

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Número de entidades

<u>Acción estratégica 1.2</u>: Fortalecer el Centro Nacional de Seguridad Digital (CNSD) como nodo central de monitoreo, coordinación y respuesta nacional.

Esta acción tiene por finalidad consolidar al Centro Nacional de Seguridad Digital como nodo operativo nacional mediante la implementación de un modelo de operación continua (24/7), estructurado en niveles, con cobertura progresiva de entidades públicas y proveedores de actividades críticas. Su implementación comprende el despliegue de infraestructura tecnológica de monitoreo, estandarización de procedimientos de gestión de incidentes de seguridad digital y fortalecimiento de capacidades humanas especializadas.

Responsables:
Secretaría de Gobierno y Transformación Digital – PCM.
Centro Nacional de Seguridad Digital.

---

[65] Los criterios de priorización serán determinados por la SGTD-CNSD.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Corresponsables:
Entidades públicas.

Indicador:
Porcentaje de incidentes de seguridad digital gestionados por el Centro Nacional de Seguridad Digital dentro del plazo/protocolo definido.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El cálculo del indicador se realiza a partir del total de incidentes de seguridad digital que han sido reportados al Centro Nacional de Seguridad Digital (CNSD) durante el periodo de medición.

Sobre este conjunto, se identifican aquellos incidentes que han sido atendidos o gestionados por el CNSD dentro del plazo/protocolo definido, entendiéndose como tales los que cuentan con intervención del CNSD, aplicación del protocolo de gestión de incidentes, coordinación con la(s) entidad(es) afectada(s), registro completo y trazable del proceso de gestión, y cierre formal del incidente.

El valor del indicador se obtiene relacionando ambos conjuntos y expresando el resultado en términos porcentuales, a fin de reflejar el nivel de atención o gestión efectiva de los incidentes por parte del CNSD en el periodo evaluado.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de incidentes de seguridad digital gestionados por el CNSD dentro del plazo/protocolo definido.
B = Número total de incidentes de seguridad digital reportados al Centro Nacional de Seguridad Digital (CNSD) durante el periodo de medición.

Logro esperado:
2026: 15%
2027: 25%
2028: 40%
2029: 55%
2030: 75%

Tipo de logro esperado: No acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje.

<u>Acción estratégica 1.3</u>: Implementar y consolidar los CSIRT institucionales, priorizando proveedores de actividades críticas y gobiernos subnacionales (regionales y locales).

La finalidad de esta acción es desarrollar y fortalecer capacidades técnicas y operativas de respuesta ante incidentes de seguridad digital en entidades públicas, especialmente en proveedores de actividades críticas, gobiernos regionales y locales, a fin de reducir las brechas de vulnerabilidad y la asimetría en capacidades tecnológicas, organizativas y humanas identificadas en el diagnóstico.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Su implementación comprende el despliegue progresivo de CSIRT institucionales, mediante asistencia técnica especializada, la estandarización de lineamientos y protocolos de gestión de incidentes de seguridad digital, y su integración operativa bajo la coordinación del Centro Nacional de Seguridad Digital.

Como resultado, se busca establecer capacidades descentralizadas de detección, análisis, respuesta y recuperación ante incidentes de seguridad digital, asegurando una respuesta oportuna, articulada y alineada con la gestión de incidentes de seguridad digital.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Entidades públicas

Corresponsables:
Gobiernos regionales
Gobiernos locales
Proveedores de actividades críticas

Indicador:
Porcentaje de entidades públicas priorizadas[66], incluyendo gobiernos regionales y locales, que cuentan con un CSIRT institucional operativo e integrado.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de entidades públicas priorizadas conforme a criterios definidos por el ente rector.

En segundo lugar, se contabilizan aquellas entidades que cuentan con un CSIRT institucional que cumple con tener una constitución formal mediante instrumento de gestión institucional; operatividad evidenciada por la capacidad de gestionar incidentes de seguridad digital conforme a protocolos definidos; e, integración, mediante su conexión e interoperabilidad incluyendo el intercambio de información, reporte de incidentes bajo la coordinación del Centro Nacional de Seguridad Digital.

Posteriormente, se divide el número de entidades que cumplen dichas condiciones entre el total de entidades priorizadas.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de entidades públicas priorizadas con un CSIRT institucional operativo e integrado.
B = Número total de entidades públicas priorizadas.

Logro esperado:
2026: 15%
2027: 35%
2028: 55%
2029: 75%
2030: 85%

[66] Los criterios de priorización serán determinados por la SGTD-CNSD.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje

Acción estratégica 1.4: Desarrollar e integrar una plataforma nacional de gestión de incidentes de seguridad digital.

Esta plataforma tiene el objetivo de permitir el registro, monitoreo, trazabilidad, coordinación y respuesta articulada frente a incidentes de seguridad digital, incorporando capacidades de automatización operativa (SOAR) e intercambio seguro de información a través de la plataforma nacional de gestión de incidentes de seguridad digital.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Centro Nacional de Seguridad Digital

Corresponsables:
Entidades públicas

Indicador:
Porcentaje de entidades públicas priorizadas[67] integradas a la plataforma nacional de gestión de incidentes de seguridad digital.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de entidades públicas priorizadas para su integración a la plataforma nacional de gestión de incidentes de seguridad digital, conforme a los criterios definidos por el ente rector en materia de seguridad digital.

En segundo lugar, se contabilizan aquellas entidades públicas que se encuentran integradas a la plataforma nacional de gestión de incidentes de seguridad digital.

Se considera que una entidad se encuentra integrada operativamente cuando cuenta con acceso habilitado, capacidad de registro y reporte de incidentes, intercambio de información conforme a los protocolos establecidos, y/o participación activa en los mecanismos de gestión y trazabilidad de incidentes definidos por el Centro Nacional de Seguridad Digital.

Posteriormente, se divide el número de entidades que cumplen dichas condiciones entre el total de entidades priorizadas.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de entidades públicas priorizadas integradas operativamente a la plataforma.
B = Número total de entidades públicas priorizadas para su integración a la plataforma.

[67] Los criterios de priorización serán determinados por la SGTD-CNSD.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Logro esperado:
2026: 0% (Período de preparación)
2027: 10%
2028: 15%
2029: 20%
2030: 30%

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje.

Acción estratégica 1.5: Institucionalizar simulacros nacionales de ciberseguridad y ejercicios de respuesta frente a incidentes de seguridad digital.

Su implementación se realizará a través de la programación periódica, obligatoria y multisectorial de ejercicios de ciberseguridad, incluyendo simulacros técnicos y pruebas controladas de detección y respuesta, bajo la coordinación del Centro Nacional de Seguridad Digital.

Estos ejercicios permitirán evaluar tiempos de detección, capacidad de coordinación interinstitucional, eficacia de los protocolos de respuesta y mecanismos de recuperación, así como identificar brechas operativas y oportunidades de mejora en seguridad digital.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Centro Nacional de Seguridad Digital

Corresponsables:
Entidades públicas

Indicador:
Porcentaje de entidades públicas participantes con ejercicios nacionales de ciberseguridad concluidos.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de entidades públicas convocadas a participar en simulacros y ejercicios nacionales de ciberseguridad durante el periodo de medición.

En segundo lugar, se contabilizan aquellas entidades que participan y completan el ejercicio, entendiéndose como tal la ejecución de las actividades previstas, incluyendo la activación de sus equipos de respuesta, la gestión del escenario simulado y la entrega de los resultados o reportes requeridos conforme a los lineamientos establecidos.

Posteriormente, se divide el número de entidades que cumplen dichas condiciones entre el total de entidades convocadas.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Donde:
A = Número de entidades públicas convocadas que participan y concluyen los ejercicios nacionales de ciberseguridad.
B = Número total de entidades públicas convocadas a participar en los ejercicios nacionales de ciberseguridad.

Logro esperado:
2026: 5%
2027: 30%
2028: 35%
2029: 40%
2030: 45%

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje.

OBJETIVO ESTRATÉGICO N.° 2
FORTALECER LA CIBERSEGURIDAD DE LOS ACTIVOS CRÍTICOS NACIONALES, LAS ACTIVIDADES CRÍTICAS Y LOS SERVICIOS PÚBLICOS ESENCIALES FRENTE A AMENAZAS DE SEGURIDAD DIGITAL

Este objetivo estratégico busca fortalecer la resiliencia y la ciberseguridad de los Activos Críticos Nacionales, las actividades críticas y los Servicios Públicos Esenciales mediante la gestión de riesgos de seguridad digital, la reducción de vulnerabilidades, la continuidad de operaciones, la detección temprana, la respuesta coordinada y la recuperación frente a incidentes, en cumplimiento de los principios de privacidad y los estándares internacionales aplicables. La protección se determina por la función crítica que dichos activos, actividades o servicios sostienen y por su contribución a la continuidad de las Capacidades Nacionales.

Su implementación se sustenta en un enfoque de gestión de riesgos que comprende la identificación, el análisis, la evaluación, el tratamiento y el monitoreo continuo de los riesgos, en función de la criticidad, la probabilidad de ocurrencia de amenazas y el impacto potencial sobre la continuidad de los Activos Críticos Nacionales, las actividades críticas y los Servicios Públicos Esenciales.
Para tal efecto, el objetivo se articula en 2 ámbitos complementarios de actuación:

a) La protección de las actividades críticas y los servicios públicos esenciales, conforme el marco de la confianza digital.
b) La protección de los activos críticos nacionales, en el marco del régimen especializado establecido por el Decreto Supremo N° 106-2017-PCM y demás disposiciones aplicables

Este objetivo se desarrolla bajo un modelo de gobernanza que involucra a las entidades competentes, los operadores respectivos, así como a las demás entidades con responsabilidades en materia de seguridad digital, lo cual implica y promueve la coordinación interinstitucional para la gestión basada en riesgos y el fortalecimiento progresivo de las capacidades nacionales de prevención, detección, contención, respuesta y recuperación frente a incidentes de seguridad digital.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

ACCIONES ESTRATÉGICAS:

Acción estratégica 2.1: Identificar, evaluar e incorporar Activos Críticos Nacionales al Inventario Nacional y fortalecer la evaluación de riesgos.

La finalidad de esta acción es asegurar la identificación, validación, incorporación al Inventario Nacional y evaluación de riesgos de los Activos Críticos Nacionales que sostienen las capacidades nacionales, mediante la aplicación del régimen especializado vigente, con la participación de la Dirección Nacional de Inteligencia en las funciones que el ordenamiento le asigna.

Su implementación comprende la identificación de los activos por los sectores responsables del Anexo 4 del Decreto Supremo N.º 106-2017-PCM en coordinación con sus operadores, la validación de las propuestas sectoriales por la Dirección Nacional de Inteligencia, la aprobación del Inventario Nacional por el Consejo de Seguridad y Defensa Nacional, y la ejecución de los servicios técnicos de la Dirección Nacional de Inteligencia para la evaluación de riesgos de seguridad digital.

Como resultado, se busca consolidar un Inventario Nacional actualizado y una cobertura progresiva de la evaluación de riesgos de seguridad digital sobre los Activos Críticos Nacionales inscritos.

Responsables:
Dirección Nacional de Inteligencia (DINI)

Corresponsables:
Operadores de Activos Críticos Nacionales.
Sectores responsables del Anexo 4 del Decreto Supremo N° 106-2017-PCM

Indicador:
Porcentaje del Inventario Nacional de Activos Críticos Nacionales con evaluación de riesgos de seguridad digital completada por la Dirección Nacional de Inteligencia.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula a partir del total de Activos Críticos Nacionales inscritos en el Inventario Nacional aprobado por el Consejo de Seguridad y Defensa Nacional.

En segundo lugar, se contabilizan los Activos Críticos Nacionales que cuentan con evaluación de riesgos completada por la Dirección Nacional de Inteligencia. Posteriormente, se divide el número de Activos Críticos Nacionales evaluados entre el total inscrito.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de Activos Críticos Nacionales con evaluación de riesgos de seguridad digital completada.
B = Número total de Activos Críticos Nacionales inscritos en el Inventario Nacional aprobado por el Consejo de Seguridad y Defensa Nacional.

Logro esperado:
2026: 6%

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

2027: 12%
2028: 18%
2029: 24%
2030: 30%

Tipo de logro esperado: Acumulado

Periodicidad: Anual.

Unidad de medida: Porcentaje

Acción estratégica 2.2: Identificar, clasificar, registrar y proteger las actividades críticas y los servicios públicos esenciales.

