PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Gobierno del Perú

Propuesta Estrategia Nacional de Ciberseguridad

Perú, 2026-2028

CONTENIDO

COMPENDIO DE FIGURAS

ACRÓNIMOS Y SIGLAS

AEC	:	Acción Estratégica de Ciberseguridad
AURORA	:	Programa Nacional para la Prevención y Erradicación de la Violencia contra las Mujeres e Integrantes del Grupo Familiar
ANA	:	Autoridad Nacional del Agua
APN	:	Autoridad Portuaria Nacional
BCRP	:	Banco Central de Reserva del Perú
CAN	:	Comisión Alto Nivel contra la Corrupción
CNPD	:	Comité de Alto nivel por un Perú Digital, Innovador y Competitivo
CCL	:	Cámara de Comercio de Lima
CENEPRED	:	Centro Nacional de Estimación, Prevención y Reducción del Riesgo
CEPLAN	:	Centro Nacional de Planeamiento Estratégico
CERT	:	(Computer Emergency Response Team) Equipo de Respuesta ante Emergencias Informáticas.
CSIRT	:	(Computer Security Incident Response Team), Equipo de Respuesta ante Incidentes de Seguridad Informática.
CNSD	:	Centro Nacional de Seguridad Digital
CNID	:	Centro Nacional de Innovación Digital e Inteligencia Artificial
COES	:	Comité de Operación Económica del Sistema Interconectado Nacional
COEN		Centro de Emergencia Nacional.
CONADIF	:	Consejo Nacional de Desarrollo de Fronteras e Integración Fronteriza
CONCYTEC	:	Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica
CTI	:	Ciencia, tecnología e innovación tecnológica
ESNACIB	:	Estrategia Nacional de Ciberseguridad – Perú, 2026-2028.
ESSALUD	:	Seguro Social de Salud
FBI	:	Federal Bureau of Investigation
FMI	:	Fondo Monetario Internacional
FONAFE	:	Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado
GEI	:	Gases de Efecto Invernadero
GEOPERU	:	Plataforma Nacional Georeferenciada GEOPERU
GOB.PE	:	Plataforma Digital Única del Estado para Orientación al Ciudadano
I+D+I	:	Investigación, desarrollo e innovación
IGM	:	Índice de Gobernanza Mundial
INAIGEM	:	Instituto Nacional de Investigación en Glaciares y Ecosistemas de Montaña
INGEI	:	Inventario Nacional de Gases de Efecto Invernadero

INEI	:	Instituto Nacional de Estadística e Informática
INDECI	:	Instituto Nacional de Defensa Civil
INDECOPI	:	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad intelectual.
OEGC	:	Objetivo Estratégico General de Ciberseguridad.
OEEC	:	Objetivo Estratégico Especifico de Ciberseguridad
IPE	:	Instituto Peruano de Economía
MEF	:	Ministerio de Economía y Finanzas
MIDIS	:	Ministerio de Desarrollo e Inclusión Social
MIMP	:	Ministerio de la Mujer y Poblaciones Vulnerables
MINCETUR	:	Ministerio de Comercio Exterior y Turismo
MINCUL	:	Ministerio de Cultura
MIDAGRI	:	Ministerio de Desarrollo Agrario y Riego
MINDEF	:	Ministerio de Defensa
MINAM	:	Ministerio del Ambiente
MINDEF	:	Ministerio de Defensa
MINEDU	:	Ministerio de Educación
MINEM	:	Ministerio de Energía y Minas
MININTER	:	Ministerio del Interior
MINJUSDH	:	Ministerio de Justicia y Derechos Humanos
MINSA	:	Ministerio de Salud
MIPYME	:	Micro, pequeña y mediana empresa
MOF	:	Manual de Organización y Funciones
MRE	:	Ministerio de Relaciones Exteriores
MTC	:	Ministerio de Transportes y Comunicaciones
MTPE	:	Ministerio de Trabajo y Promoción del Empleo
MYPE	:	Micro y pequeña empresa
OCDE	:	Organización para la Cooperación y el Desarrollo Económico
OCI	:	Órgano de Control Institucional
OCMA	:	Oficina de Control de la Magistratura
OEA	:	Organización de los Estados Americanos
OEFA	:	Organismo de Evaluación y Fiscalización Ambiental
OEI	:	Objetivo Estratégico Institucional
ONU	:	Organización de las Naciones Unidas
PCM	:	Presidencia del Consejo de Ministros
PEDN	:	Plan Estratégico de Desarrollo Nacional
PESEM	:	Plan Estratégico Sectorial Multianual

PEI	:	Plan Estratégico Institucional
PIDE	:	Plataforma Nacional de Interoperabilidad
PNGD	:	Plataforma Nacional de Gobierno Digital
PNTD	:	Proceso Nacional de Transformación Digital
POI	:	Plan Operativo Institucional
PRONIED	:	Programa Nacional de Infraestructura Educativa
PRONIS	:	Programa Nacional de Inversiones en Salud
PYME	:	Pequeña y mediana empresa
ROF	:	Reglamento de Organización y Funciones
SEDAPAL	:	Servicio de Agua Potable y Alcantarillado de Lima
SENAMHI	:	Servicio Nacional de Meteorología e Hidrología
SERFOR	:	Servicio Nacional Forestal y de Fauna Silvestre
SERVIR	:	Autoridad Nacional del Servicio Civil
SUSALUD	:	Superintendencia Nacional de Salud
SGP	:	Secretaría de Gestión Pública
SIGERSOL	:	Sistema de Información de Gestión de Residuos Sólidos
SINAPLAN	:	Sistema Nacional de Planeamiento Estratégico
SGTD	:	Secretaría de Gobierno y Transformación Digital.
SIS	:	Sistema Integral de Salud
SOAR	:	Security Orchestration, Automation, and Response (Orquestación, Automatización y Respuesta en Seguridad)
SUNASS	:	Superintendencia Nacional de Servicios de Saneamiento
SUNAT	:	Superintendencia de Administración Tributaria
SUTRAN	:	Superintendencia de Transporte Terrestre de Personas, Carga y Mercancías
TIC	:	Tecnologías de la información y la comunicación o tecnologías digitales
UE	:	Unión Europea
UIT	:	Unión Internacional de Telecomunicaciones (ITU en Inglés)

INTRODUCCIÓN

En los últimos años, los habitantes del planeta han experimentado los beneficios del crecimiento y de la difusión de las tecnologías de la información y comunicaciones (TIC), así como de las oportunidades socioeconómicas y políticas relacionadas. La vertiginosa evolución del ciberespacio ha transformado la manera en la que se interactúa en el ámbito personal, social y económico, sin embargo, a medida que las TIC evolucionan y aumenta la interconexión global impulsando la Transformación Digital, surgen también ciberamenazas cada vez más sofisticadas. El incremento sostenido de ciberataques refleja esta realidad, posicionándose como un desafío prioritario para gobiernos, entidades y ciudadanos en todo el mundo.

Los ciberataques, son una inminencia real que, en pocas horas, pueden devastar la economía, las instituciones y las estructuras de los países más vulnerables. El avance de dicha interconexión global aumenta los riesgos, que, en manos de ciberdelincuentes, ciberterroristas u otros actores maliciosos, pueden convertirse en peligros inmediatos. Estos individuos a menudo exploran nuevas herramientas informáticas, que provienen o se sostienen de tecnologías emergentes como la Inteligencia Artificial (IA), la computación cuántica, entre otras, sin considerar las consecuencias destructivas que pueden generar con su mal uso o interacción. Ante estas amenazas cibernéticas que ponen en riesgo el bienestar y los sistemas democráticos, se requiere con urgencia la implementación de marcos normativos, de estrategias y herramientas para proteger los intereses de los países. Esto implica, desarrollar capacidades clave en áreas como prevención, defensa, detección, análisis, investigación, resiliencia, recuperación y respuesta ante incidentes, así como gestionar los riesgos asociados en la búsqueda de una mejora continua.

Bajo este panorama, y considerando la definición de Seguridad Digital propuesta por la OCDE (2022) tal cual se detalla: *"La seguridad digital es la dimensión[1] económica y social de la Ciberseguridad. Es esencial para mantener la confianza en nuestras economías, cada vez más dependientes de la tecnología digital, y para aumentar la resiliencia en un mundo sujeto a crecientes conflictos geopolíticos y ciberdelitos"*[2], denota que la Ciberseguridad emerge como un cimiento ineludible, ya que garantiza la protección de infraestructuras críticas, datos sensibles y la continuidad operativa en un ecosistema cada vez más interdependiente. De este modo, contribuye de manera decisiva a preservar la confianza tanto en el ámbito social como económico.

[1] Dimensión: Del lat. dimensio, -ōnis. f. Aspecto o faceta de algo.

[2] Enlace web referido a la denominación de "Seguridad Digital" según la OCDE: https://www.oecd.org/en/topics/digital-security.html

Asimismo, es fundamental que los países asuman la responsabilidad de enfrentar las diversas ciberamenazas que ponen en riesgo los activos de información digitales en el ciberespacio; esto conlleva a que para poder aprovechar los beneficios, superar los desafíos de la Transformación Digital y así lograr una gobernanza efectiva y segura, es necesario que los países alineen el desarrollo de infraestructuras y servicios basados en las TIC, con una Estrategia de Ciberseguridad, la cual tiene que ser actualizada de forma continua. Otras agrupaciones, como la Organización de las Naciones Unidas (ONU), Unión Internacional de Telecomunicaciones (UIT), el Consejo de Europa, la Alianza Global para la Confianza Digital, la Organización para la Cooperación y el Desarrollo Económico (OCDE), el Foro Económico Mundial (WEF), la Agencia para la Ciberseguridad de la Unión Europea (ENISA), la Asociación de Naciones del Sudeste Asiático (ASAEAN), la Agencia Internacional para la Energía Atómica, la OEA, entre otras, han desarrollado marcos normativos y estrategias para proteger la información digital.

Ante este escenario global, Perú, como parte activa de la comunidad internacional, prioriza la Ciberseguridad y su interrelación con la seguridad digital, reconociendo su impacto estratégico principalmente en el desarrollo económico, social y político del país. Por ello, desde la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno y Transformación Digital[3] (SGTD – PCM)[4], se promueve un marco normativo integral con herramientas y recursos de gestión, que incluyen estrategias y mecanismos diseñados para garantizar un entorno digital seguro y confiable para el Estado y los ciudadanos.

En consecuencia, la SGTD – PCM, en coordinación con el Centro Nacional de Seguridad Digital[5] (CNSD)[6], con la colaboración y consenso de las entidades del Estado Peruano, sector privado, la Academia y de la ciudadanía, ha elaborado la "Estrategia Nacional de Ciberseguridad. Perú 2026-2028." (ESNACIB), constituyendo el principal instrumento estratégico del Estado Peruano respecto a esta temática, orientado a alcanzar un ciberespacio seguro, resiliente y confiable, crucial para habilitar y proteger el desarrollo sostenible y la competitividad del país en el contexto de la Transformación Digital. Se alinea con los componentes del Índice Global de Ciberseguridad (GCI) que promueve la Unión Internacional de Telecomunicaciones (UIT) de la Organización de las

[3] *"Artículo 8.- Ente Rector en Materia de Gobierno Digital"* del *"Capitulo I. Gobierno Digital"* del *"Título II. Gobierno Digital"* del "Decreto Legislativo Nº1412. Decreto Legislativo que aprueba la Ley de Gobierno Digital" y el *"Artículo 5. Ente Rector del Marco de Confianza Digital"* y el *"Artículo 6. Atribuciones del Ente Rector"* del *"Capítulo II: Marco de Confianza Digital"* del "Decreto de Urgencia Nº 007-2020. Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento."

[4] La Secretaría de Gobierno y Transformación Digital (SGTD) tiene a cargo a la "Subsecretaría de Política y Regulación Digital", la "Subsecretaria de Servicios e Innovación Digital" y la "Subsecretaría de Tecnologías y Seguridad Digital" Según el Reglamento de Organización y Funciones de la PCM, aprobado por "Resolución Ministerial N° 224-2023-PCM"

[5] *"Artículo 7.- Centro Nacional de Seguridad Digital"* del *"Capitulo II. Marco de Confianza Digital"* del "Decreto de Urgencia Nº 007-2020. Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento."

[6] El Centro Nacional de Seguridad Digital (CNSD), actualmente está adscrita a la "Subsecretaría de Tecnologías y Seguridad Digital" de la SGTD - PCM.