La finalidad de esta acción es consolidar y aprobar el inventario de actividades y funciones críticas, así como de los servicios públicos esenciales en el Marco de Confianza Digital, disponiendo la implementación de las medidas de protección en seguridad digital aplicables.

Dicho inventario permite clasificar las actividades y funciones críticas por niveles de criticidad, según su posible afectación sobre la salud, la seguridad ciudadana y la prosperidad económica y social. Asimismo, permite registrar la cadena de suministro digital asociada y priorizar la gestión de riesgos en materia de seguridad digital, entre otros determinados por el ente rector. El inventario se actualiza mediante resoluciones de la Secretaría de Gobierno y Transformación Digital.

Cuando una misma entidad ostente simultáneamente la condición de operador de Activos Críticos Nacionales, conforme al régimen especializado vigente, y la condición de prestador de Servicios Públicos Esenciales o de operador de actividades críticas, conforme al Marco de Confianza Digital, cada una de dichas condiciones se sujeta al régimen aplicable y a las autoridades competentes correspondientes.

Cuando una actividad crítica o un Servicio Público Esencial se encuentre simultáneamente bajo regulación sectorial específica, las obligaciones del Marco de Confianza Digital se articulan con dicha regulación bajo la coordinación del ente rector y el regulador sectorial competente, sin duplicación de obligaciones y en aplicación al principio de especialidad sectorial.

Responsables:
Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de ministros (SGTD-PCM)

Corresponsables:
Operadores de actividades críticas
Prestadores de servicios públicos esenciales
Centro Nacional de Seguridad Digital (CNSD)
Dirección Nacional de Inteligencia (DINI) en la vinculación con Activos Críticos Nacionales
Sectores responsables del Anexo 4 del Decreto Supremo N.° 106-2017-PCM en lo relativo a sus operadores
Organismos reguladores y supervisores competentes

Indicador:
Porcentaje de actividades críticas y servicios públicos esenciales registrados con vinculación documentada y con medidas de protección en seguridad digital implementadas conforme a los lineamientos del ente rector.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Sentido esperado del indicador: Ascendente.

Método de cálculo:
Se identifica el total de actividades críticas y servicios públicos esenciales comprendidos en el ámbito de aplicación conforme a los lineamientos del ente rector.

Se contabilizan los que cuentan con identificación formal, clasificación por nivel de criticidad y medidas de protección en seguridad digital implementadas conforme a los lineamientos técnicos aplicables.

El número de actividades y servicios que cumplen estas condiciones se divide entre el total considerado.

El resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de actividades críticas y servicios públicos esenciales con vinculación documentada y medidas de protección implementadas.
B = Número total de actividades críticas y servicios públicos esenciales comprendidos en el ámbito de aplicación.

Logro esperado:
2026: 5%
2027: 15%
2028: 30%
2029: 45%
2030: 60%

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje

<u>Acción estratégica 2.3</u>: Fortalecer medidas para la gestión de riesgos de seguridad digital respecto de operadores de activos críticos nacionales, así como de las actividades críticas y los servicios públicos esenciales.

La finalidad de esta acción es lograr la adopción de medidas mínimas de seguridad digital respecto de los operadores de Activos Críticos Nacionales, de las actividades críticas y los Servicios Públicos Esenciales, mediante la implementación progresiva de Sistemas de Gestión de Seguridad de la Información (SGSI) u otros modelos equivalentes, sustentados en un enfoque de gestión de riesgos. En los entornos de tecnología operativa, las medidas se enmarcan en la gestión de riesgos industriales, conforme a los estándares internacionales aplicables y al nivel de criticidad identificada por cada operador.

Como resultado, se busca fortalecer la capacidad para gestionar riesgos de seguridad digital de manera sistemática, reducir la exposición a incidentes de ciberseguridad y garantizar la continuidad de los servicios esenciales.

Responsables:
Secretaría de Gobierno y Transformación Digital – PCM
Dirección Nacional de Inteligencia - DINI, en el marco de sus competencias.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Corresponsables:
Operadores de Activos Críticos Nacionales.
Operadores de actividades críticas
Prestadores de Servicios Públicos Esenciales.

Indicador:
Porcentaje de operadores de Activos Críticos Nacionales, de actividades críticas y los Servicios Públicos Esenciales que cuentan con un Sistema de Gestión de Seguridad de la Información (SGSI) implementado y, en sus entornos de tecnología operativa, con la segmentación en zonas y conductos y los niveles de seguridad correspondientes a la gestión de riesgos industriales, conforme a los lineamientos técnicos aplicables.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de operadores de activos críticos nacionales, así como de las actividades críticas, sus operadores y los servicios públicos esenciales registrados por el ente rector.

En segundo lugar, se contabilizan los operadores de Activos Críticos Nacionales, de actividades críticas y los Servicios Públicos Esenciales que cuentan con un Sistema de Gestión de Seguridad de la Información implementado, auditado y conforme con los lineamientos, controles mínimos y estándares aplicables según la competencia de cada entidad. Para los Activos Críticos Nacionales, la evaluación atiende las disposiciones de la DINI, sin perjuicio de los lineamientos de seguridad digital y confianza digital que correspondan a la SGTD. En los entornos industriales o híbridos IT/OT, la evaluación considera además la gestión de riesgos sobre los sistemas de control industrial y las tecnologías operativas, con criterios de segmentación en zonas y conductos, asignación de niveles de seguridad, reducción de la exposición, continuidad operativa y mitigación de riesgos industriales, conforme a las referencias técnicas nacionales e internacionales aplicables.

Posteriormente, se divide el número de operadores de activos críticos nacionales, así como de las actividades críticas, sus operadores y los servicios públicos esenciales que cumplen dichas condiciones entre el total de operadores registrados.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de operadores de Activos Críticos Nacionales, actividades críticas y Servicios Públicos Esenciales que cumplen las condiciones establecidas en el indicador.
B = Número total de operadores de Activos Críticos Nacionales, actividades críticas y Servicios Públicos Esenciales registrados.

Logro esperado:
2026: 10%
2027: 30%
2028: 55%
2029: 60%
2030: 70%

Tipo de logro esperado: Acumulado.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Periodicidad: Anual.

Unidad de medida: Porcentaje

Acción estratégica 2.4: Implementar programas nacionales de gestión de vulnerabilidades, pruebas de intrusión y evaluación continua.

La finalidad de esta acción es identificar, evaluar y gestionar de manera anticipada las vulnerabilidades en los sistemas de las entidades públicas, de los operadores de Activos Críticos Nacionales y de los operadores de actividades críticas, a fin de reducir la exposición a incidentes de seguridad digital y fortalecer la resiliencia frente a amenazas en constante evolución. En el caso de los operadores de Activos Críticos Nacionales, la gestión de vulnerabilidades y las pruebas de intrusión en sus entornos operativos se conducen conforme a su régimen especializado.

Su implementación comprende el diseño y ejecución de programas nacionales de gestión de vulnerabilidades, que incluyan escaneos periódicos, pruebas de intrusión controladas y evaluaciones técnicas continuas, así como la adopción de medidas de mitigación y remediación conforme a los resultados obtenidos.

Responsables:
Entidades públicas
Secretaría de Gobierno y Transformación Digital – PCM

Corresponsables:
Operadores de actividades críticas

Indicador:
Porcentaje de proveedores de actividades críticas y entidades públicas que ejecutaron pruebas de vulnerabilidad en el periodo.

Sentido esperado del indicador: Ascendente

Método de cálculo:
El indicador mide el porcentaje de proveedores de actividades críticas y entidades públicas que realizaron al menos una evaluación de vulnerabilidades durante el periodo de medición.

Para calcularlo, se identifica el total de proveedores de actividades críticas y entidades públicas priorizados; luego, se contabiliza cuántos de ellos realizaron al menos una evaluación de vulnerabilidades (escaneo o pentesting) durante el periodo de medición.

Finalmente, se divide el número de proveedores de actividades críticas y entidades públicas que realizaron al menos una evaluación de vulnerabilidades (escaneo o pentesting) entre el total de proveedores de actividades críticas y entidades públicas priorizados y se multiplica por 100.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de proveedores de actividades críticas y entidades públicas que ejecutaron pruebas de vulnerabilidad y gestión asociada.
B = Número total de proveedores de actividades críticas y entidades públicas priorizados.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Logro esperado:
2026: 15%
2027: 30%
2028: 55%
2029: 60%
2030: 75%

Tipo de logro esperado: No acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje

Acción estratégica 2.5: Implementar controles de seguridad en entornos industriales.

La finalidad de esta acción es reducir los riesgos de seguridad digital en entornos industriales y sistemas de tecnología operativa de los Activos Críticos Nacionales, los operadores de actividades críticas y los prestadores de Servicios Públicos Esenciales, mediante la implementación de arquitecturas de red segmentadas y controles de seguridad específicos que limiten accesos indebidos, movimientos laterales y la propagación de amenazas hacia sistemas críticos.

La segmentación adecuada y los controles industriales contienen la propagación de incidentes y protegen los procesos críticos que sostienen los servicios esenciales para la población, la economía y el Estado.

Su implementación se desarrolla conforme al ámbito de competencia, mediante dos líneas de actuación articuladas, complementadas por la definición de lineamientos técnicos y criterios por parte del ente rector.

1. En el ámbito de los Activos Críticos Nacionales, con la participación de la Dirección Nacional de Inteligencia, los operadores de Activos Críticos Nacionales con redes IT/OT adoptan los estándares internacionales aplicables. La verificación técnica de la segmentación y los controles industriales se articula con los servicios de la Dirección Nacional de Inteligencia en coordinación con los sectores responsables.

2. En el Marco de Confianza Digital, bajo los lineamientos de la Secretaría de Gobierno y Transformación Digital, los operadores de actividades críticas y los prestadores de Servicios Públicos Esenciales con redes IT/OT adoptan los mismos estándares internacionales, conforme a los lineamientos técnicos del ente rector y en coordinación con las entidades competentes.

Como resultado, se busca fortalecer la seguridad de los sistemas de control industrial, reducir la superficie de ataque, contener la propagación de incidentes y mejorar la resiliencia del ecosistema nacional de ciberseguridad frente a amenazas dirigidas a entornos industriales.

Responsable principal:
Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros

Corresponsables:
Operadores de Activos Críticos Nacionales
Operadores de actividades críticas
Prestadores de Servicios Públicos Esenciales con redes IT/OT.
Centro Nacional de Seguridad Digital (CNSD)
Dirección Nacional de Inteligencia (DINI) en el ámbito de los Activos Críticos Nacionales

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Sectores responsables del Anexo 4 del Decreto Supremo N° 106-2017-PCM en lo relativo a sus operadores
Organismos reguladores y supervisores competentes
Demás autoridades sectoriales competentes según el sector.

Indicador:
Porcentaje de operadores con redes IT/OT que han aplicado controles de seguridad industrial conforme a estándares internacionales en la materia y lineamientos de la entidad competente.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
Se identifica el total de operadores y prestadores priorizados por el ente rector y los sectores responsables con redes IT/OT, que comprende a los operadores de Activos Críticos Nacionales, a los operadores de actividades críticas y a los prestadores de Servicios Públicos Esenciales.

Se contabilizan aquellos que cuentan con segmentación de redes IT/OT validada y controles de seguridad en entornos industriales implementados conforme a los lineamientos emitidos por la entidad competente.

Para los operadores de Activos Críticos Nacionales se considera la verificación articulada con la Dirección Nacional de Inteligencia. Para los operadores de actividades críticas y prestadores de Servicios Públicos Esenciales se considera la verificación conforme a los lineamientos del ente rector.

El número de operadores y prestadores que cumplen dicha condición se divide entre el total priorizado.

El resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de operadores con redes IT/OT que aplicaron controles de seguridad industrial.
B = Número total de operadores con redes IT/OT priorizados.

Logro esperado:
2026: 1%
2027: 15%
2028: 25%
2029: 35%
2030: 45%

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje

<u>Acción estratégica 2.6</u>: Desplegar y fortalecer capacidades operativas de monitoreo, detección, contención y respuesta temprana frente a amenazas e incidentes de seguridad digital, mediante la implementación de tecnologías especializadas.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

La finalidad de esta acción es fortalecer las capacidades operativas de monitoreo continuo, detección y respuesta temprana frente a amenazas e incidentes de seguridad digital, mediante la implementación de tecnologías especializadas que permitan mejorar la visibilidad, correlación de eventos, identificación de anomalías y generación de alertas oportunas, a fin de reducir los tiempos de detección y contención de incidentes de seguridad digital.

Su implementación comprende el despliegue progresivo de herramientas y capacidades tecnológicas.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Entidades públicas

Indicador:
Porcentaje de entidades públicas priorizadas que cuentan con capacidades operativas de monitoreo, detección y respuesta temprana implementadas.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de entidades públicas priorizadas, conforme a criterios definidos por el ente rector.

En segundo lugar, se contabilizan aquellas entidades que cuentan con capacidades operativas implementadas para el monitoreo, detección y respuesta temprana frente a amenazas e incidentes de seguridad digital, incluyendo herramientas o servicios especializados o mecanismos automatizados de alerta y monitoreo continuo.

Posteriormente, se divide el número de entidades que cumplen dichas condiciones entre el total de entidades priorizadas.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de entidades públicas priorizadas con capacidades operativas de monitoreo, detección y respuesta temprana implementadas.
B = Número total de entidades públicas priorizadas.

Logro esperado:
2026: 0% (Período de preparación)
2027: 5%
2028: 10%
2029: 15%
2030: 20%

Tipo de logro esperado: Acumulado.

Periodicidad: Anual (con seguimiento trimestral recomendado).

Unidad de medida: Porcentaje.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

OBJETIVO ESTRATÉGICO N.° 3
DESARROLLAR UNA CULTURA NACIONAL DE CIBERSEGURIDAD Y SÓLIDAS CAPACIDADES OPERATIVAS EN EL TALENTO HUMANO DEL SECTOR PÚBLICO Y LA CIUDADANIA

El objetivo estratégico se orienta a desarrollar una cultura nacional de ciberseguridad y fortalecer las capacidades del talento humano en el sector público y la ciudadanía, mediante la formación progresiva de competencias, la profesionalización de los equipos especializados y la reducción de vulnerabilidades asociadas al factor humano.

Su implementación se sustenta en un enfoque integral que busca articular la educación formal, la formación especializada y la asistencia técnica, promoviendo el desarrollo de competencias en la ciudadanía, los servidores públicos y los especialistas en ciberseguridad.

ACCIONES ESTRATÉGICAS:

Acción estratégica 3.1: Promover la inclusión de la ciberseguridad en el sistema educativo nacional.

La finalidad de esta acción es desarrollar competencias que permitan a la ciudadanía estar preparada para afrontar los riesgos asociados a la ciberseguridad.

Esta iniciativa se implementa mediante la articulación pedagógica con el Currículo Nacional de la Educación Básica, con especial énfasis en la reflexión y el fortalecimiento de competencias que contribuyan a la prevención y atención de dichos riesgos, tales como *"Se desenvuelve en los entornos virtuales generados por las TIC"* y *"Convive y participa democráticamente en la búsqueda del bien común"*, entre otras.

De este modo, se promueve un aprovechamiento responsable, ético y seguro de las tecnologías digitales.

Responsables:
Ministerio de Educación - MINEDU
Secretaría de Gobierno y Transformación Digital - PCM
Entidades públicas

Indicador:
Porcentaje de instituciones educativas que implementan contenidos o actividades para el fortalecimiento de competencias vinculadas a la prevención y atención de riesgos de ciberseguridad, en el marco del Currículo Nacional de la Educación Básica.

Sentido esperado del indicador: Ascendente.

Método de cálculo:

El indicador se calcula identificando, en primer lugar, el universo de instituciones educativas comprendidas en el ámbito de aplicación de la acción estratégica, en coordinación con el Ministerio de Educación.

En segundo lugar, se contabilizan las instituciones educativas que implementan contenidos o actividades orientados al fortalecimiento de competencias vinculadas a la prevención y atención de riesgos de ciberseguridad, en el marco del Currículo Nacional de la Educación Básica.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Posteriormente, se divide el número de instituciones educativas que implementan dichos contenidos o actividades entre el total de instituciones educativas comprendidas en el universo definido.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de instituciones educativas que implementan contenidos o actividades de ciberseguridad.
B = Número total de instituciones educativas comprendidas en el ámbito de aplicación.

Logro esperado:
2026: 0% (Período de preparación)
2027: 5%
2028: 10%
2029: 15%
2030: 20%

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje

Acción estratégica 3.2: Implementar programas de capacitación, especialización y certificación dirigidos a los servidores públicos.

La finalidad de esta acción es fortalecer las capacidades técnicas y operativas de los servidores públicos vinculados a funciones relacionadas con la seguridad digital y la ciberseguridad, mediante el desarrollo progresivo de programas de capacitación, especialización y certificación orientados al cierre de brechas de conocimientos y competencias requeridas para el adecuado desempeño de sus funciones.

Su implementación comprende el diseño y articulación de una oferta formativa especializada, desarrollada por la Secretaría de Gobierno y Transformación Digital, en coordinación con la Autoridad Nacional del Servicio Civil.

Las acciones formativas priorizarán contenidos vinculados con gestión de incidentes de seguridad digital, análisis de amenazas, seguridad de la información, monitoreo de sistemas y demás materias relacionadas con la implementación de la Política Nacional de Transformación Digital.

Las entidades públicas incorporarán las acciones formativas que correspondan en sus respectivos Planes de Desarrollo de las Personas (PDP), de acuerdo con sus necesidades institucionales, disponibilidad presupuestal y prioridades estratégicas.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM

Corresponsables:
Autoridad Nacional del Servicio Civil - SERVIR, en el marco de sus competencias
Entidades públicas

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Indicador:
Número de servidores públicos que aprobaron programas de capacitación, especialización y/o certificación en ciberseguridad incorporados en los Planes de Desarrollo de las Personas (PDP) de las entidades públicas.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula identificando, en primer lugar, a los servidores públicos que participaron en programas de capacitación, especialización y/o certificación en ciberseguridad incorporados en los respectivos Planes de Desarrollo de las Personas (PDP) de las entidades públicas.

En segundo lugar, se contabilizan aquellos servidores públicos que aprobaron dichos programas durante el periodo de medición, conforme a los mecanismos de evaluación establecidos para cada actividad formativa.

Finalmente, el resultado del indicador corresponde al número total de servidores públicos que aprobaron programas de capacitación, especialización y/o certificación en ciberseguridad incorporados en los respectivos Planes de Desarrollo de las Personas (PDP) de las entidades públicas durante el periodo evaluado.

Logro esperado:
2026: 0 servidores (Período de preparación)
2027: 500 servidores
2028: 1000 servidores
2029: 1,500 servidores
2030: 1,800 servidores

Tipo de logro esperado: No acumulado.

Periodicidad: Anual

Unidad de medida: Número de servidores públicos que aprobaron programas de capacitación, especialización y/o certificación en ciberseguridad

Acción estratégica 3.3: Fortalecer la asistencia técnica descentralizada a gobiernos regionales y locales.

La finalidad de esta acción es elevar el nivel de madurez en ciberseguridad en los gobiernos regionales y locales, mediante la provisión de asistencia técnica orientada a la implementación de capacidades mínimas operativas en gestión de incidentes de seguridad digital, monitoreo de seguridad y protección de la información.

Su implementación comprende el diseño y despliegue de programas de asistencia técnica, la provisión de herramientas básicas de gestión de ciberseguridad, así como el acompañamiento técnico para la adopción de roles, procesos y controles mínimos conforme a lineamientos del ente rector, con énfasis en los gobiernos regionales y locales.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Centro Nacional de Seguridad Digital - CNSD

Corresponsables:
Gobiernos regionales
Gobiernos locales

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Indicador:
Porcentaje de gobiernos regionales y locales priorizados[68] asistidos técnicamente en materia de ciberseguridad

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de gobiernos regionales y locales priorizados, conforme a criterios de criticidad, nivel de riesgo o capacidad institucional definidos por el ente rector.

En segundo lugar, se cuentan aquellos gobiernos regionales y locales que han recibido asistencia técnica en materia de ciberseguridad durante el periodo de medición.

Posteriormente, se divide el número de gobiernos regionales y locales que recibieron asistencia técnica entre el total de gobiernos regionales y locales priorizados.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de gobiernos regionales y locales priorizados que recibieron asistencia técnica en materia de ciberseguridad.
B = Número total de gobiernos regionales y locales priorizados.

Logro esperado:
Gobiernos regionales:
2026: 10%
2027: 20%
2028: 35%
2029: 50%
2030: 60%

Gobiernos locales:
2026: 5%
2027: 10%
2028: 15%
2029: 25%
2030: 30%

Tipo de logro esperado: No acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje

<u>Acción Estratégica 3.4</u>: Promover la investigación, el desarrollo tecnológico y la innovación en materia de ciberseguridad, mediante la articulación y coordinación de los actores del Sistema Nacional de Ciencia, Tecnología e Innovación – Sinacti.

La finalidad de esta acción es fortalecer las capacidades nacionales en ciberseguridad mediante la promoción de actividades de investigación, desarrollo tecnológico e innovación,

[68] Los criterios de priorización serán determinados por la SGTD-CNSD.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

impulsando la articulación y coordinación entre los actores del Sistema Nacional de Ciencia, Tecnología e Innovación (SINACTI).

Responsables:
SGTD – PCM
Consejo Nacional de Ciencia, Tecnología e Innovación - CONCYTEC

Indicador: Número de iniciativas[69] de promoción, articulación o fortalecimiento de la investigación, desarrollo tecnológico e innovación en materia de ciberseguridad implementadas en el marco del SINACTI.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
En primer lugar, se identifican las iniciativas de promoción, articulación o fortalecimiento de la investigación, desarrollo tecnológico e innovación en materia de ciberseguridad implementadas en el marco del SINACTI, que cumplan con los criterios establecidos por la Secretaría de Gobierno y Transformación Digital, en coordinación con el CONCYTEC.

Posteriormente, se verifica su implementación mediante la documentación que la sustente.

Finalmente, se contabiliza el número total de iniciativas registradas durante el período de medición.

Logro esperado:
2026: 0 (Período de preparación)
2027: 2
2028: 4
2029: 7
2030: 10

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Número de iniciativas.

OBJETIVO ESTRATÉGICO N.° 4:
CONSOLIDAR LA COOPERACIÓN INTERNACIONAL Y EL INTERCAMBIO DE INFORMACIÓN SOBRE AMENAZAS DE SEGURIDAD DIGITAL

El objetivo estratégico se orienta a fortalecer la cooperación internacional y el intercambio de información en ciberseguridad mediante la integración activa del país en redes y foros internacionales, la suscripción de acuerdos de cooperación y la implementación de mecanismos seguros, confiables y sostenibles para el intercambio de inteligencia sobre amenazas digitales.

Se sustenta en la naturaleza transfronteriza de las amenazas de seguridad digital, que exige mecanismos de coordinación internacional para su prevención, detección y respuesta, así como para fortalecer la preparación y recuperación frente a incidentes de alcance

[69] Comprende, alternativamente, programas, proyectos, convocatorias, redes de investigación, alianzas interinstitucionales, grupos de trabajo, eventos científicos especializados y otras acciones equivalentes.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

transnacional. Asimismo, responde a la necesidad de mejorar el acceso oportuno a información estratégica, capacidades técnicas especializadas y buenas prácticas internacionales y a los criterios o marcos legales internacionales que contribuyan al fortalecimiento de la resiliencia del ecosistema digital nacional.

Su implementación busca posicionar al país como un actor confiable en el ecosistema internacional de ciberseguridad, fortaleciendo su nivel de madurez, su capacidad de respuesta ante incidentes de seguridad digital y su integración en esquemas de cooperación técnica y operativa.

ACCIONES ESTRATÉGICAS:

Acción estratégica 4.1: Consolidar la presencia multilateral en redes y foros internacionales de ciberseguridad e inteligencia de amenazas (*threat intelligence*).

Esta acción tiene por finalidad fortalecer la integración del país en mecanismos internacionales de cooperación en ciberseguridad, mediante una participación activa y sostenida en redes, foros, plataformas y espacios de intercambio de inteligencia sobre amenazas digitales, con el propósito de contribuir al fortalecimiento de capacidades nacionales, la cooperación técnica, la confianza internacional y la respuesta coordinada frente a riesgos de seguridad digital de alcance transfronterizo.

Su implementación comprende la gestión de membresías y otros mecanismos de cooperación internacional, la participación en actividades técnicas especializadas, así como el intercambio estructurado de información sobre amenazas digitales, bajo la coordinación del Centro Nacional de Seguridad Digital y el Ministerio de Relaciones Exteriores.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM

Corresponsables:
Ministerio de Relaciones Exteriores (MRE)

Indicador:
Número de participaciones del país en redes y foros internacionales de ciberseguridad e inteligencia de amenazas efectivamente realizadas.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula identificando las participaciones efectivas del país en redes y foros internacionales durante el periodo de medición.