Naciones Unidas (ONU), mediante sus pilares establecidos, con los Objetivos de Desarrollo Sostenible (ODS) de la ONU, el Marco de Seguridad Digital de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), todo ello sustentada en el marco normativo peruano vigente que incluye la Constitución Política del Perú, Ley de Gobierno Digital (Decreto Legislativo Nº 1412) y su reglamento (Decreto Supremo Nº 029-2021-PCM), con la Ley de Protección de datos personales y su reglamento, Ley de Ciberdefensa y su reglamento así como el Marco de Confianza Digital (Decreto de Urgencia Nº 007-2020), con la visión del Perú al 2050, las diversas Políticas de Estado Peruano[7] 9, 18, 20 y 35 en su Acuerdo Nacional y con los principales documentos de gestión como la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030, la Política Nacional de Transformación Digital al 2030, con el Plan Estratégico de Desarrollo Nacional al 2050 y el Plan Estratégico Sectorial Multianual – PESEM 2024-2030 - Sector PCM. De igual forma, se destaca el panorama actual de la Ciberseguridad a nivel global y en el contexto nacional, A través de este enfoque integral, la ESNACIB responde de manera proactiva a los crecientes desafíos y oportunidades de la era digital.

La ESNACIB se estructura en cuatro secciones: "*I. Contexto General, II. Aspectos Generales. III. Situación actual de la Ciberseguridad y alineación de la ESNACIB con las principales políticas internacionales y marcos: normativo y de gobernanza del país. IV. De la Estrategia Nacional de Ciberseguridad (ESNACIB)"*, con el fin de tener un enfoque holístico, generando una adecuada salvaguarda de la información en el entorno digital como nación, asegurando así una protección efectiva y fomentando la confianza digital necesaria en el entorno actual.

Impulsado por el liderazgo del Estado peruano y la activa participación de todos los actores del ecosistema digital nacional[8], la ESNACIB, busca consolidar un Perú ciberseguro, resiliente y confiable, promoviendo un entorno digital inclusivo que genere oportunidades para la ciudadanía, el sector productivo y las instituciones públicas y privadas. Su propósito central es fortalecer las capacidades de Ciberseguridad del país, coadyuvando a proteger su soberanía digital. Finalmente, la ESNACIB contribuye al fortalecimiento de una sociedad digital segura, impulsando el bienestar y el progreso integral del país en el contexto del Gobierno y la Transformación Digital.

SECRETARIA DE GOBIERNO Y TRANSFORMACIÓN DIGITAL
PRESIDENCIA DEL CONSEJO DE MINISTROS – PERÚ

[7] Políticas del Estado Peruano del Acuerdo Nacional que se alinean con la ESNACIB: *"9. Política de Seguridad Nacional", "18. Búsqueda de la competitividad, productividad y formalización de la actividad económica", "20. Desarrollo de la ciencia y la tecnología" y la "35. Sociedad de la Información y Sociedad del Conocimiento"*

[8] El ecosistema digital nacional, lo conforman el sector público, sector privado, la academia y sociedad civil.

I. CONTEXTO GENERAL

1.1. CIBERSEGURIDAD Y SU RELACIÓN CON EL MARCO DE LA SEGURIDAD DIGITAL EN EL PERÚ

En el actual contexto de la acelerada Transformación Digital, el Perú experimenta profundos cambios en su actividad social, económica y gubernamental. En este escenario, **la Ciberseguridad se consolida como un cimiento estratégico** para la protección del entorno digital nacional y una condición determinante para consolidar una sociedad digital que sea accesible, inclusiva, confiable y generadora de oportunidades.

Siguiendo el enfoque adoptado por la **Organización para la Cooperación y el Desarrollo Económicos (OCDE)**, se reconoce que la **Seguridad Digital constituye una dimensión clave dentro del marco más amplio de la Ciberseguridad**[9] (OCDE, 2022), en tanto contribuye directamente a la estabilidad y confianza en los sistemas sociales y económicos digitales. Así, la Ciberseguridad no solo implica medidas técnicas, sino también capacidades institucionales para gestionar riesgos sociales, económicos y gubernamentales en el entorno digital.

Figura. 1. Seguridad Digital, aspectos económicos y sociales de la Ciberseguridad

Nota: Adaptada al español por la SGTD – PCM, fuente: OECD Policy Framework On Digital Security. Pg. 12.
Enlace Web: https://www.oecd.org/en/publications/oecd-policy-framework-on-digital-security_a69df866-en.html

La OCDE define la Seguridad Digital como el conjunto de principios, políticas, normativas y herramientas destinadas a gestionar los riesgos digitales que afectan a la actividad económica, la interacción social y el bienestar de los ciudadanos. **Esta dimensión de la Ciberseguridad**

[9] Enlace web: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf

es asumida en el Perú a través del Decreto de Urgencia N° 007-2020, que establece el Marco de Confianza Digital, el cual considera la protección de derechos, activos e intereses en el ciberespacio como una responsabilidad transversal del Estado, dicho decreto se articula con el **Decreto de Urgencia Nº006-2020. Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital,** en el Marco del Gobierno y la Transformación Digital. También, en concordancia con este enfoque, dentro del marco legal peruano, lo precedido se sustenta en la **Ley N.º 30999, Ley de Ciberdefensa**, que regula la protección de infraestructuras críticas de información, así como el **Decreto Legislativo N.º 1412 que aprueba la Ley de Gobierno Digital,** junto con el **Decreto Supremo Nº 029-2021-PCM que reglamenta dicha ley**, dicho marco normativo, busca impulsar la incorporación de las tecnologías digitales en los servicios ofrecidos por las entidades públicas en favor de la reactivación económica de la nación, fortaleciendo las instituciones públicas y promoviendo el respeto de los derechos fundamentales en el ámbito digital.

1.2. FINALIDAD

El presente documento establece la Estrategia Nacional de Ciberseguridad para la República del Perú (ESNACIB), cuyo horizonte es del 2026-2028, tiene por finalidad establecer las iniciativas trazando el camino para avanzar en dirección a un país ciberseguro, fomentando la preparación necesaria para interactuar en el Ciberespacio, con los niveles adecuados de seguridad, desarrollar la resiliencia frente a posibles ciberataques, proteger nuestras infraestructuras críticas y activos de información digitales, así como promover una reflexión profunda sobre la importancia de la Ciberseguridad para el país.

1.3. ALCANCE

Este documento establece las directrices para implementar una Estrategia Nacional de Ciberseguridad, orientada a proteger a los activos de información digitales del país en el ciberespacio, garantizando la confidencialidad, integridad y disponibilidad de la información. Su alcance, abarca la seguridad de infraestructuras críticas, datos sensibles y servicios digitales esenciales, buscando generar conciencia cibernética, fortaleciendo la confianza de los usuarios en el ecosistema digital, contribuyendo al desarrollo socioeconómico y fomentando la cooperación público-privada e internacional, alineada con estándares y buenas prácticas globales para un ecosistema digital seguro y resiliente.

1.4. ÁMBITO DE APLICACIÓN

La ESNACIB está diseñada para ser implementada por el ecosistema digital peruano, siendo de cumplimiento obligatorio para las entidades del sector público en todos los niveles de gobierno (nacional, regional y local) de forma progresiva y valorada por el sector privado, la academia, la sociedad civil y por la ciudadanía en general, con el fin de fortalecer la protección y la capacidad de respuesta ante ciberamenazas, promover la inclusión de la Ciberseguridad en la educación, la investigación e innovación (I+D+I) y generar conciencia en la población sobre los riesgos y buenas prácticas en el entorno digital.

1.5. COMPONENTES DE LA ESTRATEGIA

La ESNACIB tiene los siguientes componentes:

Figura. 2. Componentes claves de la ESNACIB

Nota: Elaboración propia

1.6. REVISIÓN DE LA ESTRATEGIA

La ESNACIB tiene un horizonte de tres años. No obstante, durante el último año de su vigencia, se contempla su revisión con el propósito de actualizar o generar nuevo contenido o cuando surjan cambios estratégicos, de gestión o normativos que resulten relevantes en el ámbito de la Ciberseguridad, ya sea a nivel nacional o internacional de la que esté sujeta.

II. ASPECTOS GENERALES REFERIDOS A LA CIBERSEGURIDAD

2.1. DEFINICIÓN DE CIBERSEGURIDAD

El término "Ciberseguridad" ha adquirido múltiples definiciones y connotaciones como resultado de su evolución constante frente a los desafíos del entorno digital. No obstante, antes de establecer su definición actual, resultó fundamental revisar su definición en el marco normativo peruano, por ende, en el literal h) del "Artículo 3. Definiciones" del "Capitulo I. Disposiciones Generales" del Decreto de Urgencia Nº 007-2020[10], se 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(…)".*

Asimismo, dicha definición se relaciona con el marco de la **"Seguridad Digital",** establecido en la Ley de Gobierno Digital mediante el Decreto Legislativo Nº 1412[11], particularmente en sus artículos: 30° y 33° este último, en concordancia con la "Seguridad de la Información" de acuerdo al *"Capítulo VI: Seguridad Digital" del "Título II. Gobierno Digital"* de la mencionada ley.

En ese contexto, reconociendo la importancia de lo ya expuesto, sin perjuicio de lo que se añade, para los propósitos de este documento, conforme a lo establecido por el estándar internacional "ISO/IEC 27032:2023: Ciberseguridad - Directrices para la Seguridad en Internet (segunda edición)"[12] y fundamentado en los lineamientos de la Unión Internacional de Telecomunicaciones (UIT)[13], se presenta la actualización de la definición de "Ciberseguridad", tal y como se expresa:

"Conjunto de políticas, directrices, metodologías, mejores prácticas, programas de formación, acciones, herramientas y/o soluciones de gestión de riesgos, garantías y tecnologías, ***diseñadas o que pueden utilizarse para proteger la disponibilidad, integridad y confidencialidad de los activos de información digitales conectados****. Estos activos, que*

[10] Decreto de Urgencia Nº 007-2020. Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. Enlace Web: https://cdn.www.gob.pe/uploads/document/file/2790485/Decreto%20de%20Urgencia%20N%C2%BA%20007-2020.pdf?v=1643322610

[11] Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital. Enlace Web: https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf?v=1566312763

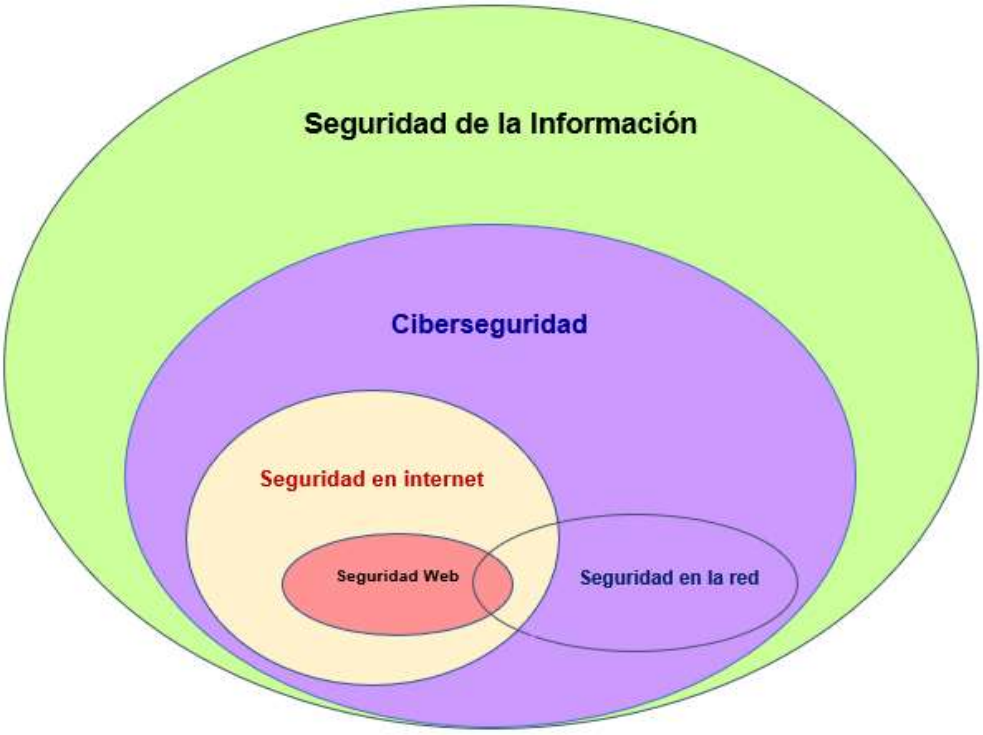
[12] Adaptada en nuestro país mediante la Resolución Directoral N° 017-2024-INACAL/DN, Aprueban Normas Técnicas Peruanas sobre hortalizas, Ciberseguridad y otras. NTP ISO/IEC 27032:2024: Ciberseguridad. Directrices para la seguridad en Internet. 1ª Edición. Vigente desde el 12 de setiembre de 2024.

[13] "Guía para la elaboración de una estrategia nacional de Ciberseguridad - Participación estratégica en la Ciberseguridad" de la UIT. Enlace Web: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf

pertenecen al gobierno, entidades u organizaciones de los diferentes sectores y ciudadanos, abarcan dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y datos del entorno digital."

Su representación, quedaría de la siguiente forma:

Figura. 3. Definición de la Ciberseguridad



Nota: Adaptada al español por la SGTD – PCM, fuente: https://www.iso27001security.com/html/27032.html

2.2. NORMATIVIDAD VIGENTE

1. Constitución Política del Perú, vigente desde el 31 de diciembre de 1993.
2. Ley Nº 30999, Ley de Ciberdefensa, vigente desde el 28 de agosto de 2019.
3. Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, vigente desde el 14 de setiembre de 2018, con excepción de lo descrito en la "Quinta" de la parte denominada: "Disposición Complementaria Final"[14].
4. Ley Nº 30171, Ley que modifica la Ley Nº 30096: Ley de Delitos Informáticos, vigente desde el 11 de marzo de 2014.

[14] "*(…) Disposición Complementaria Final,* ***Quinta.-*** *Vigencia El presente Decreto Legislativo entra en vigencia a partir del día siguiente de su publicación, con excepción de lo previsto en los artículos 11, 12, 14, 15, 19, 20, 21, 22, 25, 27, 31 y numerales 18.1, 18.5, 18.6 y 18.8 del artículo 18, que entrarán en vigor con la norma reglamentaria correspondiente. (…)*"

5. Ley Nº 29733: Ley de Protección de Datos Personales, vigente desde el 4 de julio de 2011.
6. Ley N° 28493: Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM), vigente desde el 13 de abril de 2005.
7. Ley Nº 27806, Ley Transparencia y Acceso a la Información Pública y sus modificatorias, vigente desde el 3 de agosto de 2002.
8. Ley N° 27269, Ley de Firmas y Certificados Digitales, vigente desde el 29 de mayo de 2000.
9. Resolución Directoral N° 017-2024-INACAL/DN, Aprueban Normas Técnicas Peruanas sobre hortalizas, Ciberseguridad y otras.
   - NTP ISO/IEC 27032:2024, Ciberseguridad. Directrices para la seguridad en Internet. 1ª Edición.

   Vigente desde el 12 de setiembre de 2024.
10. Decreto Supremo Nº 017-2024-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 30999, Ley de Ciberdefensa, vigente desde el 14 de febrero de 2024.
11. Resolución de Secretaría de Gobierno y Transformación Digital Nº 001-2024-PCM/SGTD, Crean la Alianza Nacional por una Internet Segura, vigente desde 3 de febrero de 2024.
12. Resolución de Secretaría de Gobierno y Transformación Digital N.º 003-2023-PCM/SGTD, Establecen la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas, vigente desde el 9 de setiembre de 2023.
13. Resolución de Secretaría de Gobierno y Transformación Digital Nº 002-2023-PCM/SGTD, Aprueban la Directiva Nº 001-2023-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital, vigente desde el 9 de setiembre de 2023.
14. Decreto Supremo N.º 085-2023-PCM, Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030, vigente desde el 29 de julio de 2023.
15. Resolución Directoral Nº 022-2022-INACAL/DN - Aprueban Normas Técnicas Peruanas sobre turismo, acuicultura y otros:

    (…)

    - NTP-ISO/IEC 27001:2022, Seguridad de la información, Ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3º Edición.

- NTP-ISO/IEC 27002:2022, Seguridad de la información, Ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2º Edición.
- NTP-ISO/IEC 27005:2022, Seguridad de la información, Ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3º Edición.

(…). Vigente desde el 13 de enero de 2023.

16. Resolución de Secretaría de Gobierno y Transformación Digital Nº 002-2022-PCM/SGTD, aprueban la Guía para el uso e integración de la Plataforma Nacional de Firma Digital en las entidades de la Administración Pública, vigente desde el 25 de setiembre de 2022.
17. Decreto Supremo N°095-2022-PCM, Decreto Supremo que aprueba el Plan Estratégico de Desarrollo Nacional al 2050, vigente desde el 29 de julio de 2022.
18. Decreto Supremo Nº 157-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, vigente desde el 26 de setiembre de 2021.
19. Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2021-PCM/SGTD, Aprueban la Directiva Nº 002-2021-PCM/SGTD, Directiva que regula la generación y uso del Código de Verificación Digital en las entidades de la Administración Pública, vigente desde el 18 de setiembre de 2021.
20. Resolución de Secretaría de Gobierno Digital Nº 001-2021-PCM/SGD, Aprueban la "Directiva N° 001-2021-PCM/SGD, "Directiva que establece los Lineamientos para la Conversión Integral de Procedimientos Administrativos a Plataformas o Servicios Digitales", vigente desde el 20 de junio del 2021 y su modificatoria Resolución SBS Nº 03797-2023.
21. Decreto Supremo Nº 029-2021-PCM, Decreto Supremo que aprueba el 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, vigente desde el 20 de febrero del 2021.
22. Resolución SBS Nº 504-2021, que aprueba el reglamento para la gestión de la Seguridad de la Información y la Ciberseguridad. Vigente desde el 20 de febrero de 2021.
23. Decreto Supremo N° 016-2020-PCM, Decreto Supremo que amplía los servicios de información en el marco del Decreto Legislativo Nº 1246, del Decreto Legislativo Nº 1427 y del Plan Nacional de Competitividad y Productividad, vigente desde el 4 de febrero de 2020.

24. Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, vigente desde el 10 de enero de 2020.
25. Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, vigente desde el 10 de enero de 2020.
26. Resolución de Secretaría de Gobierno Digital N° 003-2019-PCM/SEGDI, Disponen la creación del Laboratorio de Gobierno y Transformación Digital del Estado en la Presidencia del Consejo de Ministros, vigente desde el 6 de octubre del 2019.
27. Resolución Ministerial N° 266-2019-PCM, Derogan la R.M. Nº381-2008-PCM que aprobó los lineamientos y mecanismos establecidos, en los "Estándares y Especificaciones de Interoperabilidad del Estado Peruano", vigente desde el 25 de julio de 2019.
28. Resolución de Secretaría de Gobierno Digital N.° 002-2019-PCM/SEGDI, Aprueban Estándares de Interoperabilidad de la Plataforma de Interoperabilidad (PIDE) y medidas adicionales para despliegue, vigente desde el 27 de julio de 2019.
29. Resolución de Secretaría de Gobierno Digital N.° 001-2019-PCM/SEGDI, Aprueba la Directiva Nº 001-2019-PCM/SEGDI, "Directiva para compartir y usar Software Público Peruano", vigente desde el 18 de abril de 2019.
30. Resolución Ministerial N° 087-2019-PCM, Aprueban disposiciones sobre la conformación y funciones del Comité de Gobierno Digital, vigente desde el 22 de marzo de 2019.
31. Resolución de Secretaría de Gobierno Digital N°005-2018-PCM/SEGDI, Aprueban "Lineamientos para la formulación del Plan de Gobierno Digital", vigente desde el 23 de diciembre de 2018.
32. Resolución de Secretaría de Gobierno Digital N° 004-2018-PCM/SEGDI, Aprueban los "Lineamientos del Líder de Gobierno Digital" vigente desde el 23 de diciembre de 2018.
33. Resolución de Secretaría de Gobierno Digital N° 003-2018-PCM/SEGDI, Modifican el artículo 4 de la Resolución de Secretaría de Gobierno Digital N° 001-2017-PCM/SEGDI referente al Modelo de Gestión Documental, vigente desde el 22 de setiembre de 2018.
34. Decreto Supremo N° 051-2018-PCM, Decreto Supremo, que crea el Portal de Software Público Peruano y establece disposiciones adicionales sobre el software público peruano, vigente desde el 16 de mayo de 2018.
35. Decreto Supremo N° 050-2018-PCM, Aprueban la definición de Seguridad Digital de ámbito nacional, vigente desde el 16 de mayo de 2018.

36. Resolución Ministerial N.° 119-2018-PCM, Disponen la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública, vigente desde el 11 de mayo de 2018.
37. Decreto Supremo N° 033-2018-PCM, Decreto Supremo que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital, vigente desde el 24 de marzo de 2018.
38. Resolución de Secretaría de Gobierno Digital N.° 002-2018-PCM/SEGDI, Aprueban los Lineamientos para la suscripción de un Acuerdo de Nivel de Servicio (ANS) para la adecuada gestión de los servicios que publiquen las entidades públicas en la Plataforma de Interoperabilidad del Estado Peruano (PIDE), vigente desde el 3 de febrero de 2018.
39. Resolución de Secretaría de Gobierno Digital Nº 001-2018-PCM/SEGDI, Aprueban lineamientos para uso de servicios en la nube para entidades de la Administración Pública del Estado Peruano, vigente desde el 13 de enero del 2018.
40. Decreto Supremo N.° 081-2017-PCM, Decreto Supremo que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública, vigente desde el 10 de agosto de 2017.
41. Resolución de Secretaría de Gobierno Digital N.° 001-2017-PCM/SEGDI, Aprueban Modelo de Gestión Documental en el marco del Decreto Legislativo N° 1310, vigente desde el 10 de agosto de 2017.
42. Decreto Supremo N.° 067-2017-PCM, Decreto Supremo que establece los plazos aplicables a las entidades de la Administración Pública para la implementación de la interoperabilidad en el marco del Decreto Legislativo N° 1246 y dicta otras disposiciones, vigente desde 23 de junio de 2017.
43. Resolución Ministerial N.° 041-2017-PCM, Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2016 Ingeniería de Software y Sistemas, Procesos del ciclo de vida del software. 3° Edición", en todas las entidades integrantes del Sistema Nacional de Informática, vigente desde el 3 de marzo de 2017.
44. Decreto Legislativo N° 1310, Decreto Legislativo que aprueba medidas adicionales de simplificación administrativa, vigente desde el 31 de diciembre de 2016[15].

[15] La primera Disposición Complementaria Final del Decreto Legislativo Nº 1310, dispone que "El presente Decreto Legislativo entra en vigencia al día siguiente de su publicación, salvo lo dispuesto en el artículo 9º que regula el Diario Oficial "El Peruano", el cual entra en vigencia el primer día hábil del mes siguiente a la fecha de publicación del Decreto Supremo a que se refiere el citado artículo".

2.3. TERMINOLOGÍA

1. **Activo de información:** Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la entidad.
2. **Activos de información digitales:** Los activos de información digitales incluyen bases de datos, documentos electrónicos, plataformas digitales, software, registros de sistemas y cualquier dato o información almacenada en medios digitales. (ISO, 2022).
3. **Actores involucrados:** Denominados también partes interesadas, son todas las personas, grupos, organizaciones o entidades que tienen un interés, influencia o participación directa o indirecta en un proyecto, proceso, decisión o sistema. Estos actores pueden afectar o ser afectados por las acciones y resultados del mismo.
4. **Amenaza**: Ente o circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos, provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede ser natural, accidental o intencionada.
5. **Amenaza Persistente Avanzada (APT):** Del inglés como APT (Advanced Persistent Threat), ciberamenazas sofisticadas y prolongadas en el tiempo, ejecutadas por actores malintencionados con recursos elevados (como grupos estatales o criminales organizados), que buscan infiltrarse en redes o sistemas para robar información crítica o causar daños, evitando ser detectadas. Se caracterizan por su alto nivel de sigilo, adaptabilidad y persistencia.
6. **Aspecto:** Del lat. *aspectus. m. Elemento, faceta o matiz de algo. Ejm. Los aspectos más interesantes de una obra.*
7. **Autenticación digital**: Proceso de verificar la identidad de los usuarios o dispositivos en entornos digitales para evitar accesos no autorizados. Las técnicas más comunes incluyen contraseñas, biometría o autenticación multifactor.
8. **Cracker:** (Del inglés “to crack”, que significa romper o quebrar) se utiliza para referirse a las personas que rompen o vulneran algún sistema de seguridad informática. Usualmente de forma ilícita, los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío (Cracker, 2025)
9. **Ciberataque**: Es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos de información digitales a través del acceso

no autorizado a una red, sistema informático o dispositivo digital. Operación cibernética, ya sea ofensiva o defensiva, de la que cabe esperar razonablemente que cause lesiones, daño o la destrucción de recursos.