El resultado del indicador corresponde al conteo total de participaciones efectivas del país en redes y foros internacionales.

Logro esperado:
2026: 0 (Período de preparación)
2027: 2
2028: 3
2029: 4
2030: 5

Tipo de logro esperado: No acumulado.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Periodicidad: Anual.

Unidad de medida: Número de participaciones efectivas del país en ciberseguridad

<u>Acción estratégica 4.2</u>: Promover acuerdos, instrumentos e iniciativas de cooperación bilateral y multilateral en ciberseguridad.

Esta acción tiene por finalidad fortalecer la cooperación internacional mediante la suscripción, renovación, implementación progresiva y seguimiento de acuerdos bilaterales y multilaterales en ciberseguridad que permitan el desarrollo de capacidades, el intercambio seguro y oportuno de información y la respuesta coordinada ante incidentes de seguridad digital.

Responsables:
Ministerio de Relaciones Exteriores (MRE)

Corresponsables:
Secretaría de Gobierno y Transformación Digital - PCM

Indicador:
Número de acuerdos, instrumentos o iniciativas internacionales de cooperación en ciberseguridad iniciados formalmente, suscritos o implementados

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula contabilizando el número total acumulado de acuerdos, instrumentos o iniciativas internacionales de cooperación en ciberseguridad que cuenten con evidencia documentada de avance (iniciados, suscritos o implementados) hasta el final del periodo de medición.

Logro esperado:
2026: 0 (Período de preparación)
2027: 1
2028: 2
2029: 3
2030: 4

Tipo de logro esperado: No acumulado.

Periodicidad: Anual.

Unidad de medida: Número de acuerdos, instrumentos o iniciativas internacionales de cooperación en ciberseguridad.

<u>Acción estratégica 4.3</u>: Participar y organizar ejercicios internacionales en materia de ciberseguridad en coordinación con la entidad competente, según corresponda.

Esta acción tiene por finalidad fortalecer las capacidades nacionales de prevención, detección y respuesta ante incidentes de seguridad digital mediante la participación y organización de ejercicios internacionales que permitan evaluar escenarios complejos, mejorar la coordinación interinstitucional e identificar oportunidades de mejora para la preparación y recuperación frente a incidentes de alcance transnacional.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Su implementación comprende la participación en ejercicios internacionales, así como la promoción y organización de ejercicios conjuntos, en el ámbito de la ciberseguridad y la ciberdefensa, según las competencias de las entidades involucradas.

Responsables:
Secretaría de Gobierno y Transformación Digital – SGTD
Centro Nacional de Seguridad Digital

Corresponsable:
Ministerio de Relaciones Exteriores (MRE)

Indicador:
Número de ejercicios internacionales de ciberseguridad en los que el país participa u organiza.

Sentido esperado del indicador: No definido.

Método de cálculo:
El indicador se calcula contabilizando el número de ejercicios internacionales de ciberseguridad en los que el país participa o que organiza durante el periodo de medición.

El resultado del indicador corresponde al conteo total de ejercicios internacionales de ciberseguridad en los que el país participa o que organiza.

Logro esperado:
2026: 0 (Período de preparación)
2027: 1
2028: 2
2029: 2
2030: 2

Tipo de logro esperado: No acumulado.

Periodicidad: Anual.

Unidad de medida: Número de ejercicios internacionales de ciberseguridad

<u>Acción estratégica 4.4</u>: Adoptar, promover y difundir normas técnicas internacionales aplicables a la gestión de la ciberseguridad, en coordinación con el INACAL y las entidades y/o autoridades competentes.

Esta acción tiene por finalidad armonizar las prácticas nacionales en ciberseguridad con normas técnicas internacionales y buenas prácticas reconocidas, mediante la identificación, priorización, adopción nacional y promoción de normas técnicas aplicables a la gestión de la ciberseguridad, seguridad de la información, gestión de riesgos, continuidad del negocio, protección de datos, gobernanza digital y materias conexas.

La implementación de esta acción estratégica se realizará en coordinación con el Instituto Nacional de Calidad – INACAL, en el marco de sus competencias en normalización técnica, y con las entidades competentes responsables de la implementación, seguimiento y promoción de dichos instrumentos en el sector público y demás actores del ecosistema digital.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Instituto Nacional de Calidad (INACAL), en el marco de sus competencias asignadas.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Indicador:
Número de normas técnicas internacionales de ciberseguridad priorizadas y adoptadas como Normas Técnicas Peruanas

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula contabilizando el número de normas técnicas internacionales de ciberseguridad priorizadas y adoptadas como Normas Técnicas Peruanas durante el periodo de medición.

El resultado del indicador corresponde al conteo total de normas técnicas internacionales de ciberseguridad priorizadas y adoptadas como Normas Técnicas Peruanas.

Logro esperado:
2026: 0 (Período de preparación)
2027: 1
2028: 2
2029: 3
2030: 4

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Número de normas técnicas internacionales

<u>Acción estratégica 4.5</u>: Fortalecer mecanismos de intercambio seguro de información sobre amenazas digitales.

Esta acción tiene por finalidad asegurar el intercambio confiable, oportuno y transfronterizo de inteligencia sobre amenazas digitales, mediante el uso de plataformas seguras, protocolos estandarizados y mecanismos de gobernanza que garanticen la confidencialidad, integridad y trazabilidad de la información, tanto a nivel nacional como internacional.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM

Corresponsables:
Entidades públicas
Sector privado

Indicador:
Número de intercambios de información sobre amenazas digitales realizados

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula contabilizando el número de intercambios de información sobre amenazas digitales realizados durante el periodo de medición, entre el Centro Nacional de Seguridad Digital y equipos CSIRT, redes, plataformas u organismos especializados en ciberseguridad a nivel nacional e internacional.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

El resultado del indicador corresponde al conteo total de intercambios de información sobre amenazas digitales realizados durante el periodo de medición.

Logro esperado:
2026: 0 intercambios (Período de preparación)
2027: 5 intercambios
2028: 10 intercambios
2029: 15 intercambios
2030: 20 intercambios

Tipo de logro esperado: No acumulado.

Periodicidad: Anual.

Unidad de medida: Número de intercambios de información sobre amenazas digitales

Acción estratégica 4.6: Promover un modelo de cooperación sostenible para la ciberseguridad nacional.

Esta acción busca fortalecer las capacidades nacionales en ciberseguridad mediante la identificación y promoción de mecanismos de cooperación internacional que faciliten el acceso a fuentes complementarias de financiamiento, asistencia técnica especializada, transferencia de conocimiento, intercambio de experiencias y recursos de cooperación técnica no reembolsable.

Su implementación comprende el diseño, puesta en funcionamiento y seguimiento de un modelo articulado de cooperación internacional en ciberseguridad, liderado por la Secretaría de Gobierno y Transformación Digital, que permita identificar oportunidades de cooperación, formular y promover iniciativas, articular con entidades nacionales y socios internacionales, y realizar el seguimiento de las actividades orientadas al fortalecimiento del ecosistema nacional de ciberseguridad.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM

Indicador:
Número de iniciativas de cooperación internacional en ciberseguridad promovidas o gestionadas.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
Se contabiliza el número acumulado de iniciativas de cooperación internacional en ciberseguridad promovidas, gestionadas o articuladas por la Secretaría de Gobierno y Transformación Digital durante el periodo de implementación de la Estrategia.

Logro esperado:
2026: 0 (Período de preparación)
2027: 3
2028: 5
2029: 7
2030: 10

Tipo de logro esperado: Acumulado.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Periodicidad: Anual.

Unidad de medida: Número de iniciativas de cooperación internacional en ciberseguridad promovidas o gestionadas.

OBJETIVO ESTRATÉGICO N.º 5
FORTALECER LA GOBERNANZA Y EL MARCO NORMATIVO EN CIBERSEGURIDAD EN LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA

El objetivo estratégico se orienta a fortalecer la gobernanza y el marco normativo en ciberseguridad, mediante la definición clara de roles y responsabilidades, la consolidación de mecanismos de supervisión y cumplimiento en el sector público.

ACCIONES ESTRATÉGICAS:

Acción estratégica 5.1: Evaluar el marco normativo y modelo de gobernanza nacional vigente, con arreglo a los roles, responsabilidades, mecanismos de articulación entre los diferentes niveles de gobierno y sectores, y el nivel estratégico del Centro Nacional de Seguridad Digital.

Esta acción tiene por finalidad revisar y optimizar el marco normativo vigente en materia de ciberseguridad, así como el modelo de gobernanza nacional, a efectos de garantizar claridad en la asignación de competencias, coherencia regulatoria y efectividad en su implementación.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM

Corresponsables:
Entidades públicas

Indicador:
Porcentaje de avance en la revisión y propuesta de actualización del marco normativo y modelo de gobernanza nacional en ciberseguridad.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador mide el avance progresivo del proceso de revisión, evaluación y formulación de propuestas de actualización del marco normativo y del modelo de gobernanza nacional en materia de ciberseguridad.

Para ello, se asigna un porcentaje de avance a cada fase culminada durante el periodo de evaluación, conforme al siguiente esquema:

- 0% = No iniciado.
- **25% - Evaluación preliminar**: Mapeo y análisis del marco normativo vigente, identificación de vacíos regulatorios, superposición o ausencia de competencias, mecanismos de articulación interinstitucional y evaluación de la estructura, capacidades y nivel estratégico del Centro Nacional de Seguridad Digital.
- **50% - Validación técnica e institucional**: Desarrollo de procesos de articulación y validación técnica con entidades públicas, sectores involucrados y actores relevantes, respecto de los hallazgos, brechas identificadas y alternativas de mejora del modelo de gobernanza.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

- **75% - Diagnóstico y recomendaciones**: Informe o diagnóstico legal con las recomendaciones de modificación normativa y nuevo diseño del modelo de gobernanza.
- **100% - Propuesta normativa y modelo de gobernanza**: Formulación de la propuesta normativa y del modelo de gobernanza nacional en ciberseguridad, incluyendo roles, competencias, mecanismos de coordinación y lineamientos para su implementación.

Logro esperado:
2026: 0% (Período de preparación)
2027: 50%
2028: 100%

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje

Acción estratégica 5.2: Fortalecer mecanismos de supervisión y monitoreo en ciberseguridad en las entidades de la Administración Pública.

Esta acción tiene por finalidad asegurar el cumplimiento efectivo de las obligaciones en materia de ciberseguridad mediante el fortalecimiento de mecanismos de supervisión, monitoreo y verificación de cumplimiento en las entidades públicas.

Ello se realizará a través de la plataforma de cumplimiento digital, que defina niveles de cumplimiento progresivo, mecanismos de seguimiento y verificación, orientados a asegurar el cumplimiento efectivo de las obligaciones en materia de ciberseguridad.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Centro Nacional de Seguridad Digital

Corresponsables:
Entidades públicas

Indicador:
Porcentaje de entidades públicas priorizadas[70] con verificación de cumplimiento en materia de ciberseguridad.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de entidades públicas priorizadas para la supervisión, monitoreo y verificación de cumplimiento en materia de ciberseguridad durante el periodo de medición.

En segundo lugar, se contabilizan aquellas entidades públicas que han sido objeto de mecanismos de supervisión, monitoreo y verificación del cumplimiento de obligaciones en materia de ciberseguridad.

Posteriormente, se divide el número de entidades verificadas entre el total de entidades priorizadas.

[70] Los criterios de priorización serán determinados por la SGTD-CNSD.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de entidades públicas priorizadas con verificación de cumplimiento en materia de ciberseguridad.
B = Número total de entidades públicas priorizadas.

Logro esperado:
2026: 0% (Período de preparación)
2027: 15%
2028: 30%
2029: 45%
2030: 60%

Tipo de logro esperado: Acumulado

Periodicidad: Anual.

Unidad de medida: Porcentaje

Acción estratégica 5.3: Evaluar y fortalecer el modelo de rectoría en ciberseguridad y marco normativo a nivel nacional.

Esta acción busca fortalecer el modelo de rectoría en ciberseguridad mediante la formulación de propuestas de adecuación normativa que refuercen las funciones del ente rector, bajo la conducción de la PCM y la Secretaría de Gobierno y Transformación Digital, garantizando su articulación con las entidades competentes.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM

Corresponsables:
Centro Nacional de Seguridad Digital
Indicador:
Número de instrumentos normativos, lineamientos o mecanismos aprobados para fortalecer el modelo nacional de rectoría y gobernanza en ciberseguridad.