10. **Cibercrimen**: Actividades ilegales cometidas mediante el uso de tecnologías digitales, especialmente a través de Internet y redes informáticas. Esto incluye una amplia gama de delitos, como el acceso no autorizado a sistemas o datos, el robo de identidad, el fraude en línea, el espionaje cibernético, la distribución de malware, el phishing, el secuestro de datos (ransomware), entre otros. Los ciberdelincuentes utilizan vulnerabilidades tecnológicas para obtener beneficios económicos, realizar ataques a infraestructuras críticas o causar daño a individuos, organizaciones y gobiernos.
11. **Ciberdefensa:** En el entorno global, es vinculada a la protección de infraestructuras críticas y activos de información digitales nacionales frente a ciberataques, especialmente aquellos con motivación política, militar o estratégica. Incluye operaciones defensivas y ofensivas en el ciberespacio, respuesta a ataques patrocinados por estados (guerra cibernética) y colaboración entre gobiernos, ejércitos y organismos de inteligencia.

    En el Perú, *"Entiéndase por ciberdefensa a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional"*[16].
12. **Ciberdelincuencia:** Hechos cometidos en los que los datos o sistemas informáticos son el objeto contra el que se dirige el delito, así como el medio para cometer el delito (ONU)[17]. Según INTERPOL[18], son actividades delictivas que se cometen utilizando computadoras, internet y otros dispositivos digitales, y que pueden incluir robo de identidad, fraude, acoso, entre otros.
13. **Ciberdelito o delito informático**. Delito que se comete a través de internet[19], ejemplos: fraude, suplantación de identidad, robo, crimen organizado, etc.
14. **Ciberespacio**: Espacio virtual creado por la interconexión de computadoras, servidores, redes y sistemas a través de internet. Implica todo el ecosistema digital, incluyendo la web, las redes sociales, los correos electrónicos, las aplicaciones y otros servicios que se desarrollan y operan en internet. El ciberespacio tiene una connotación más abstracta, como el "lugar" donde se llevan a cabo interacciones en línea.

[16] Definición que se encuentra citada en el "Artículo 4" de la Ley Nº 30999. Ley de Ciberdefensa.
[17] Definición de Ciberdelincuencia según la ONU: https://observatorio.ceplan.gob.pe/ficha/t85
[18] Definición de Ciberdelincuencia: https://www.interpol.int/es/Delitos/Ciberdelincuencia
[19] RAE: https://www.rae.es/

15. **Ciberguerra:** Refiere al desplazamiento de un conflicto, en principio de carácter bélico que toma el ciberespacio y las tecnologías de la información como escenario principal, para producir alteraciones en datos y sistemas del enemigo, a la vez que se protege del atacante, a la información y sus activos.
16. **Ciberinteligencia:** Actividades de inteligencia en soporte de la Ciberseguridad. Se trazan ciberamenazas, se analizan las intenciones y oportunidades de los ciber adversarios con el fin de identificar, localizar, atribuir fuentes de ciberataques y se utilizan prácticas de Threat Hunting (caza de amenazas), para prevenir los ciberataques.
17. **Cibernético:** hace referencia a todo lo relacionado con la Cibernética, que es la ciencia que estudia los sistemas de control y comunicación en máquinas y organismos. En un contexto más amplio, se utiliza para describir aspectos vinculados a la informática, redes, sistemas digitales y la interacción entre estos elementos, especialmente en lo que respecta al procesamiento y transmisión de información.
18. **Ciberresiliencia o resiliencia cibernética:** Es la capacidad de una organización para anticipar, resistir y recuperarse de incidentes de Ciberseguridad. asegurando la continuidad de sus operaciones y la protección de sus activos digitales, incluso frente a amenazas desconocidas o persistentes.
19. **Ciberterrorismo:** Un acto delictivo perpetrado mediante el uso de computadoras y capacidades de telecomunicaciones, que resulta en violencia, destrucción y/o interrupción de los servicios para crear miedo, al causar confusión e incertidumbre dentro de una población determinada, con el objetivo de influir en un gobierno o población para que se ajuste a una agenda política, social o ideológica particular.
20. **Confianza Digital**: Es la certeza que los usuarios tienen sobre la seguridad, privacidad y autenticidad de las interacciones digitales. Se refiere a la capacidad de las plataformas, servicios y personas para actuar de manera segura y transparente en el entorno digital.
21. **Confidencialidad:** Es la propiedad de la información que permite garantizar el acceso a la misma, solo por el personal autorizado.
22. **Digital:** Dicho de un dispositivo o sistema: que crea, presenta, transporta o almacena información mediante la combinación de bits. Adj. Que se realiza o transmite por medios digitales.
23. **Disponibilidad:** Capacidad de la información de ser accesible y utilizable cuando sea requerida por los usuarios y es uno de los pilares de la seguridad de la información.
24. **Entorno Digital:** Refiere al espacio virtual y tecnológico en el que interactúan los usuarios, sistemas, dispositivos y plataformas mediante el uso de internet y/o tecnologías

informáticas. Incluye una amplia variedad de componentes, como redes sociales, aplicaciones, sitios web, dispositivos conectados, servicios en la nube, y más. En este entorno, la información se genera, comparte, procesa y almacena, facilitando una conectividad global y transformando diversos aspectos de la vida cotidiana, desde el trabajo hasta las relaciones personales y la economía.

Según la normativa peruana, refiere al *"Dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes e infraestructuras de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, plataformas que sirven como base para la interacción entre personas, empresas, entidades públicas o dispositivos"*[20].

25. **Estrategia:** Según la RAE: "Del lat. Strategĭa, provincia bajo el mando de un general, f. Arte de dirigir las operaciones militares. Sin.: táctica. f. Arte, traza para dirigir un asunto".
26. **Gobernanza Digital:** Según la Ley de Gobierno Digital[21], es el conjunto de procesos, estructuras, herramientas, y normas que nos permiten dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales en la organización.
27. **Incidente de seguridad de la información:** Cualquier evento o suceso que afecta la confidencialidad, integridad o disponibilidad de la información y sus activos, como también la continuidad del servicio proporcionado por los sistemas que la contienen, de un determinado ente.
28. **Incidente de seguridad digital:** Según el D.U. 007-2020 es un "evento o serie de eventos que puedan 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".
29. **Infraestructura crítica**: Refiere a los sistemas, plataformas, instalaciones, redes, servicios y activos físicos o virtuales que son esenciales para el funcionamiento de una sociedad, economía y seguridad nacional. Su interrupción o daño puede tener graves consecuencias, afectando la seguridad pública, la salud, la economía y la estabilidad del estado.
30. **Integridad:** Propiedad de la información que garantiza la exactitud de los datos enviados para asegurar que no se han realizado alteraciones, perdida o destrucción al momento de la transferencia o almacenamiento.

[20] Según el literal c) del "Artículo 3: Definiciones" del "Capítulo I: Disposiciones Generales" del "Decreto Supremo 007-2020 - Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. En concordancia con el ítem 2 del Artículo.3 del "Decreto Legislativo Nº 1412. Decreto Legislativo que aprueba la Ley de Gobierno Digital".
[21] Según el Ítem 2 del "Artículo 3: Definiciones" del "Titulo I. Disposiciones Generales" del "Decreto Legislativo Nº 1412. Decreto Legislativo que aprueba la Ley de Gobierno Digital".

31. **Metamorfismo:** Reescribe completamente su código sin cambiar la funcionalidad.
32. **Polimorfismo:** Refiere a un cambio de código (por ejemplo, cifrado u ofuscación) cada vez que se ejecuta.
33. **Política de Seguridad:** son las medidas de seguridad que han sido establecidos en una organización para mantener la seguridad de sus sistemas de información, luego de evaluar sus activos de información y los riesgos a los que se encuentran expuestos.
34. **Ransomware**: (en español: malware de rescate). Es un malware sofisticado que se aprovecha de las debilidades del sistema y utiliza un cifrado sólido para mantener los datos o la funcionalidad del sistema como rehenes. Los ciberdelincuentes utilizan ransomware para exigir un pago a cambio de liberar el sistema. Un desarrollo reciente de ransomware es el complemento de tácticas de extorsión.
35. **Riesgo cibernético:** Consiste en la probabilidad de ocurrencia que una amenaza explote o aproveche alguna vulnerabilidad de un activo de información digital, por tanto, ocasione pérdida o dañe a una entidad.
36. **Riesgo en Seguridad de la Información:** refiere a la probabilidad de ocurrencia de que una amenaza explote o aproveche alguna vulnerabilidad en un activo de información, de una organización o individuo causando daño o pérdida. Este riesgo está determinado por dos factores principales: **a) La probabilidad de ocurrencia** de un ataque o incidente de seguridad (como un ciberataque, virus, robo de datos, etc.) **b) El impacto potencial** de dicho incidente en caso de que se materialice (como pérdida de datos, daños financieros, interrupción del servicio, etc.).
37. **Sistema Nacional de Transformación Digital: "***Es un sistema funcional del Poder Ejecutivo, conformado por un conjunto de principios, normas, procedimientos, técnicas e instrumentos mediante los cuales se organizan las actividades de la administración pública y se promueven las actividades de las empresas, la sociedad civil y la academia orientadas a alcanzar los objetivos del país en materia de Transformación Digital.*

    (…) *El Sistema Nacional de Transformación Digital se sustenta en la articulación de los diversos actores públicos y privados de la sociedad y abarca, de manera no limitativa, las materias de gobierno digital, economía digital, conectividad digital, educación digital, tecnologías digitales, innovación digital, servicios digitales, sociedad digital, ciudadanía e inclusión digital y confianza digital; sin afectar las autonomías y atribuciones propias de cada sector, y en coordinación con estos en lo que corresponda en el marco de sus competencias.*"[22]

[22] Según los numerales 4.1 y 4.2 del *"Artículo 4.- Sistema Nacional de Transformación Digital"* del *"Decreto de Urgencia Nº006-2020 - Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital".*

38. **SOAR:** Solución tecnológica que integra herramientas y procesos para mejorar la eficiencia en la gestión de incidentes de seguridad (IBM, 2020).
39. **Seguridad Digital:** Es la dimensión económica y social de la Ciberseguridad. Es esencial para mantener la confianza en nuestras economías, cada vez más dependientes de la tecnología digital, y para aumentar la resiliencia en un mundo sujeto a crecientes conflictos geopolíticos y ciberdelitos (OCDE)
40. **Soberanía Digital:** Refiere al control y la autonomía de un país o entidad sobre sus propios datos, infraestructuras tecnológicas y políticas digitales, sin depender de potencias extranjeras o empresas globales. Implica la capacidad de gestionar, almacenar y proteger la información dentro de sus fronteras, establecer normativas locales para la privacidad y la seguridad en línea, y asegurar que los datos sensibles de sus ciudadanos y organizaciones estén protegidos de influencias externas. La soberanía digital también aborda la preservación de los derechos digitales y la libertad de acceso y uso de la tecnología dentro de un marco legal y ético propio.
41. **Tecnologías emergentes:** Tecnologías digitales capaces de generar soluciones innovadoras; dentro de estas tecnologías destacan: la robótica, la analítica de datos, la inteligencia artificial, la computación cuántica, las tecnologías cognitivas, la nanotecnología, el internet de las cosas (IoT), entre otras, que conforman la industria 4.0 como la nueva revolución que combina técnicas avanzadas, de producción y operaciones con tecnología, generando un impacto en el ecosistema digital, las organizaciones y las personas[23].
42. **Vulnerabilidad:** Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un objetivo o recurso informático importante para la entidad.
43. **Zero Trust (Confianza Cero):** Es un modelo de Ciberseguridad (que opera bajo el principio de "nunca confiar, siempre verificar". Este enfoque elimina la suposición implícita de que usuarios, dispositivos o redes internas son inherentemente confiables. En su lugar, requiere autenticación estricta, autorización continua y validación de contexto para cada solicitud de acceso a recursos, independientemente de su origen (interno o externo) (NIST, 2020).

[23] Según el literal h) del "Artículo 3: Definiciones" del "Capítulo I: Disposiciones Generales" del "Decreto Supremo Nº157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia Nº 006-2020. Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital".

III. PANORAMA ACTUAL DE LA CIBERSEGURIDAD Y ALINEACIÓN DE LA ESNACIB CON LAS PRINCIPALES POLÍTICAS INTERNACIONALES Y MARCOS: NORMATIVO Y DE GOBERNANZA DEL PAÍS

3.1. ALINEACIÓN DE LA ESNACIB CON LAS PRINCIPALES POLÍTICAS INTERNACIONALES

La ESNACIB, integra los compromisos internacionales adquiridos por el país en materia de Ciberseguridad y lucha contra la ciberdelincuencia. Su enfoque incluye el fortalecimiento de la cooperación bilateral y multilateral con otros Estados y organismos internacionales, así como la adopción de estándares y buenas prácticas globales. Además, se promoverán alianzas con iniciativas nacionales vinculadas a la ciudadanía digital, con el objetivo de incentivar un uso responsable y seguro de las tecnologías digitales entre la población.

3.1.1. ALINEACIÓN CON EL INDICE GLOBAL DE CIBERSEGURIDAD QUE PROMUEVE LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT)

Figura. 4. International Telecommunication Union (ITU)

La Unión Internacional de Telecomunicaciones (en inglés: International Telecommunication Union (ITU)), es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU) el cual promueve el Índice Global de Ciberseguridad (IGC) (en inglés: “Global Cybersecurity Index” (GCI)), el cual es una herramienta confiable que evalúa el nivel de compromiso de los países con la Ciberseguridad, destacando su importancia y sus múltiples dimensiones. Esta medición considera el grado de desarrollo en cinco pilares fundamentales: medidas legales, técnicas, organizacionales, desarrollo de capacidades y cooperación. Dado el carácter transversal de la Ciberseguridad en diversos sectores, el índice permite comparar el desempeño global de cada nación. La puntuación final que emite el IGC, refleja una visión integral del avance en políticas y acciones de ciberprotección.

Figura. 5. Índice Global de Ciberseguridad (IGC)

La ESNACIB se alinea con el Índice Global de Ciberseguridad (IGC), al adoptar sus pilares descritos en el presente documento, con los pilares que promueve el IGC como son el ámbito legal, técnico, organizacional y de cooperación. La ESNACIB promueve marcos normativos robustos y holísticos, capacidades técnicas avanzadas y la formación de especialistas, reflejando los criterios del GCI para medir la madurez en Ciberseguridad. Además, fomenta la colaboración público-privada junto con la academia, sociedad civil

y la participación en iniciativas internacionales, clave para mejorar su puntuación en el índice. Esto demuestra un esfuerzo por alcanzar estándares globales y fortalecer la resiliencia digital del país.

Sin embargo, persisten desafíos como la necesidad de mayor inversión en infraestructura y concienciación ciudadana, aspectos críticos para escalar en el IGC. La ESNACIB busca cerrar estas brechas mediante planes de implementación progresiva y alianzas estratégicas, siguiendo las mejores prácticas del GCI. La articulación con organismos como la OEA y el BID también refuerza su alineación con métricas internacionales. Aunque hay avances, el Perú debe acelerar la ejecución de sus objetivos para mejorar su posición global en Ciberseguridad.

3.1.2. CONCORDANCIA DE LA ESNACIB CON LA AGENDA 2030 PARA EL DESARROLLO SOSTENIBLE DE LAS NACIONES UNIDAS (ONU)

La ESNACIB, se alinea directamente con la Agenda 2030[24] para el Desarrollo Sostenible de las Naciones Unidas (ONU) Objetivos de Desarrollo Sostenible (ODS) promovidos por la ONU, especialmente con el **ODS 9 (Industria, innovación e infraestructura), ODS 16 (Paz, justicia e instituciones sólidas) y ODS 17 (Alianzas para lograr los objetivos)**. Al fortalecer las capacidades nacionales en Ciberseguridad, la ESNACIB impulsa el desarrollo de infraestructuras digitales resilientes y seguras, esenciales para la Transformación Digital inclusiva y sostenible del país. Asimismo, al promover una gobernanza cibernética transparente y colaborativa, se fortalece el Estado de derecho y la confianza de los ciudadanos en las instituciones públicas.

Por otro lado, la implementación efectiva de la ESNACIB también contribuye al **ODS 4 (Educación de calidad)** mediante la promoción de competencias digitales y la formación en Ciberseguridad para todos los niveles educativos. Esto se complementa con la cooperación internacional y público-privada que refuerza el ODS 17, al facilitar el intercambio de buenas prácticas, tecnologías y marcos regulatorios entre países y actores estratégicos.

En conjunto, la estrategia no solo protege los activos digitales del país, sino que también actúa como un catalizador para el desarrollo sostenible, inclusivo y seguro en el entorno digital peruano.

[24] Cumbre sobre los ODS, realizada en septiembre de 2019.

Figura. 6. Objetivos de Desarrollo Sostenible que promueve la ONU

Nota: Fuente: ODS, enlace web: https://www.un.org/sustainabledevelopment/es/2015/09/la-asamblea-general-adopta-la-agenda-2030-para-el-desarrollo-sostenible/

3.1.3. CONCORDANCIA CON EL MARCO DE SEGURIDAD DIGITAL QUE PROMUEVE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓNIMO (OCDE)

Desde que Perú se convirtió en "país candidato" al ingreso en la OCDE en enero de 2022, mediante una invitación formal el 25 de enero[25], mantuvo un roadmap aprobado por el Consejo Ministerial de la OCDE el 10 de junio de 2022. En ese plan se comprometió a implementar más de 24 recomendaciones en áreas como gobernanza, políticas regulatorias, conducta empresarial responsable, anticorrupción, Transformación Digital, derechos humanos y gestión pública. Particularmente en Ciberseguridad y economía digital, Perú adoptó en 2020 el Marco de Confianza Digital (Decreto de Urgencia 007-2020), creó la Secretaría de Gobierno Digital (SEGDI),

[25] Enlace web: https://www.investinperu.pe/en/pi/detail-news/oecd-evaluates-peru-on-responsible-business-condu?utm_source=chatgpt.com

actualmente la Secretaría de Gobierno y Transformación Digital (SGTD) y avanzó en Protección de datos, Seguridad Digital y Transparencia[26].

A la fecha, aunque Perú no es aún miembro pleno de la OCDE, ha completado etapas clave como por ejemplo en abril de 2025 presentó ante el Comité de Política Regulatoria evidencia de haber implementado el 100 % de las recomendaciones de junio de 2024; se ha continuado recibiendo asistencia técnica de la OCDE en finanzas públicas[27], y fue objeto de misiones de evaluación sobre conducta empresarial responsable en julio de 2024.

Asimismo, con la elaboración de la ESNACIB se alcanza el alineamiento con las recomendaciones siguientes:

- ✓ "Recomendación del Consejo sobre la Gestión de Riesgos de Seguridad Digital"[28](OCDE, 2022), incorporada en el **"Pilar 4. Denominado: Gestión de Riesgos, resiliencia y respuesta a incidentes" de la ESNACIB.**
- ✓ "Recomendación del Consejo sobre Estrategias Nacionales de Seguridad Digital"[29] (OCDE, 2022), considerada en todo su contexto por la **ESNACIB**.
- ✓ "Recomendación del Consejo sobre la Seguridad Digital de las actividades críticas"[30] (OCDE, 2019), incorporada en el **"Pilar 2. Salvaguarda a las Infraestructuras críticas y activos de información digitales.", de la ESNACIB.**
- ✓ "Recomendación del Consejo sobre la seguridad digital de los productos y servicios"[31] (OCDE, 2022), considerada en el "**Principio 7. Entorno de Confianza" de la ESNACIB**
- ✓ "Recomendación del Consejo sobre el tratamiento de las vulnerabilidades de Seguridad Digital"[32] (OCDE, 2022), inmersa en el **"Pilar 4. Gestión de Riesgos, resiliencia y respuesta a incidentes"** y el "**Pilar 2. Salvaguarda a las Infraestructuras críticas y activos de información digitales" de la ESNACIB.**

Siendo así, Perú ya está en una fase avanzada del proceso, con fuertes compromisos establecidos y avances concretos, teniendo en cuenta la elaboración de la presente estrategia.

[26] Enlace web: https://www.trade.gov.http.akamai-trials.com/country-commercial-guides/peru-digital-economy?utm_source=chatgpt.com
[27] Enlace web: https://andina.pe/agencia/noticia-peru-mef-will-receive-oecd-technical-advice-to-strengthen-and-consolidate-public-finances-992389.aspx?utm_source=chatgpt.com
[28] Enlace web: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479
[29] Enlace web: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480
[30] Enlace web: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456
[31] Enlace web: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481
[32] Enlace web: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482

3.2. ALINEACIÓN DE LA ESNACIB CON LOS MARCOS: NORMATIVO Y DE GOBERNANZA DEL PAÍS

En el marco regulatorio, la ESNACIB se alinea con los principales dispositivos normativos tales como:

3.2.1. CONSTITUCIÓN POLÍTICA DEL PERÚ

Figura. 7. Constitución Política del Perú

La ESNACIB del Perú, se alinea principalmente con el **artículo 1**° de la Constitución Política, ya que busca proteger a la persona humana y su dignidad en el entorno digital. Promueve la seguridad, privacidad y derechos fundamentales de los ciudadanos frente a amenazas cibernéticas. Además, garantiza un ciberespacio confiable que respalde el desarrollo humano y social. Al priorizar la protección de datos, la inclusión digital segura y la defensa de los más vulnerables, la ESNACIB cumple con el fin supremo del Estado. Así, traslada los principios constitucionales al ámbito tecnológico actual.

También se alinea con el **artículo 2º** de la Constitución Política del Perú, ya que **garantiza el derecho a la seguridad personal, la inviolabilidad de las comunicaciones y el acceso a la información**. La ESNACIB protege estos derechos fundamentales mediante la defensa de la privacidad digital y la integridad de los datos personales, evitando ciberataques, fraudes electrónicos y otras formas de vulneración digital. Así, contribuye a que los ciudadanos puedan ejercer sus derechos en un entorno digital seguro y confiable, respetando las libertades individuales y colectivas.

Además, la ESNACIB se relaciona estrechamente con el **artículo 44º**, que establece la **Defensa Nacional** como un deber supremo y un principio rector para garantizar la soberanía e integridad territorial del país. Mediante la protección de las infraestructuras críticas digitales y la ciberdefensa del Estado, la estrategia refuerza la seguridad nacional en el ámbito digital, previniendo ciberamenazas que puedan comprometer la estabilidad y el orden interno. De esta manera, la ESNACIB garantiza que la **soberanía nacional** se mantenga firme en el contexto de la creciente dependencia tecnológica.

3.2.2. LEY DE GOBIERNO DIGITAL Y SU REGLAMENTO[33]

La ESNACIB se alinea directamente con la Ley de Gobierno Digital, cuyo enfoque principal es promover la Transformación Digital segura y eficiente del Estado peruano. La ESNACIB garantiza la protección de los sistemas y servicios digitales estatales frente a ciberamenazas, asegurando la continuidad operativa y la integridad de la información pública. Esto es clave para fortalecer la confianza ciudadana en las plataformas digitales gubernamentales, permitiendo un acceso ágil y seguro a los servicios públicos. Además, fomenta la implementación de estándares que complementan las disposiciones de la ley para la interoperabilidad y la gestión de datos.

También, la ESNACIB impulsa la capacitación y sensibilización de los servidores públicos en materia de Ciberseguridad, alineándose con la visión de la Ley de Gobierno Digital de fortalecer capacidades internas. Promueve la creación de mecanismos de respuesta rápida ante incidentes cibernéticos, garantizando la protección de la información estratégica y personal conforme a la normativa vigente. De esta forma, la estrategia contribuye a consolidar un gobierno digital resiliente, inclusivo y transparente, enmarcado en la modernización del Estado y la protección de derechos digitales, pilares fundamentales de la Ley de Gobierno Digital.