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula contabilizando el número de instrumentos normativos, lineamientos, protocolos, mecanismos aprobados durante el periodo de medición para fortalecer el modelo nacional de rectoría y gobernanza en materia de ciberseguridad.

El valor final del indicador corresponde a la suma total de instrumentos normativos, lineamientos o mecanismos aprobados durante el periodo de evaluación.

Logro esperado:
2026: 0 (Período de preparación)
2027: 1 instrumento normativo aprobado.
2028: 1 instrumento normativo aprobado.
2029: 1 instrumento normativo aprobado.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

2030: 2 instrumentos normativos aprobados.

Tipo de logro esperado: No acumulado.

Periodicidad: Anual.

Unidad de medida: Número de instrumentos

Acción estratégica 5.4: Fortalecer el rol estratégico de los Oficiales de Seguridad y Confianza Digital en las entidades públicas.

Esta acción tiene por finalidad fortalecer el rol estratégico de los Oficiales de Seguridad y Confianza Digital (OSCD) mediante el desarrollo continuo y especializado de capacidades técnicas, la estandarización de sus funciones y la consolidación de mecanismos de coordinación institucional, a fin de mejorar la gestión de riesgos digitales en las entidades públicas.

Su implementación contempla la provisión de asistencia técnica especializada, así como la creación de mecanismos formales de articulación entre los OSCD y el Centro Nacional de Seguridad Digital, orientados al intercambio de información, la difusión de buenas prácticas y la coordinación efectiva para la gestión de incidentes de seguridad digital.

Responsables:
Secretaría de Gobierno y Transformación Digital – PCM
Centro Nacional de Seguridad Digital

Corresponsables:
Entidades públicas

Indicador:
Porcentaje de entidades públicas priorizadas[71] con Oficial de Seguridad y Confianza Digital formalmente designado

Sentido esperado del indicador: Ascendente.
Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de entidades públicas priorizadas para la implementación y fortalecimiento del rol de Oficial de Seguridad y Confianza Digital (OSCD) durante el periodo de medición.

En segundo lugar, se contabilizan aquellas entidades públicas que cuentan con un OSCD formalmente designado.

Posteriormente, se divide el número de entidades que cumplen dichas condiciones entre el total de entidades públicas priorizadas.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de entidades públicas priorizadas con OSCD formalmente designado.
B = Número total de entidades públicas priorizadas.

[71] Los criterios de priorización serán determinados por la SGTD-CNSD.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Logro esperado:
2026: 0% (Período de preparación)
2027: 50%
2028: 60%
2029: 70%
2030: 80%

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje

Acción estratégica 5.5: Elaborar normas, lineamientos, directivas, guías o políticas para el uso de criptografía a efectos de proteger la confidencialidad, integridad y autenticidad de activos y objetos digitales.

Esta acción estratégica busca fortalecer la protección de la información y de los activos digitales mediante la elaboración de disposiciones que orienten la implementación y gestión de mecanismos criptográficos en las entidades públicas y, cuando corresponda, en otros actores relevantes del ecosistema digital.

Su implementación contempla la elaboración y aprobación de normas, lineamientos, directivas, guías o políticas que definan criterios para el uso seguro de tecnologías criptográficas, incluyendo el cifrado de información, la gestión de claves criptográficas, las firmas digitales, los certificados digitales y otros mecanismos destinados a garantizar la confidencialidad, integridad, autenticidad y no repudio de la información, de conformidad con estándares y buenas prácticas internacionales de ciberseguridad.

La ejecución de esta acción estratégica podrá apoyarse en cooperación técnica internacional no reembolsable, destinada a fortalecer capacidades, promover la transferencia de conocimientos especializados y apoyar el desarrollo de normas, lineamientos, directivas, guías o políticas para la protección de activos y objetos digitales mediante el uso de criptografía.

Asimismo, busca promover la adopción homogénea de controles criptográficos en los procesos, servicios y plataformas digitales críticas, contribuyendo a reducir los riesgos asociados al acceso no autorizado, la alteración de datos, la suplantación de identidad y otras amenazas que afectan la confianza y seguridad del entorno digital.

Esta acción también contribuirá a alinear al país con la Recomendación del Consejo sobre Directrices para la Política de Criptografía de la OCDE (OECD/LEGAL/0289), promoviendo un equilibrio adecuado entre la protección de la información, la gestión de riesgos, la innovación digital, el comercio electrónico y la confianza en el entorno digital.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI

Corresponsables:
Entidades públicas

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Indicador:
Número de normas, lineamientos, directivas, guías o políticas aprobadas para el uso de criptografía aplicables a la Infraestructura Oficial de Firma Electrónica (IOFE) y servicios de confianza digital; así como al almacenamiento, procesamiento e intercambio de datos e información entre plataformas o sistemas de información.

Sentido esperado del indicador: Ascendente

Método de cálculo:
El indicador se calcula contabilizando el número de normas, lineamientos, directivas, guías o políticas aprobadas para el uso de criptografía en entidades públicas y/o otros actores relevantes del ecosistema digital aplicables a la Infraestructura Oficial de Firma Electrónica (IOFE) y servicios de confianza digital; así como al almacenamiento, procesamiento e intercambio de datos e información entre plataformas o sistemas de información.

Logro esperado:
2026: 0 (Período de preparación)
2027: 0 (Período de preparación)
2028: 1 norma, lineamiento, directiva, guía o política aprobada
2029: 2 normas, lineamientos, directivas, guías o políticas aprobadas
2030: 4 normas, lineamientos, directivas, guías o políticas aprobadas

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Número de normas, lineamientos, directivas, guías o políticas aprobadas.

Acción estratégica 5.6: Incorporar en los Planes de Gobierno Digital el componente de ciberseguridad.

Esta acción busca impulsar la incorporación efectiva de la ciberseguridad en los Planes de Gobierno Digital (PGD), con el fin de integrar la gestión de riesgos y las medidas de protección en la planificación estratégica tecnológica de las entidades públicas.

Ello, en concordancia con los Lineamientos para la formulación del Plan de Gobierno Digital, aprobados mediante la Resolución de Secretaría de Gobierno Digital N.º 005-2018-PCM/SEGDI, los cuales establecen la necesidad de evaluar la incorporación de controles de seguridad de la información en los proyectos de gobierno digital orientados a la digitalización de servicios, así como la adopción de marcos de referencia y buenas prácticas para la gestión de riesgos en dichos proyectos.

Su ejecución requerirá que los Comités de Gobierno y Transformación Digital, en coordinación con el Oficial de Seguridad y Confianza Digital (OSCD) de cada entidad, incluyan dentro del portafolio de proyectos de su PGD las iniciativas orientadas a mitigar vulnerabilidades e implementar controles de ciberseguridad.

Responsables:
Entidades públicas (Comités de Gobierno y Transformación Digital y Oficial de Seguridad y Confianza Digital)

Corresponsables:
Secretaría de Gobierno y Transformación Digital - PCM

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Indicador:
Porcentaje de Planes de Gobierno Digital (PGD) aprobados con componentes de ciberseguridad incorporados conforme a los lineamientos del ente rector.

Sentido esperado del indicador: Ascendente

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de Planes de Gobierno Digital aprobados en las entidades públicas comprendidas en el ámbito de aplicación.

En segundo lugar, se contabilizan aquellos Planes de Gobierno Digital que incorporan componentes de ciberseguridad conforme a los lineamientos definidos por el ente rector.

Posteriormente, se divide el número de Planes de Gobierno Digital que incorporan componentes de ciberseguridad entre el total de planes aprobados.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de Planes de Gobierno Digital con componentes de ciberseguridad incorporados.
B = Número total de Planes de Gobierno Digital aprobados.

Logro esperado:
2026: 35%
2027: 45%
2028: 60%
2029: 75%
2030: 90%

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje.

Acción estratégica 5.7: Promover la integración progresiva de la ciberseguridad como un componente dentro de los Planes Operativos Institucionales (POI) y/o en las actualizaciones de los Planes Estratégicos Institucionales (PEI).

La finalidad de esta acción es asegurar la sostenibilidad de la ciberseguridad en la gestión pública, mediante su incorporación en los Planes Estratégicos Institucionales (PEI) y/o Planes Operativos Institucionales (POI), según corresponda, alineando los objetivos de ciberseguridad con la gestión de riesgos y la continuidad de los servicios esenciales.

Responsables:
Entidades públicas
Secretaría de Gobierno y Transformación Digital - PCM
CEPLAN

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Indicador:
Porcentaje de entidades públicas que incorporan objetivos, indicadores, metas en materia de ciberseguridad en los Planes Operativos Institucionales (POI) y/o en las actualizaciones de los Planes Estratégicos Institucionales (PEI).

Sentido esperado: Ascendente.

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de entidades públicas comprendidas en el ámbito de aplicación, conforme a los criterios definidos por el ente rector.

En segundo lugar, se contabilizan aquellas entidades que incorporan, en los Planes Operativos Institucionales (POI) y/o en las actualizaciones de los Planes Estratégicos Institucionales (PEI), elementos en materia de ciberseguridad, en coherencia con los lineamientos establecidos por el ente rector.

Posteriormente, se divide el número de entidades que cumplen dichas condiciones entre el total de entidades comprendidas en el ámbito de aplicación.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de entidades públicas que incorporan objetivos, indicadores y metas en materia de ciberseguridad en el POI y/o PEI.
B = Número total de entidades públicas comprendidas en el ámbito de aplicación.

Logro esperado:
2026: 0% (Período de preparación)
2027: 0% (Período de preparación)
2028: 30%
2029: 40%
2030: 60%

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Porcentaje

OBJETIVO ESTRATÉGICO N.° 6
DESARROLLAR CAPACIDADES NACIONALES DE GESTIÓN DE RIESGOS DIGITALES E INTELIGENCIA EN CIBERSEGURIDAD EN LAS ENTIDADES DEL ESTADO Y SECTORES ESTRATÉGICOS

Este objetivo busca fortalecer la capacidad del Estado para anticipar, identificar y gestionar riesgos digitales, transitando de un enfoque reactivo a uno preventivo basado en inteligencia.

Se fundamenta en la ausencia de metodologías estandarizadas de gestión de riesgos y en la limitada capacidad de anticipación frente a amenazas de alto impacto.

Su implementación se orienta al desarrollo de capacidades técnicas, metodológicas y de inteligencia en ciberseguridad, que permitan una detección temprana de amenazas y una toma de decisiones informada.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

ACCIONES ESTRATÉGICAS:

Acción estratégica 6.1: Implementar un modelo nacional de gestión de riesgos de ciberseguridad con enfoque sectorial.

Esta acción busca estandarizar la identificación, evaluación y mitigación de riesgos digitales en las entidades públicas, superando la actual gestión fragmentada y no homogénea. Su implementación contempla la adopción de una metodología oficial basada en estándares internacionales, con perfiles de riesgo diferenciados según la criticidad de cada sector.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Centro Nacional de Seguridad Digital - CNSD

Corresponsables:
Entidades públicas

Indicador:
Número de sectores con el modelo nacional de gestión de riesgos de ciberseguridad adoptado

Sentido esperado del indicador: Ascendente.

Método de cálculo:
El indicador se calcula contabilizando el número de sectores que han adoptado formalmente el modelo nacional de gestión de riesgos de ciberseguridad durante el periodo de medición.

Se considera que un sector adopta el modelo cuando ha aprobado o incorporado el modelo mediante instrumento formal (lineamientos sectoriales, directivas u otros) o existe evidencia documental de dicha adopción.

El resultado corresponde al conteo total de sectores que cumplen dichas condiciones.

Logro esperado:
2026: 0 sectores (Período de preparación)
2027: 5 sectores
2028: 7 sectores
2029: 9 sectores
2030: 11 sectores

Tipo de logro esperado: Acumulado.

Periodicidad: Anual.

Unidad de medida: Número de sectores que han adoptado formalmente el modelo nacional de gestión de riesgos de ciberseguridad

Acción estratégica 6.2: Desarrollar una plataforma nacional de inteligencia de amenazas digitales (*Threat Intelligence*).

Esta acción se encuentra orientada a la recolección, correlación, análisis e intercambio de información sobre amenazas, vulnerabilidades, indicadores de compromiso y tácticas de ataque, a fin de fortalecer la alerta temprana y la coordinación nacional en ciberseguridad.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Centro Nacional de Seguridad Digital

Corresponsables:
Entidades públicas

Indicador:
Plataforma Nacional de Inteligencia de Amenazas Digitales implementada y operativa.