Figura. 8. Ley de Gobierno Digital y su reglamento

Asimismo, la ESNACIB se alinea con el Reglamento de la Ley de Gobierno Digital al operacionalizar los principios y disposiciones normativas para la seguridad de la información y la gestión de riesgos tecnológicos en las entidades públicas. Este reglamento establece las responsabilidades, roles y procedimientos que las organizaciones deben seguir para garantizar la protección de sus sistemas digitales, lo cual es un pilar fundamental en la implementación de la estrategia. La ESNACIB contribuye a estandarizar estas prácticas, asegurando la correcta aplicación de controles técnicos y administrativos para prevenir, detectar y responder a incidentes cibernéticos en el sector público.

Además, el reglamento enfatiza la necesidad de una gestión integrada de la seguridad digital, promoviendo la coordinación entre entidades y el uso de tecnologías seguras, lo

[33] Ley de Gobierno Digital aprobado por el Decreto Legislativo N° 1412 y su Reglamento aprobado por el (Decreto Supremo N° 029-2021-PCM.

que está directamente respaldado por la ESNACIB. La estrategia impulsa la creación de capacidades especializadas y la implementación de planes de continuidad operacional y recuperación ante desastres digitales, alineándose con las exigencias regulatorias. De este modo, la ESNACIB fortalece la gobernanza digital y la resiliencia del Estado, facilitando un entorno seguro y confiable para la prestación de servicios públicos digitales conforme a lo establecido en el reglamento.

3.2.3. LEY DE PROTECCIÓN DE DATOS PERSONALES Y SU REGLAMENTO

La ESNACIB, se alinea estrechamente con la Ley de Protección de Datos Personales (Ley N° 29733) y su reglamento, al establecer mecanismos para garantizar la confidencialidad, integridad y disponibilidad de la información personal en entornos digitales. La ESNACIB promueve la implementación de controles técnicos y organizativos que eviten accesos no autorizados, filtraciones o usos indebidos de datos personales por parte de entidades públicas y privadas. Esta protección es fundamental para resguardar los derechos constitucionales a la privacidad y a la autodeterminación informativa, pilares de la ley, asegurando un manejo responsable y seguro de la información sensible.

Figura. 9. Protección de Datos Personales

Asimismo, la ESNACIB refuerza la capacidad de respuesta ante incidentes de seguridad que comprometan datos personales, promoviendo la colaboración entre organismos reguladores, operadores de sistemas y el sector privado. Incorpora buenas prácticas en gestión de riesgos y auditorías continuas, alineándose con las obligaciones establecidas por la Ley y su reglamento para proteger los datos durante todo su ciclo de vida. De esta forma, la estrategia contribuye a fortalecer la confianza de la ciudadanía en el entorno digital y a garantizar un marco seguro para el desarrollo de la economía y la sociedad digital en el Perú.

3.2.4. LEY DE CIBERDEFENSA Y SU REGLAMENTO[34]

La ESNACIB, se alinea de manera integral con la Ley N° 30999. Ley de Ciberdefensa, ya que ambas buscan fortalecer la capacidad del Estado para proteger sus sistemas de

[34] Ley N° 30999 que aprueba la Ley de Ciberdefensa y su Reglamento aprobado por el Decreto Supremo Nº 017-2024-PCM

información y redes frente a amenazas y ataques cibernéticos. La ESNACIB establece lineamientos para la prevención, detección y respuesta ante incidentes en el ciberespacio, apoyando el mandato legal de la ley que faculta a las Fuerzas Armadas y organismos de defensa a ejecutar acciones defensivas y ofensivas en el ámbito digital. Esto garantiza la defensa de la soberanía nacional en un contexto cada vez más digitalizado y complejo.

Además, la ESNACIB promueve la coordinación interinstitucional y la cooperación con actores públicos y privados, pilares también esenciales en la Ley de Ciberdefensa para la construcción de una postura unificada ante las amenazas cibernéticas. La estrategia impulsa la capacitación especializada y el desarrollo de capacidades tecnológicas avanzadas, en línea con las disposiciones legales que buscan consolidar una fuerza cibernética nacional robusta. De este modo, la ESNACIB no solo contribuye a la protección de la infraestructura crítica, sino también a la resiliencia operativa y estratégica del país en el ciberespacio.


El Peruano

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

DECRETO SUPREMO N° 015-2024-JUS

DECRETO SUPREMO QUE APRUEBA EL REGLAMENTO DE LA LEY N° 29733, LEY DE PROTECCIÓN DE DATOS PERSONALES

NORMAS LEGALES

Figura. 10. Reglamento de la Ley de Ciberdefensa mostrado en el Diario Oficial "El Peruano"

Asimismo, la ESNACIB se alinea con el Reglamento de la Ley de Ciberdefensa al operacionalizar las directrices para la organización, funciones y procedimientos de las unidades encargadas de la ciberdefensa. La estrategia promueve la implementación de protocolos claros para la detección y respuesta ante ciberataques, así como la coordinación efectiva entre Fuerzas Armadas, entidades del sector público y privado. Además, refuerza la capacitación continua y el desarrollo tecnológico que exige el reglamento para mantener una postura defensiva actualizada y eficiente. Así, la ESNACIB asegura la aplicación práctica y efectiva de las disposiciones reglamentarias para proteger la soberanía digital del país.

3.2.5. DECRETO DE URGENCIA N° 007-2020-PCM QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL

La ESNACIB, se alinea con el Decreto de Urgencia N° 007-2020-PCM, que establece el Marco de Confianza Digital, al promover un enfoque integral para garantizar la seguridad en el entorno digital. La ESNACIB contribuye a la implementación de medidas que

coadyuvan a fortalecer el Centro Nacional de Seguridad Digital, encargado de gestionar y coordinar la seguridad digital en el país. Además, la estrategia apoya que se tenga un Registro Nacional de Incidentes de Seguridad Digital, facilitando la recopilación y análisis de incidentes para mejorar la respuesta ante amenazas cibernéticas.


El Peruano

NORMAS LEGALES

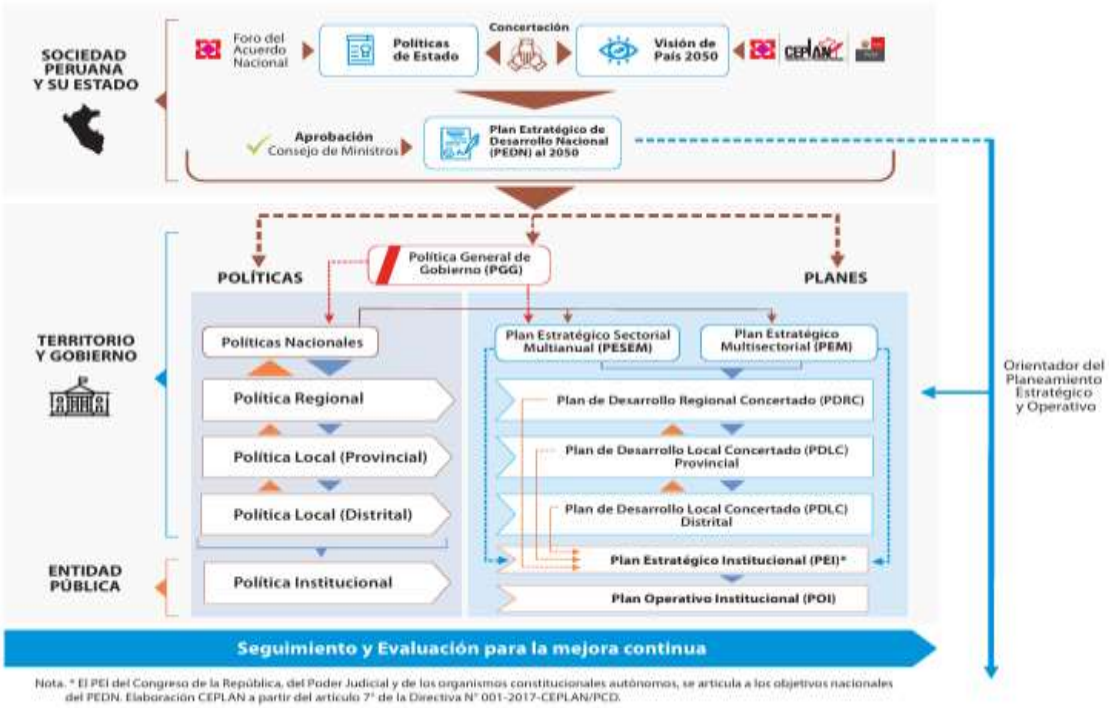
D. S. Nº 007-2020-DE.- Decreto Supremo que aprueba las condiciones, reglas y procedimientos para la aplicación de la Décimo Tercera Disposición Complementaria Final del Decreto Legislativo N° 1132. Decreto Legislativo que aprueba la nueva estructura de ingresos aplicable al personal militar de las Fuerzas Armadas y policial de la Policía Nacional del Perú

Figura. 11. Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

Asimismo, la ESNACIB respalda las obligaciones establecidas en el Decreto de Urgencia para los proveedores de servicios digitales, como la notificación de incidentes al Centro Nacional de Seguridad Digital y la implementación de medidas de seguridad adecuadas. La estrategia también promueve la formación de equipos de respuesta ante incidentes de seguridad digital en las entidades públicas, conforme a las disposiciones del Decreto. De esta manera, la ESNACIB refuerza la confianza digital en el país, alineándose con las políticas y medidas establecidas en el Decreto de Urgencia N° 007-2020-PCM.

Respecto a la articulación de políticas y planes de acuerdo con el Sistema Nacional de Planeamiento Estratégico (SINAPLAN) se tiene:

Figura. 12. Articulación de Políticas y Planes en el SINAPLAN



Nota: Fuente: Plan Estratégico de Desarrollo Nacional al 2050.

Enlace Web: www.gob.pe/uploads/document/file/5133337/Peru%20-%20Plan%20Estrategico%20de%20Desarrollo%20Nacional%20al%202050.pdf?v=1694719008

Aunque la ESNACIB constituye un documento estratégico que actúa como instrumento de política pública en materia de Ciberseguridad, su diseño y enfoque están articulados con las principales políticas y planes nacionales, por lo que se expone su vinculación con estos marcos de acción:

3.2.6. ALINEACIÓN DE LA ESNACIB CON LAS POLÍTICAS DE ESTADO DEL ACUERDO NACIONAL

El Acuerdo Nacional del Perú es un instrumento clave de concertación que orienta las políticas públicas a largo plazo, promoviendo el desarrollo sostenible y la gobernabilidad democrática. En el contexto de la Ciberseguridad, su relevancia radica en que reconoce la Seguridad Nacional, como un eje estratégico (Política 9), incorporando la protección del ciberespacio como parte fundamental de la defensa del Estado, así como promueve la "Sociedad de la información y sociedad del conocimiento" (Política 35). Esto impulsa la formulación de políticas como la ESNACIB, alineadas con los compromisos del Acuerdo. Así, fortalece la resiliencia digital del país frente a amenazas crecientes.

La ESNACIB, se alinea con las principales Políticas de Estado del Acuerdo Nacional, en sus secciones como:

SECCIÓN I. DEMOCRACIA Y ESTADO DE DERECHO

Numeral "9. Política de Seguridad Nacional"

La ESNACIB, se articula directamente con la Política 9 del Acuerdo Nacional, que promueve una Seguridad Nacional integral frente a amenazas tradicionales y emergentes. La Ciberseguridad, en este contexto, es un componente esencial para resguardar la soberanía, la estabilidad institucional y el bienestar de la población frente a riesgos en el ciberespacio. ESNACIB refuerza esta visión al priorizar la protección de infraestructuras críticas, la gestión de riesgos digitales y la coordinación interinstitucional, aspectos clave también en la doctrina de seguridad nacional. Asimismo, promueve la anticipación y respuesta frente a incidentes cibernéticos, contribuyendo a una defensa efectiva del país en entornos digitales hostiles.

Complementando los principios de la Política 9, la ESNACIB adopta un enfoque estratégico que reconoce la interdependencia entre seguridad digital, desarrollo nacional y gobernabilidad democrática. Esto incluye la promoción de capacidades técnicas y humanas, el fortalecimiento de la ciberdefensa en sectores estratégicos, y el impulso de una cultura de Seguridad Digital en todos los niveles del Estado y la sociedad. Alineada

con la Seguridad Nacional, fomenta una arquitectura cibernética resiliente que garantice la continuidad operativa del Estado y la protección de los derechos ciudadanos. De esta manera, la ESNACIB no solo responde a los desafíos actuales, sino que se convierte en un instrumento clave para consolidar un Perú más seguro, soberano y preparado frente a las amenazas del siglo XXI.

SECCIÓN III. COMPETITIVIDAD DEL PAÍS

Numeral "18. Búsqueda de la competitividad, productividad y formalización de la actividad económica "

La ESNACIB, se alinea estrechamente con la Política 18 del Acuerdo Nacional, al reconocer que un entorno digital seguro es esencial para consolidar un crecimiento económico sostenido y competitivo. En un contexto global cada vez más interconectado, la protección de la infraestructura digital, la prevención del cibercrimen y la gestión segura de datos se convierten en elementos estratégicos para atraer inversiones, promover la formalización de actividades económicas y facilitar el acceso de las empresas, especialmente las MYPEs, a mercados digitales nacionales e internacionales. Así, la Ciberseguridad deja de ser solo un asunto técnico y pasa a ser un habilitador clave de la competitividad económica del país.

La ESNACIB contribuye directamente a la construcción de una administración pública moderna, transparente y eficiente, mediante el fortalecimiento de capacidades digitales seguras, la reducción de riesgos tecnológicos y el impulso de la confianza digital. Además, apoya la simplificación administrativa y el acceso equitativo a servicios electrónicos, brindando a empresas y ciudadanos un entorno digital confiable para operar y desarrollarse. Este marco también fomenta la innovación tecnológica, la protección de la propiedad intelectual digital, y la capacitación del talento humano en Ciberseguridad, aspectos que refuerzan la productividad, formalización y el desarrollo de una cultura de competitividad digital alineada con los objetivos nacionales.

Numeral "20. Desarrollo de la ciencia y la tecnología"

La ESNACIB se articula con la Política 20 al reconocer que la Ciberseguridad es un pilar fundamental en el ecosistema de ciencia, tecnología e innovación, especialmente en un entorno marcado por el auge de tecnologías emergentes como por ejemplo la Inteligencia Artificial. El desarrollo de estas tecnologías exige infraestructura digital robusta y entornos seguros que garanticen su uso ético, confiable y responsable. Al proteger estos espacios, se facilita la investigación, la transferencia tecnológica y la

generación de valor desde el conocimiento. Esto fortalece la competitividad nacional basada en la innovación y el talento.

Asimismo, la ESNACIB impulsa la cooperación entre el Estado, el sector privado, la academia y la sociedad civil, para avanzar en investigaciones aplicadas en Ciberseguridad, promoviendo el uso seguro de estas tecnologías. Alineada con la Política 20, fomenta la protección de la propiedad intelectual digital y el desarrollo de marcos normativos que resguarden los datos y algoritmos utilizados en procesos científicos. También incentiva la formación de profesionales altamente calificados en sectores tecnológicos estratégicos, consolidando una cultura de pensamiento crítico y uso responsable de tecnologías emergentes desde la educación básica hasta la especialización técnica.

SECCIÓN IV. ESTADO EFICIENTE, TRANSPARENTE Y DESCENTRALIZADO

Numeral "35. Sociedad de la información y sociedad del conocimiento"

La Política 35, aprobada el 16 de agosto de 2017, destaca que:

> *"(…) Promoveremos el acceso* universal *al conocimiento a través de las Tecnologías de la Información y Comunicación (TIC), acompañado de la generación de contenidos, servicios y bienes digitales, así como del desarrollo de capacidades para que todos los peruanos puedan desempeñarse plenamente y de manera segura en el entorno digital, y de igual manera promoveremos mecanismos que fortalezcan el acceso, conectividad y su uso en las regiones del país. (…)*".

Es así que, la ESNACIB, se alinea estrechamente con la Política 35 del Acuerdo Nacional, al garantizar un entorno digital seguro, libre y accesible, protegiendo los derechos humanos en el ciberespacio y fomentando el uso confiable de las TIC, asegurando la integridad, confidencialidad y disponibilidad de la información, pilares esenciales para el acceso universal al conocimiento y la modernización del Estado. Además, refuerza la gobernabilidad democrática mediante sistemas digitales transparentes y resilientes frente a amenazas. La inclusión digital segura contribuye a cerrar brechas sociales y regionales. Asimismo, una infraestructura tecnológica protegida permite impulsar ciudades inteligentes y sectores productivos sostenibles. Finalmente, el enfoque regulatorio promueve un internet libre pero seguro, base de una sociedad del conocimiento robusta y confiable.

3.2.7. ALINEAMIENTO DE LA ESNACIB CON LA POLÍTICA NACIONAL MULTISECTORIAL DE SEGURIDAD Y DEFENSA NACIONAL AL 2030

La Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030[35] aprobada mediante el Decreto Supremo N° 055-2021-DE, es un instrumento clave para la seguridad y defensa del Perú, establece lineamientos y acciones para garantizar la seguridad y defensa del país al 2030. La ESNACIB, se alinea al objetivo de **"1. Garantizar la defensa de los intereses nacionales destinados a la paz y seguridad internacional"** al fortalecer la cooperación cibernética regional y global, promoviendo la confianza digital entre Estados. A través del intercambio de inteligencia, la adhesión a marcos internacionales de Ciberseguridad y la participación activa en foros multilaterales, el Perú contribuye a la estabilidad del ciberespacio. Esta estrategia permite prevenir conflictos digitales transnacionales y combatir amenazas globales como el ciberterrorismo o el cibercrimen organizado. Así, la Ciberseguridad nacional se proyecta como un sustento clave para la paz y la seguridad internacional.

Asimismo, se alinea con el objetivo **"2. Garantizar el normal funcionamiento de la institucionalidad política-jurídica-social en el país.",** contribuyendo a garantizar el normal funcionamiento de la institucionalidad política, jurídica y social fortaleciendo la protección de los sistemas informáticos del Estado frente a ciberataques que puedan afectar la gobernabilidad, la justicia y la participación democrática. Establece protocolos para la continuidad operativa y resiliencia digital de las entidades públicas. Además, promueve la integridad de la información y la lucha contra la desinformación y manipulación digital, preservando la confianza ciudadana en las instituciones.

Se alinea con el objetivo **"3. Alcanzar las condiciones necesarias contribuyentes a la Seguridad Nacional",** ya que la ESNACIB, fortalece las condiciones para la Seguridad Nacional estableciendo un marco integral de prevención, detección y respuesta ante amenazas cibernéticas que ponen en riesgo la estabilidad del Estado. Impulsa la cooperación interinstitucional y el desarrollo de capacidades tecnológicas para proteger infraestructuras críticas y datos sensibles. Así, garantiza la continuidad operativa y resiliencia frente a ataques digitales, asegurando un entorno seguro para el desarrollo político, económico y social del país.

[35] Enlace web: https://www.gob.pe/institucion/mindef/informes-publicaciones/3212559-politica-nacional-multisectorial-de-seguridad-y-defensa-nacional-al-2030

Todo lo antecedido, se logra mediante una arquitectura nacional de Ciberseguridad que articule a las fuerzas armadas (FF. AA), sector inteligencia (PNP), CNSD, CSIRTs y sector privado; con el fin de contribuir a los objetivos de interoperabilidad y descentralización del sistema de defensa, en aras de consolidar la soberanía digital como componente esencial de la integridad nacional.

3.2.8. ALINEAMIENTO CON LA POLÍTICA NACIONAL DE TRANSFORMACIÓN DIGITAL AL 2030

La presente estrategia, está alineada de forma transversal con la Política Nacional de Transformación Digital al 2030 (PNTD), instrumento de política pública por el cual se determinan los lineamientos, objetivos, estándares, acciones, servicios, indicadores, actividades, metas y responsables para alcanzar la Transformación Digital del país, en sus objetivos:

OP1: Garantizar el acceso inclusivo, seguro y de calidad al entorno digital a todas las personas. (Conectividad digital segura e inclusiva)

La ESNACIB, brinda el marco para proteger la infraestructura crítica y las redes de telecomunicaciones, para garantizar el acceso digital sin riesgos. Promueve el establecimiento de protocolos de seguridad para proveedores de internet, evitando interrupciones por ciberataques. Apoya a la inclusión digital con medidas de protección para poblaciones vulnerables. Así, asegura que la conectividad sea accesible, estable y resistente a amenazas.

OP2: Vincular la economía digital a los procesos productivos sostenibles del país. (Gobernanza digital con seguridad integrada)

Este objetivo busca integrar la economía digital con procesos productivos sostenibles, lo cual requiere una base sólida de ciberseguridad para garantizar la integridad, disponibilidad y confidencialidad de los sistemas digitales. La ESNACIB se alinea al proporcionar lineamientos para proteger infraestructuras críticas. (Pilar 2), fomentar la cultura de seguridad (PIlar 7) y gestionar riesgos tecnológicos (Pilar 4). Esta sinergia permite que la transformación digital en sectores productivos sea resiliente y confiable. Además, fortalece la confianza en plataformas digitales, impulsa la innovación segura y protege la continuidad operativa. Así, la ciberseguridad se convierte en un habilitador clave para el desarrollo sostenible digital del país.

Asimismo, la ESNACIB, establece el uso de estándares internacionales reconocidos junto con marcos normativos (por ejemplo: ISO 27001, NIST y otros de corresponder) y roles claros para entidades públicas. Establece sistemas de monitoreo y auditoría para evaluar riesgos cibernéticos debidamente controlados bajo el orden jurídico. Promueve cooperación regional e internacional frente a ciberamenazas transnacionales. Esto asegura una Transformación Digital ordenada, transparente y resiliente.

OP3: Garantizar la disponibilidad de servicios públicos digitales inclusivos, predictivos y empáticos con la ciudadanía. (Gobierno digital confiable y resiliente)

La ESNACIB, fortalece los servicios públicos digitales mediante autenticación robusta y cifrado de datos. Previene ataques a plataformas estatales que podrían afectar trámites esenciales. Implementa marcos de continuidad operativa para garantizar disponibilidad permanente. Esto refuerza la confianza ciudadana en servicios digitales inclusivos y empáticos.

OP4: Fortalecer el talento digital en todas las personas. (Talento digital con competencias en seguridad)

La ESNACIB, integra formación en Ciberseguridad en programas de capacitación digital pública y privada (Pilar 7). Fomenta certificaciones técnicas en protección de datos y respuesta a incidentes. Incentiva la especialización en áreas críticas como análisis de malware y forense digital. Así, desarrolla capacidades para enfrentar desafíos tecnológicos con enfoque seguro.

OP5: Consolidar la seguridad y confianza digital en la sociedad. (Confianza digital en el ecosistema peruano)

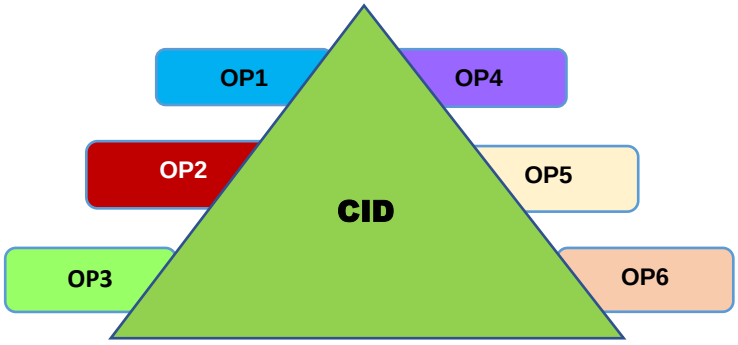
Mediante regulaciones y estándares, la ESNACIB, afianza el combate contra los fraudes en banca digital, comercio electrónico y redes sociales. Establece mecanismos de denuncia y respuesta ante ciberdelitos. Promueve alianzas con entidades, para proteger datos personales y transacciones en línea. Esto consolida un entorno digital seguro para ciudadanos y entidades.

OP6: Garantizar el uso ético y adopción de las tecnologías exponenciales y la innovación en la sociedad. (Innovación digital ética y protegida)

La ESNACIB, promueve el marco para el uso seguro de tecnologías exponenciales (IA, IoT, blockchain, computación cuántica, entre otros). Así como los riesgos como sesgos algorítmicos o violaciones de privacidad en soluciones emergentes. Fomenta

investigación en Ciberseguridad aplicada a smart cities y automatización. Así, la innovación avanza sin comprometer derechos digitales o seguridad nacional.