Método de cálculo:
El indicador verifica la implementación y operatividad de una plataforma nacional de inteligencia de amenazas digitales orientada a la recolección, correlación, análisis e intercambio de información sobre amenazas, vulnerabilidades, indicadores de compromiso y tácticas de ataque.

Para efectos de medición, se considera cumplido el indicador cuando la plataforma se encuentre implementada, cuente con capacidades funcionales para el intercambio de inteligencia de amenazas y se encuentre operativa para las entidades públicas y proveedores de actividades críticas definidos conforme a los lineamientos técnicos establecidos por la Secretaría de Gobierno y Transformación Digital.

Logro esperado:
2028: Plataforma implementada y operativa.

Periodicidad: Anual.

Unidad de medida: Implementación de la plataforma.

Acción estratégica 6.3: Establecer mecanismos de intercambio estructurado de información (STIX/TAXII).

Esta acción busca automatizar el intercambio de información sobre ciberamenazas entre entidades públicas, mediante el uso de estándares que permitan una comunicación eficiente, segura y en tiempo real.

Responsables:
Secretaría de Gobierno y Transformación Digital – PCM
Centro Nacional de Seguridad Digital – CNSD

Corresponsables:
Entidades públicas

Indicador:
Plataforma de intercambio de información sobre ciberamenazas implementada y operativa

Método de cálculo:
El indicador verifica el cumplimiento de las condiciones técnicas y operativas previstas para la implementación de la plataforma de intercambio estructurado de información sobre ciberamenazas.

Logro esperado:
2030: Una plataforma implementada y operativa.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Periodicidad: Anual.

Unidad de medida: Plataforma implementada y operativa.

Acción estratégica 6.4: Generar informes/reportes/documentos periódicos de riesgos y amenazas para la toma de decisiones estratégicas.

Esta acción busca traducir la información técnica sobre amenazas digitales en productos que faciliten la toma de decisiones estratégicas en los niveles directivos del Estado. Su implementación estará a cargo de la Secretaría de Gobierno y Transformación Digital (SGTD-PCM), mediante la elaboración y difusión de informes que integren análisis de riesgos, tendencias de amenazas, evaluación de impacto y recomendaciones estratégicas.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Centro Nacional de Seguridad Digital – CNSD

Corresponsables:
Entidades públicas

Indicador:
Número de informes/reportes/documentos periódicos de riesgos y amenazas elaborados y difundidos para la toma de decisiones estratégicas.

Sentido esperado del indicador: Ascendente

Método de cálculo:
El indicador se calcula contabilizando el número total de informes elaborados para la toma de decisiones estratégicas durante el periodo de medición.

Logro esperado:
2026: 1 informe
2027: 2 informes
2028: 3 informes
2029: 4 informes
2030: 5 informes

Tipo de logro esperado: No acumulado.

Periodicidad: Anual.

Unidad de medida: Número de informes.

Acción estratégica 6.5: Integrar capacidades nacionales de analítica avanzada e inteligencia artificial para la anticipación y análisis predictivo de amenazas de seguridad digital.

Esta acción busca fortalecer las capacidades nacionales de anticipación y análisis predictivo frente a amenazas de seguridad digital, mediante la incorporación progresiva de herramientas de analítica avanzada e inteligencia artificial orientadas a la correlación de eventos, detección de anomalías, análisis de comportamiento e identificación de patrones de ataque, con el fin de mejorar la generación de alertas estratégicas, la prevención de incidentes y la toma de decisiones en materia de ciberseguridad.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Su implementación contempla el desarrollo e integración de capacidades de análisis automatizado sobre información de amenazas, eventos e incidentes de seguridad digital, incluyendo modelos de aprendizaje automático y mecanismos avanzados de correlación y análisis predictivo en el ámbito del Centro Nacional de Seguridad Digital.

Responsables:
Secretaría de Gobierno y Transformación Digital - PCM
Centro Nacional de Seguridad Digital – CNSD

Corresponsables:
Entidades públicas

Indicador:
Porcentaje de alertas de amenazas generadas mediante capacidades de analítica avanzada e inteligencia artificial.

Sentido esperado del indicador: Ascendente

Método de cálculo:
El indicador se calcula identificando, en primer lugar, el total de alertas por amenazas de seguridad digital generadas durante el periodo de medición.

En segundo lugar, se contabilizan aquellas alertas de amenazas generadas mediante el uso de capacidades de analítica avanzada e inteligencia artificial durante el mismo periodo.

Posteriormente, se divide el número de alertas generadas mediante dichas capacidades entre el total de alertas de amenazas de seguridad digital generadas durante el periodo de medición.

Finalmente, el resultado se multiplica por 100 para expresarlo en porcentaje.

Fórmula para el indicador porcentual:
Fórmula: **A / B × 100**
Donde:
A = Número de alertas de amenazas generadas mediante analítica avanzada e inteligencia artificial.
B = Número total de alertas de amenazas generadas.

Logro esperado:
2027: 5%
2028: 15%
2029: 20%
2030: 25%

Tipo de logro esperado: No acumulado

Periodicidad: Anual.

Unidad de medida: Porcentaje.

La matriz consolidada de los Objetivos Estratégicos, Acciones Estratégicas e Indicadores de la ENC se desarrolla en el Anexo II.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

VI. SEGUIMIENTO, MONITOREO Y EVALUACIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

El seguimiento, monitoreo y evaluación de la Estrategia Nacional de Ciberseguridad tiene por finalidad verificar el avance en el cumplimiento de los objetivos y acciones estratégicas, identificar brechas y riesgos en su implementación, generar información para la toma de decisiones y promover la mejora continua de las capacidades nacionales de ciberseguridad.

Entidad responsable:

La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de ministros, en su calidad de ente rector en materia de confianza digital y responsable de la conducción de la Estrategia Nacional de Ciberseguridad, lidera el proceso de seguimiento y evaluación de su implementación.

Para dicho fin, coordina con el Centro Nacional de Seguridad Digital, las entidades responsables y corresponsables de cada acción estratégica, así como con las demás entidades públicas y actores involucrados en su ejecución.

Monitoreo de las acciones estratégicas:

El monitoreo tiene por objeto verificar el avance en la ejecución de las acciones estratégicas previstas en la Estrategia.

Las entidades responsables y corresponsables deberán proporcionar la información necesaria para la medición de los indicadores establecidos para cada acción estratégica, conforme a los medios de verificación definidos.

El monitoreo se realizará de manera:

- **Semestral**, para verificar el avance de ejecución de las acciones estratégicas y detectar oportunamente retrasos, riesgos o necesidades de ajuste.
- **Anual**, para determinar el nivel de cumplimiento de las metas previstas para cada indicador durante el correspondiente año.

Evaluación de resultados:

La evaluación tiene por finalidad analizar el nivel de contribución de las acciones estratégicas al logro de los objetivos de la Estrategia y a la reducción progresiva de las brechas identificadas en materia de ciberseguridad.

La evaluación considerará, entre otros aspectos:

- El grado de cumplimiento de metas.
- La evolución de las capacidades nacionales de prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital.
- El fortalecimiento de la gobernanza nacional de la ciberseguridad.
- El desarrollo de capacidades técnicas, institucionales y de talento especializado.
- Los avances en cooperación nacional e internacional.

Informes de seguimiento y evaluación:

La Secretaría de Gobierno y Transformación Digital - SGTD elabora:

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

a) **Informes semestrales de seguimiento**, que contendrán el estado de avance de las acciones estratégicas, riesgos identificados y recomendaciones para facilitar su implementación.

b) **Informes anuales de evaluación**, que analizarán el cumplimiento de las metas e indicadores establecidos para cada año de vigencia de la Estrategia.

Los resultados podrán ser puestos en conocimiento de las entidades involucradas para la adopción de medidas correctivas, preventivas o de mejora que resulten necesarias.

Evaluación de medio término y evaluación final:

Con la finalidad de verificar la efectividad de la Estrategia y realizar los ajustes que resulten necesarios durante su vigencia, se realizarán las siguientes evaluaciones:

- **Evaluación de medio término:** durante el año 2028.
- **Evaluación final:** durante el año 2030.

Estas evaluaciones analizarán el avance global de la Estrategia, la pertinencia de sus acciones, el cumplimiento de los objetivos estratégicos y la necesidad de incorporar ajustes o medidas complementarias para fortalecer la política nacional de ciberseguridad.

Mejora continua:

Los resultados del seguimiento y de las evaluaciones constituyen insumos para la actualización de prioridades, la adopción de medidas de mejora y el fortalecimiento progresivo de las capacidades nacionales de ciberseguridad, promoviendo una implementación flexible y adaptativa frente a la evolución de las amenazas y riesgos en el entorno digital.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

ANEXOS

I. Matriz de alineación entre los Objetivos Prioritarios y Lineamientos de la PNTD con los Objetivos y Acciones Estratégicas de la ENC.

Objetivo Prioritario de la PNTD	Lineamiento PNTD	Objetivo Estratégico de la ENC	Acción Estratégica ENC	Sustento de la alineación
OP3. Garantizar la disponibilidad de servicios públicos digitales inclusivos, predictivos y empáticos con la ciudadanía.	**3.1.** Incorporar el enfoque de transformación digital en la formulación del plan estratégico de desarrollo nacional, políticas nacionales, regionales y locales.	**OE5.** Fortalecer la gobernanza y el marco normativo en ciberseguridad en las entidades de la administración pública.	**AE 5.6.** Incorporar en los Planes de Gobierno Digital el componente de ciberseguridad. **AE 5.7.** Promover la integración progresiva de la ciberseguridad como un componente dentro de los Planes Operativos Institucionales (POI) y/o en las actualizaciones de los Planes Estratégicos Institucionales (PEI).	La PNTD busca que la transformación digital sea incorporada en los instrumentos de planificación. La ENC concreta esta orientación al incorporar la ciberseguridad en los instrumentos de gobierno y planificación institucional, asegurando que la transformación digital considere la seguridad como componente transversal.
	3.2. Desplegar la estrategia de gobierno como plataforma de regulación, servicios digitales, datos abiertos e interoperabilidad entre organizaciones públicas y privadas.	**OE5.** Fortalecer la gobernanza y el marco normativo en ciberseguridad en las entidades de la administración pública; y, **OE2.** Fortalecer la ciberseguridad de los activos críticos nacionales, las actividades críticas y los servicios públicos esenciales frente a amenazas de seguridad digital.	**AE 5.5.** Elaborar normas, lineamientos, directivas, guías o políticas para el uso de criptografía a efectos de proteger la confidencialidad, integridad y autenticidad de activos y objetos digitales.	La PNTD promueve servicios interoperables y el intercambio de información entre entidades. La ENC incorpora medidas para proteger la confidencialidad, integridad y autenticidad de los datos y, a su vez, establece medidas de protección de activos críticos nacionales y servicios públicos esenciales. La relación es especialmente relevante porque la seguridad constituye una condición habilitante para la interoperabilidad.
	3.4. Ofrecer servicios digitales predictivos a las personas, con el uso de tecnologías exponenciales y en colaboración con los actores del ecosistema digital.	**OE1.** Fortalecer las capacidades nacionales de prevención, detección, respuesta y recuperación ante incidentes de seguridad digital; y	**AE 1.1.** Consolidar una arquitectura nacional de ciberseguridad basada en un modelo SOC de SOCs e iSOC para redes OT (Redes Industriales), articulando entidades públicas, sectores estratégicos y el Centro Nacional de Seguridad Digital. **AE 1.2.** Fortalecer el Centro Nacional de Seguridad Digital (CNSD) como nodo central de monitoreo, coordinación y respuesta nacional. **AE 1.4.** Desarrollar e integrar una plataforma nacional de gestión de incidentes de seguridad digital.	La PNTD promueve el uso de tecnologías exponenciales y servicios predictivos. La ENC complementa esta transformación mediante capacidades de monitoreo, gestión de incidentes, analítica avanzada e inteligencia artificial destinadas a anticipar amenazas de seguridad digital, contribuyendo a la resiliencia de los entornos donde operan dichos servicios.
	3.5. Implementar el estándar de datos para contrataciones abiertas en los procesos de contrataciones públicas.	**OE5.** Fortalecer la gobernanza y el marco normativo en ciberseguridad en las entidades de la administración pública	**AE 5.5.** Elaborar normas, lineamientos, directivas, guías o políticas para el uso de criptografía a efectos de proteger la confidencialidad, integridad y autenticidad de activos y objetos digitales.	La PNTD impulsa la apertura, intercambio y utilización de datos en las contrataciones públicas. La ENC complementa esta orientación mediante mecanismos destinados a proteger los datos durante su almacenamiento, procesamiento e intercambio entre plataformas o sistemas, permitiendo que la apertura de información se realice bajo condiciones de seguridad y confianza digital.
OP4. Fortalecer el talento digital en todas las personas.	**4.1.** Implementar mecanismos de desarrollo digital y productivo en áreas STEAM y tecnologías exponenciales, previstos en la Estrategia Nacional de Talento Digital, para todas las personas	**OE3.** Desarrollar una cultura nacional de ciberseguridad y sólidas capacidades operativas en el talento humano del sector público y la ciudadanía.	**AE 3.4.** Promover la investigación, el desarrollo tecnológico y la innovación en materia de ciberseguridad, mediante la articulación y coordinación de los actores del Sistema Nacional de Ciencia, Tecnología e Innovación – Sinacti.	La PNTD busca desarrollar capacidades en ciencia, tecnología e innovación. La ENC complementa esta orientación incorporando específicamente la investigación, desarrollo e innovación en ciberseguridad, contribuyendo a la formación de capacidades especializadas necesarias para el ecosistema digital.

PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Gobierno y Transformación Digital

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Objetivo Prioritario de la PNTD	Lineamiento PNTD	Objetivo Estratégico de la ENC	Acción Estratégica ENC	Sustento de la alineación
	haciendo especial énfasis en niñas			
	4.2. Transversalizar el aprovechamiento de las tecnologías exponenciales en el sistema educativo nacional, con énfasis en los grupos de especial protección	**OE3.** Desarrollar una cultura nacional de ciberseguridad y sólidas capacidades operativas en el talento humano del sector público y la ciudadanía.	**AE 3.1.** Promover la inclusión de la ciberseguridad en el sistema educativo nacional.	La PNTD plantea incorporar la dimensión digital de manera transversal en el sistema educativo. La ENC aterriza esta orientación en el componente específico de ciberseguridad mediante la incorporación de contenidos y actividades de prevención y atención de riesgos de ciberseguridad en el sistema educativo.
	4.3. Desarrollar las competencias digitales y de innovación en servidores públicos y ciudadanía para toda la vida.	**OE3.** Desarrollar una cultura nacional de ciberseguridad y sólidas capacidades operativas en el talento humano del sector público y la ciudadanía.	**AE 3.2.** Implementar programas de capacitación, especialización y certificación dirigidos a los servidores públicos. **AE 3.3** Fortalecer la asistencia técnica descentralizada a gobiernos regionales y locales.	La PNTD establece el desarrollo de competencias digitales para la ciudadanía y los servidores públicos. La ENC concretiza esta orientación mediante capacitación, especialización y certificación en ciberseguridad, así como asistencia técnica a gobiernos regionales y locales.
	4.4. Promover la innovación digital como criterio de desempeño en los servidores públicos.	**OE3.** Desarrollar una cultura nacional de ciberseguridad y sólidas capacidades operativas en el talento humano del sector público y la ciudadanía.	**AE 3.2.** Implementar programas de capacitación, especialización y certificación dirigidos a los servidores públicos. **AE 3.4.** Promover la investigación, el desarrollo tecnológico y la innovación en materia de ciberseguridad, mediante la articulación y coordinación de los actores del Sistema Nacional de Ciencia, Tecnología e Innovación – Sinacti.	La PNTD busca incorporar una cultura de innovación en el sector público. La ENC complementa dicha orientación fortaleciendo las capacidades especializadas de los servidores públicos e impulsando la investigación e innovación específicamente en ciberseguridad.
OP5. Consolidar la seguridad y confianza digital en la sociedad	**5.1.** Asegurar el adecuado funcionamiento del Sistema Nacional de Transformación Digital, elaborando y articulando las estrategias nacionales con énfasis en seguridad y confianza digital.	**OE5.** Fortalecer la gobernanza y el marco normativo en ciberseguridad en las entidades de la administración pública.	**AE 5.1.** Evaluar el marco normativo y modelo de gobernanza nacional vigente, con arreglo a los roles, responsabilidades, mecanismos de articulación entre los diferentes niveles de gobierno y sectores, y el nivel estratégico del Centro Nacional de Seguridad Digital; **AE 5.3.** Evaluar y fortalecer el modelo de rectoría en ciberseguridad y marco normativo a nivel nacional; **AE 5.6.** Incorporar en los Planes de Gobierno Digital el componente de ciberseguridad; Y, **AE 5.7.** Promover la integración progresiva de la ciberseguridad como un componente dentro de los Planes Operativos Institucionales (POI) y/o en las actualizaciones de los Planes Estratégicos Institucionales (PEI).	Esta constituye una de las vinculaciones más directas entre ambos instrumentos. La PNTD establece la seguridad y confianza digital como componente de la transformación digital; la ENC desarrolla dicha orientación mediante gobernanza, rectoría, marco normativo e incorporación de la ciberseguridad en los instrumentos de planificación pública.
	5.2. Fomentar una cultura de gestión de riesgos y confianza digitales, con énfasis en la protección de niños, niñas y adolescentes.	**OE6.** Desarrollar capacidades nacionales de gestión de riesgos digitales e inteligencia en ciberseguridad en las entidades del estado y sectores estratégicos; y, **OE3.** Desarrollar una cultura nacional de ciberseguridad y sólidas capacidades operativas en el talento humano del sector público y la ciudadanía.	**AE 6.1.** Implementar un modelo nacional de gestión de riesgos de ciberseguridad con enfoque sectorial; **AE 3.1.** Promover la inclusión de la ciberseguridad en el sistema educativo nacional; Y, **AE 3.2.** Implementar programas de capacitación, especialización y certificación dirigidos a los servidores públicos.	La PNTD plantea desarrollar una cultura de gestión de riesgos y confianza digital. La ENC operacionaliza esta orientación mediante un modelo nacional de gestión de riesgos y, desde el componente de cultura y capacidades, mediante educación, alfabetización digital y especialización en ciberseguridad.

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Objetivo Prioritario de la PNTD	Lineamiento PNTD	Objetivo Estratégico de la ENC	Acción Estratégica ENC	Sustento de la alineación
OP6. Garantizar el uso ético y adopción de las tecnologías exponenciales y la innovación en la sociedad.	6.1. Implementar espacios de innovación en tecnologías exponenciales con los integrantes del Sistema Nacional de Transformación Digital, en beneficio de los sectores productivos e industriales a nivel nacional	OE3. Desarrollar una cultura nacional de ciberseguridad y sólidas capacidades operativas en el talento humano del sector público y la ciudadanía; y, OE6. Desarrollar capacidades nacionales de gestión de riesgos digitales e inteligencia en ciberseguridad en las entidades del estado y sectores estratégicos.	AE 3.4. Promover la investigación, el desarrollo tecnológico y la innovación en materia de ciberseguridad, mediante la articulación y coordinación de los actores del Sistema Nacional de Ciencia, Tecnología e Innovación – Sinacti.; y, AE 6.5. Integrar capacidades nacionales de analítica avanzada e inteligencia artificial para la anticipación y análisis predictivo de amenazas de seguridad digital.	La PNTD promueve la innovación y adopción responsable de tecnologías exponenciales considerando privacidad, seguridad y uso ético de los datos. La ENC desarrolla el componente de ciberseguridad de esta orientación mediante investigación e innovación especializada y el uso de analítica avanzada e inteligencia artificial para anticipar amenazas.
	6.2 Articular la implementación de las intervenciones establecidas en las estrategias nacionales para la transformación digital.	OE5. Fortalecer la gobernanza y el marco normativo en ciberseguridad en las entidades de la administración pública; y, OE6. Desarrollar capacidades nacionales de gestión de riesgos digitales e inteligencia en ciberseguridad en las entidades del estado y sectores estratégicos.	AE 5.1. Evaluar el marco normativo y modelo de gobernanza nacional vigente, con arreglo a los roles, responsabilidades, mecanismos de articulación entre los diferentes niveles de gobierno y sectores, y el nivel estratégico del Centro Nacional de Seguridad Digital; AE 5.3. Evaluar y fortalecer el modelo de rectoría en ciberseguridad y marco normativo a nivel nacional; AE 5.6. Incorporar en los Planes de Gobierno Digital el componente de ciberseguridad; y, AE 6.1. Implementar un modelo nacional de gestión de riesgos de ciberseguridad con enfoque sectorial.	La PNTD plantea la articulación de las estrategias nacionales de transformación digital y que estas se implementen en entornos seguros y confiables. La ENC desarrolla específicamente la dimensión de ciberseguridad mediante mecanismos de gobernanza, rectoría, planificación y gestión de riesgos.
	6.3 Fortalecer mecanismos de medición y cooperación internacional para el desarrollo digital del país.	OE4. Consolidar la cooperación internacional y el intercambio de información sobre amenazas de seguridad digital.	AE 4.1. Consolidar la presencia multilateral en redes y foros internacionales de ciberseguridad e inteligencia de amenazas (threat intelligence); AE 4.2. Promover acuerdos, instrumentos e iniciativas de cooperación bilateral y multilateral en ciberseguridad; AE 4.5. Fortalecer mecanismos de intercambio seguro de información sobre amenazas digitales; y, AE 4.6. Promover un modelo de cooperación sostenible para la ciberseguridad nacional.	La PNTD reconoce la cooperación internacional como mecanismo para el desarrollo digital. La ENC aterriza esta dimensión en el ámbito específico de la ciberseguridad mediante participación internacional, acuerdos de cooperación, adopción de estándares e intercambio seguro de información sobre amenazas digitales.

Fuente: *Elaboración propia, sobre la base de la PNTD y la ENC..*

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

II. Matriz de Objetivos Estratégicos, Acciones Estratégica e Indicadores de la ENC

Objetivo Estratégico ENC	Acción estratégica ENC	Indicador de AE	Responsable del Indicador	Logro Esperado 2026	2027	2028	2029	2030
OE N.° 1: Fortalecer las capacidades nacionales de prevención, detección, respuesta y recuperación ante incidentes de seguridad digital en las entidades del ecosistema digital a nivel nacional	**AE 1.1** Consolidar una arquitectura nacional de ciberseguridad basada en un modelo SOC de SOCs e iSOC para redes OT (Redes Industriales), articulando entidades públicas, sectores estratégicos y el Centro Nacional de Seguridad Digital.	Número de entidades públicas priorizadas integradas al sistema de monitoreo del Centro Nacional de Seguridad Digital.	SGTD – PCM CNSD	0 (Periodo de preparación)	5	15	20	50
	AE 1.2 Fortalecer el Centro Nacional de Seguridad Digital (CNSD) como nodo central de monitoreo, coordinación y respuesta nacional.	Porcentaje de incidentes de seguridad digital gestionados por el Centro Nacional de Seguridad Digital dentro del plazo/protocolo definido.	SGTD – PCM CNSD	15%	25%	40%	55%	75%
	AE 1.3 Implementar y consolidar los CSIRT institucionales, priorizando proveedores de actividades críticas y gobiernos subnacionales (regionales y locales).	Porcentaje de entidades públicas priorizadas, incluyendo gobiernos regionales y locales, que cuentan con un CSIRT institucional operativo e integrado.	SGTD – PCM EP	15%	35%	55%	75%	85%
	AE 1.4. Desarrollar e integrar una plataforma nacional de gestión de incidentes de seguridad digital.	Porcentaje de entidades públicas priorizadas integradas a la plataforma nacional de gestión de incidentes de seguridad digital.	SGTD – PCM CNSD	0 % (Periodo de preparación)	10%	15%	20%	30%
	AE 1.5 Institucionalizar simulacros nacionales de ciberseguridad y ejercicios de respuesta frente a incidentes de seguridad digital.	Porcentaje de entidades públicas participantes con ejercicios nacionales de ciberseguridad concluidos.	SGTD – PCM CNSD	20%	40%	45%	50%	55%
OE N.° 2: Fortalecer la ciberseguridad de los activos críticos nacionales, las actividades críticas y los servicios	**AE 2.1** Identificar, evaluar e incorporar Activos Críticos Nacionales al Inventario Nacional y fortalecer la evaluación de riesgos.	Porcentaje del Inventario Nacional de Activos Críticos Nacionales con evaluación de riesgos de seguridad digital completada por la Dirección Nacional de Inteligencia.	DINI	6%	12%	18%	24%	30%
	AE 2.2 Identificar, clasificar, registrar y proteger las actividades críticas y los servicios públicos esenciales.	Porcentaje de actividades críticas y servicios públicos esenciales registrados con vinculación documentada y con medidas de protección en	SGTD	5%	15%	30%	45%	60%

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Objetivo Estratégico ENC	Acción estratégica ENC	Indicador de AE	Responsable del Indicador	Logro Esperado 2026	2027	2028	2029	2030
públicos esenciales frente a amenazas de seguridad digital.		seguridad digital implementadas conforme a los lineamientos del ente rector.						
	AE 2.3 Fortalecer medidas para la gestión de riesgos de seguridad digital respecto de operadores de activos críticos nacionales, así como de las actividades críticas y los servicios públicos esenciales.	Porcentaje de operadores de Activos Críticos Nacionales, de actividades críticas y los Servicios Públicos Esenciales que cuentan con un Sistema de Gestión de Seguridad de la Información (SGSI) implementado y, en sus entornos de tecnología operativa, con la segmentación en zonas y conductos y los niveles de seguridad correspondientes a la gestión de riesgos industriales, conforme a los lineamientos técnicos aplicables.	SGTD – PCM DINI	10%	30%	55%	60%	70%
	AE 2.4 Implementar programas nacionales de gestión de vulnerabilidades, pruebas de intrusión y evaluación continua.	Porcentaje de proveedores de actividades críticas y entidades públicas que ejecutan pruebas de vulnerabilidad en el periodo de análisis.	EP SGTD – PCM	15%	30%	55%	60%	75%
	AE 2.5 Implementar controles de seguridad en entornos industriales.	Porcentaje de operadores con redes IT/OT que han aplicado controles de seguridad industrial conforme a estándares internacionales en la materia y lineamientos de la entidad competente.	SGTD	1%	15%	25%	35%	45%
	AE 2.6 Desplegar y fortalecer capacidades operativas de monitoreo, detección, contención y respuesta temprana frente a amenazas e incidentes de seguridad digital, mediante la implementación de tecnologías especializadas.	Porcentaje de entidades públicas priorizadas que cuentan con capacidades operativas de monitoreo, detección y respuesta temprana implementadas.	SGTD – PCM EP	0 % (Periodo de preparación)	5%	10%	15%	20%
OE N.° 3: **Desarrollar una cultura nacional de ciberseguridad y sólidas capacidades**	**AE 3.1** Promover la inclusión de la ciberseguridad en el sistema educativo nacional.	Porcentaje de instituciones educativas que implementan contenidos o actividades para el fortalecimiento de competencias vinculadas a la prevención y atención de riesgos de ciberseguridad, en el marco del Currículo Nacional de la Educación Básica.	MINEDU SGTD – PCM	0 % (Periodo de preparación)	5%	10%	15%	20%

PRESIDENCIA DEL CONSEJO DE MINISTROS SGTD Secretaría de Gobierno y Transformación Digital

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Objetivo Estratégico ENC	Acción estratégica ENC	Indicador de AE	Responsable del Indicador	Logro Esperado 2026	2027	2028	2029	2030
operativas en el talento humano del sector público y la ciudadanía.	**AE 3.2** Implementar programas de capacitación, especialización y certificación dirigidos a los servidores públicos.	Número de servidores públicos que aprobaron programas de capacitación, especialización y/o certificación en ciberseguridad incorporados en los Planes de Desarrollo de las Personas (PDP) de las entidades públicas.	SGTD – PCM	0 servidores (Periodo de preparación)	500 servidores	1000 servidores	1500 servidores	1800 servidores
	AE 3.3 Fortalecer la asistencia técnica descentralizada a gobiernos regionales y locales.	Porcentaje de gobiernos regionales y locales priorizados asistidos técnicamente en materia de ciberseguridad.	SGTD – PCM CNSD	GR: 10% GL: 5%	GR: 20% GL: 10%	GR: 35% GL: 15%	GR: 50% GL: 25%	GR: 60% GL: 30%
	AE 3.4 Promover la investigación, el desarrollo tecnológico y la innovación en materia de ciberseguridad, mediante la articulación y coordinación de los actores del Sistema Nacional de Ciencia, Tecnología e Innovación – Sinacti.	Número de iniciativas de promoción, articulación o fortalecimiento de la investigación, desarrollo tecnológico e innovación en materia de ciberseguridad implementadas en el marco del SINACTI.	SGTD – PCM CONCYTEC	0 % (Periodo de preparación)	2%	4%	7%	10%
OE N.° 4: **Consolidar la cooperación internacional y el intercambio de información sobre amenazas de seguridad digital.**	**AE 4.1** Consolidar la presencia multilateral en redes y foros internacionales de ciberseguridad e inteligencia de amenazas (threat intelligence).	Número de participaciones del país en redes y foros internacionales de ciberseguridad e inteligencia de amenazas efectivamente realizadas.	SGTD – PCM	0 (Periodo de preparación)	2	3	4	5
	AE 4.2 Promover acuerdos, instrumentos e iniciativas de cooperación bilateral y multilateral en ciberseguridad.	Número de acuerdos, instrumentos o iniciativas internacionales de cooperación en ciberseguridad iniciados formalmente, suscritos o implementados	MRE	0 (Periodo de preparación)	1	2	3	4
	AE 4.3 Participar y organizar ejercicios internacionales en materia de ciberseguridad en coordinación con la entidad competente, según corresponda.	Número de ejercicios internacionales de ciberseguridad en los que el país participa u organiza.	SGTD – PCM CNSD	0 (Periodo de preparación)	1	2	2	2
	AE 4.4 Adoptar, promover y difundir normas técnicas internacionales aplicables a la gestión de la ciberseguridad, en coordinación con el INACAL y las entidades y/o autoridades competentes.	Número de normas técnicas internacionales de ciberseguridad priorizadas y adoptadas como Normas Técnicas Peruanas	SGTD – PCM INACAL	0 (Periodo de preparación)	1	2	3	4

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Objetivo Estratégico ENC	Acción estratégica ENC	Indicador de AE	Responsable del Indicador	Logro Esperado 2026	2027	2028	2029	2030
	AE 4.5 Fortalecer mecanismos de intercambio seguro de información sobre amenazas digitales.	Número de intercambios de información sobre amenazas digitales realizados	SGTD – PCM	0 Intercambios (Periodo de preparación)	5 intercambios	10 intercambios	15 intercambios	20 intercambios
	AE 4.6 Promover un modelo de cooperación sostenible para la ciberseguridad nacional.	Número de iniciativas de cooperación internacional en ciberseguridad promovidas o gestionadas.	SGTD – PCM	0 (Periodo de preparación)	3	5	7	10
OE N.° 5: **Fortalecer la gobernanza y el marco normativo en ciberseguridad en las entidades de la administración pública.**	**AE 5.1** Evaluar el marco normativo y modelo de gobernanza nacional vigente, con arreglo a los roles, responsabilidades, mecanismos de articulación entre los diferentes niveles de gobierno y sectores, y el nivel estratégico del Centro Nacional de Seguridad Digital.	Porcentaje de avance en la revisión y propuesta de actualización del marco normativo y modelo de gobernanza nacional en ciberseguridad.	SGTD – PCM	0 % (Periodo de preparación)	50%	100%		
	AE 5.2 Fortalecer mecanismos de supervisión y monitoreo en ciberseguridad en las entidades de la Administración Pública.	Porcentaje de entidades públicas priorizadas con verificación de cumplimiento en materia de ciberseguridad.	SGTD – PCM CNSD	0 % (Periodo de preparación)	15%	30%	45%	60%
	AE 5.3 Evaluar y fortalecer el modelo de rectoría en ciberseguridad y marco normativo a nivel nacional.	Número de instrumentos normativos, lineamientos o mecanismos aprobados para fortalecer el modelo nacional de rectoría y gobernanza en ciberseguridad.	SGTD – PCM	0 instrumentos normativos aprobados. (Periodo de preparación)	1 instrumento normativo aprobado	1 instrumento normativo aprobado	1 instrumento normativo aprobado	2 instrumentos normativos aprobados
	AE 5.4 Fortalecer el rol estratégico de los Oficiales de Seguridad y Confianza Digital en las entidades públicas.	Porcentaje de entidades públicas priorizadas con Oficial de Seguridad y Confianza Digital formalmente designado	SGTD – PCM CNSD	0 % (Periodo de preparación)	50%	50%	70%	80%
	AE 5.5 Elaborar normas, lineamientos, directivas, guías o políticas para el uso de	Número de normas, lineamientos, directivas, guías o políticas aprobadas para el uso de criptografía	SGTD – PCM	0	0	1	2	4

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

CONSORCIO DE GESTORES PÚBLICOS PERÚ

Objetivo Estratégico ENC	Acción estratégica ENC	Indicador de AE	Responsable del Indicador	Logro Esperado 2026	2027	2028	2029	2030
	criptografía a efectos de proteger la confidencialidad, integridad y autenticidad de activos y objetos digitales.	aplicables a la Infraestructura Oficial de Firma Electrónica (IOFE) y servicios de confianza digital; así como al almacenamiento, procesamiento e intercambio de datos e información entre plataformas o sistemas de información.	INDECOPI	(Periodo de preparación)	(Periodo de preparación)	norma, lineamiento, directiva, guía o política aprobada	normas, lineamientos, directivas, guías o políticas aprobadas	normas, lineamientos, directivas, guías o políticas aprobadas
	AE 5.6 Incorporar en los Planes de Gobierno Digital el componente de ciberseguridad.	Porcentaje de Planes de Gobierno Digital (PGD) aprobados con componentes de ciberseguridad incorporados conforme a los lineamientos del ente rector.	EP (Comités de Gobierno y Transformación Digital y Oficial de Seguridad y Confianza Digital)	35%	45%	60%	75%	90%
	AE 5.7. Promover la integración progresiva de la ciberseguridad como un componente dentro de los Planes Operativos Institucionales (POI) y/o en las actualizaciones de los Planes Estratégicos Institucionales (PEI).	Porcentaje de entidades públicas que incorporan objetivos, indicadores, metas en materia de ciberseguridad en los Planes Operativos Institucionales (POI) y/o en las actualizaciones de los Planes Estratégicos Institucionales (PEI).	EP SGTD – PCM CEPLAN	0 % (Periodo de preparación)	0 % (Periodo de preparación)	30%	40%	60%
OE N.° 6: **Desarrollar capacidades nacionales de gestión de riesgos digitales e inteligencia en ciberseguridad en las entidades del estado y sectores estratégicos.**	**AE 6.1.** Implementar un modelo nacional de gestión de riesgos de ciberseguridad con enfoque sectorial.	Número de sectores con el modelo nacional de gestión de riesgos de ciberseguridad adoptado.	SGTD – PCM CNSD	0 Sectores (Periodo de preparación)	5 sectores	7 sectores	9 sectores	11 sectores
	AE 6.2. Desarrollar una plataforma nacional de inteligencia de amenazas digitales (Threat Intelligence).	Plataforma Nacional de Inteligencia de Amenazas Digitales implementada y operativa.	SGTD – PCM CNSD			Plataforma implementada y operativa		
	AE 6.3. Establecer mecanismos de intercambio estructurado de información (STIX/TAXII).	Plataforma de intercambio de información sobre ciberamenazas implementada y operativa.	SGTD – PCM CNSD					Una plataforma implementada y operativa
	AE 6.4. Generar informes/reportes/documentos periódicos de riesgos y amenazas para la toma de decisiones estratégicas.	Número de informes/reportes/documentos elaborados para la toma de decisiones estratégicas.	SGTD – PCM CNSD	1 informe	2 informes	3 informes	4 informes	5 informes
	AE 6.5. Integrar capacidades nacionales de analítica avanzada e inteligencia artificial para la anticipación y análisis	Porcentaje de alertas de amenazas generadas mediante capacidades de analítica avanzada e inteligencia artificial.	SGTD – PCM CNSD	0 % (Periodo de preparación)	5%	15%	20%	25%

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe

Objetivo Estratégico ENC	Acción estratégica ENC	Indicador de AE	Responsable del Indicador	Logro Esperado				
				2026	2027	2028	2029	2030
	predictivo de amenazas de seguridad digital							

Fuente: *Elaboración propia, sobre la base de la ENC..*

SHA-256 78b7935d2b04 · verificado 2026-11-25 · gestorespublicos.pe