Figura. 13. Alineación de los principios de la información que salvaguarda la ESNACIB: C: Confidencialidad, I: Integridad y D: Disponibilidad, con los Objetivos de la PNTD.



Fuente: Elaboración propia

3.2.9. ALINEAMIENTO DE LA ESNACIB CON EL PLAN ESTRATÉGICO DE DESARROLLO NACIONAL AL 2050

En el presente plan, se considera la **visión del Perú al 2050,** en donde se detalla lo siguiente:

> *"Al 2050, somos un país democrático, respetuoso del Estado de derecho y de la institucionalidad, integrado al mundo y proyectado hacia un futuro que garantiza la defensa de la persona humana y de su dignidad en todo el territorio nacional.*
>
> *Estamos orgullosos de nuestra identidad, propia de la diversidad étnica, cultural y lingüística del país. Respetamos nuestra historia y patrimonio milenario, y protegemos nuestra biodiversidad.*
>
> *El Estado constitucional es unitario y descentralizado. Su accionar es ético, transparente, eficaz, eficiente, moderno y con enfoque intercultural.*
>
> *Juntos, hemos logrado un desarrollo inclusivo, en igualdad de oportunidades, competitivo y sostenible en todo el territorio nacional, que ha permitido erradicar la pobreza extrema y asegurar el fortalecimiento de la familia."*

Al respecto, la ESNACIB se alinea con esta visión al garantizar un entorno digital seguro que protege los derechos fundamentales, la privacidad y la dignidad de las personas frente a ciberamenazas. Fortalece la institucionalidad del Estado mediante la defensa de infraestructuras críticas y sistemas gubernamentales, asegurando un accionar transparente y eficiente en el ciberespacio. Además, promueve la inclusión digital con

enfoque intercultural, protegiendo la identidad y diversidad del país frente a riesgos como la desinformación y los ciberataques. Al fomentar la confianza en las tecnologías, contribuye a un desarrollo competitivo y sostenible, clave para erradicar la pobreza y reducir brechas. Así, la Ciberseguridad se consolida como un soporte para una democracia resiliente, integrada globalmente y basada en la ética y el Estado de derecho. Así también, de acuerdo con los **lineamientos referidos en este plan**, los cuales son importantes porque orientan el rumbo estratégico del país hacia un futuro más equitativo, seguro y digitalmente avanzado se tiene que la Ciberseguridad es un sustento preponderante para el desarrollo sostenible y la salvaguarda de la soberanía digital nacional. Los lineamientos son los siguientes:

Figura. 14. Lineamientos del Plan Estratégico de Desarrollo Nacional al 2050

Nota. Elaboración CEPLAN.

ESNACIB, concuerda con los siguientes lineamientos:

a) Lineamiento 3 - Impulsar la Ciencia y Tecnología para el Desarrollo Nacional: La ESNACIB asegura que el crecimiento de la ciencia y la tecnología no solo sea acelerado, sino también sostenido y protegido, creando un entorno más seguro para la innovación y el desarrollo tecnológico del país.

b) Lineamiento 4. Acelerar la Transformación Digital para la generación de valor de la sociedad: La ESNACIB, permite crear un entorno seguro y confiable para la adopción de tecnologías. Además, protege la infraestructura digital, fomenta la innovación, impulsa la economía digital y asegura la inclusión de todos los ciudadanos en el proceso de digitalización.

c) Lineamiento 6. Garantizar la defensa y seguridad nacional para el desarrollo integral del país.

La ESNACIB, se enfoca en garantizar que las infraestructuras críticas estén protegidas, mejorar la resiliencia ante ciberataques, y fortalecer las capacidades nacionales de defensa cibernética. Además, debe asegurar que la información sensible del gobierno y de sectores clave esté protegida y promover la cooperación internacional para mejorar la seguridad en el ciberespacio. Esto contribuye a la defensa integral del país y al desarrollo seguro y sostenible de la nación en un entorno cada vez más digitalizado.

d) Lineamiento 8. Comprender y gestionar el riesgo de desastres para el desarrollo integral del país.

La ESNACIB, está en concordancia con este lineamiento ya que se busca integrar la Ciberseguridad en los esfuerzos nacionales de gestión de riesgos de desastres. Esto implica la protección de infraestructuras críticas, la creación de planes de recuperación ante ciber incidentes, y el fortalecimiento de la resiliencia digital en situaciones de emergencia. Garantizando que los sistemas y datos esenciales para la respuesta a desastres sean seguros y funcionales, se contribuye al desarrollo integral y sostenible del país, incluso en tiempos de crisis.

e) Lineamiento 9. Consolidar un estado moderno, eficiente, eficaz y descentralizado al servicio de las personas, en cooperación con actores privados y la sociedad civil.

La ESNACIB está en concordancia con este lineamiento, ya que contribuye directamente a la modernización del Estado, la descentralización de servicios, y la cooperación efectiva entre el sector público, privado, la academia y la sociedad civil. La

Ciberseguridad es un habilitador clave para lograr un gobierno eficiente, autónomo y seguro, que brinde servicios digitales de calidad a la población fomentando la innovación y la confianza ciudadana en las tecnologías emergentes. Así se asegura a una Transformación Digital inclusiva y resiliente.

Finalmente, se tiene el enfoque sistémico de los objetivos nacionales, tal y como se muestra:

Figura. 15. Enfoque Sistémico de los Objetivos Nacionales del Plan Estratégico de Desarrollo Nacional al 2050

Nota: Fuente: Plan Estratégico de Desarrollo Nacional al 2050

Al respecto, la ESNACIB, es fundamental para el éxito del **Objetivo Nacional Nº3 (Competitividad e Innovación) del Plan Estratégico de Desarrollo Nacional al 2050 del Perú**, porque al garantizar la seguridad en el ciberespacio, se protege la infraestructura digital, se fomenta la confianza en la adopción de nuevas tecnologías, se mejora la productividad y la competitividad de las empresas u organizaciones, se atraen inversiones y se facilita la creación de un entorno propicio para la innovación. Del mismo modo, contribuye al **Objetivo Nacional N°4 (Democracia y paz)**, al proteger los sistemas estatales y privados contra ciberamenazas, asegurando un Estado efectivo y

una sociedad justa. También se vincula con el **Objetivo Nacional N° 2 (Territorio sostenible)**, ya que la gestión de riesgos cibernéticos es clave para reducir amenazas en un mundo hiperconectado, especialmente frente a desastres naturales o crisis climáticas que requieren comunicaciones seguras. Finalmente, la ESNACIB, impulsa el **Objetivo Nacional N°1 (Desarrollo de capacidades)**, al fomentar habilidades digitales en la población y reducir brechas tecnológicas. Sin embargo, su mayor impacto radica en la competitividad y gobernanza, al ser un habilitador crítico para la digitalización segura y la confianza en las instituciones, sustento del desarrollo nacional.

En resumen, la ESNACIB, no solo es una necesidad operativa, sino un elemento clave para impulsar el crecimiento económico y la innovación en el Perú del futuro.

3.2.10. ALINEAMIENTO DE LA ESNACIB CON EL PLAN ESTRATÉGICO SECTORIAL MULTIANUAL – PESEM 2024-2030 SECTOR PRESIDENCIA DEL CONSEJO DE MINISTROS

Según la Guía del PESEM del CEPLAN, los Objetivos Estratégicos Sectoriales (OES) representan las transformaciones que el sector público pretende lograr en favor de la ciudadanía y su entorno, en el marco de sus competencias institucionales. Estos objetivos se definen a partir de la visión de futuro del sector y sus prioridades estratégicas. A continuación, se presentan los OES establecidos en el PESEM 2024-2030 del Sector Presidencia del Consejo de Ministros:

Figura. 16. Objetivos Estratégicos Sectoriales (OES)

Objetivos Estratégicos Sectoriales	
Código	OES
OES 1	Mejorar la gobernanza territorial a nivel nacional
OES 2	Reducir la vulnerabilidad de la población y sus medios de vida frente a la ocurrencia de emergencias y desastres en el territorio nacional
OES 3	Incrementar la transformación digital y las capacidades científicas, tecnológicas y de innovación en el territorio nacional
OES 4	Optimizar la eficacia de las políticas públicas a nivel nacional

Nota: Fuente: Plan Estratégico Sectorial Multianual de la PCM - PESEM 2024-2030

LA ESNACIB, se alinea con el "**OES3: Incrementar la Transformación Digital y las capacidades científicas, tecnológicas y de innovación en el territorio nacional",**

directamente ya que la estrategia, busca fortalecer las capacidades tecnológicas y de innovación para garantizar un entorno digital seguro. La Ciberseguridad es un pilar fundamental en la Transformación Digital, pues sin ella no se puede asegurar la confiabilidad de los sistemas ni la protección de datos. Asimismo, también guarda relación con el **"OES4: Optimizar la eficacia de las políticas públicas a nivel nacional"**, dado que la ESNACIB requiere de marcos normativos y políticas públicas firmes para su implementación efectiva.

De otro lado, el **"OES2: Reducir la vulnerabilidad de la población y sus medios de vida frente a emergencias",** puede vincularse indirectamente con la ESNACIB, considerando que los ciberataques son una forma de emergencia digital que afecta infraestructuras críticas y servicios esenciales. Finalmente, el **"OES1: Mejorar la gobernanza territorial"** se alinea con la estrategia en parte, ya que se enfoca más en aspectos administrativos y descentralización, sin embargo, una buena gobernanza puede facilitar la coordinación interinstitucional en Ciberseguridad.

En conclusión, la ESNACIB se relaciona claramente con los objetivos estratégicos sectoriales OES3 y OES4, mientras que el OES2 tiene una conexión parcial y el OES1 una relación tangencial.

3.3. ESTADO ACTUAL DE LA CIBERSEGURIDAD A NIVEL INTERNACIONAL

El ciberespacio está en constante cambio, lo que lo convierte en un entorno extremadamente complejo. Cuando esto se combina con ciberataques y ataques físicos a infraestructuras de un país, se demuestra lo perjudiciales que pueden ser. Es por ello que la proliferación de los ciberataques a nivel global, hace evidente la necesidad de contar con un marco legal robusto que permita prevenir, detectar y mitigar riesgos en el ámbito digital.

Figura. 17. Informe Global Cybersecurity Outlook 2025.

Uno de los organismos que muestra su preocupación por el tema, es el Foro Económico Mundial (WEF) (Ver figura 2), el cual concluyó en el año 2024 que la Ciberseguridad representa un riesgo global en múltiples horizontes temporales, con amenazas y riesgos como el malware, los deepfakes y la desinformación respectivamente, que ponen en peligro las cadenas de suministro, la estabilidad financiera y la democracia y advirtió que para el 2025, la creciente habilidad de los ciberdelincuentes, los avances acelerados en

tecnologías emergentes y la expansión de las capacidades cibernéticas crearán un ciberespacio más complejo que nunca (Global Cybersecurity Outlook 2025, s. f.).

Figura. 18. Diferencias regionales en la ciberresiliencia

Fuente: Elaboración propia, adaptada y traducida al español del "Global Cybersecurity Outlook 2025. World Economic Forum"

De la figura anterior, se puede apreciar que existe en América Latina, un claro 42% de entidades que, **no están seguras** de que el país en el que tienen su sede o su organización está bien preparado para responder a ciber incidentes importantes que afecten a su infraestructura crítica. Asimismo, también dentro del reporte se destaca lo siguiente:

Figura. 19. La Ciberseguridad se está volviendo cada vez más compleja

Fuente: Elaboración propia, adaptada y traducida al español del "Global Cybersecurity Outlook 2025. World Economic Forum"

Respecto a la figura anterior, se puede concluir que, conforme los ciberdelincuentes incorporan herramientas cada vez más avanzadas, el panorama de amenazas en constante evolución requiere el desarrollo de estrategias innovadoras para enfrentar ataques cada vez más sofisticados y de mayor alcance.

De acuerdo con Forrester (2024), el 21% de las infracciones de seguridad en las entidades durante el último año fueron causadas por ataques externos dirigidos específicamente al entorno de trabajo remoto o al hogar de los empleados.

Asimismo, Albarrán y Albarrán (2024), en el informe de las Naciones Unidas, publicado por la Unión Internacional de Telecomunicaciones (UIT), evalúa el progreso mundial para ofrecer un futuro digital seguro para todos. Como principal conclusión indica que, aunque se ha avanzado mucho, todavía es necesario intensificar las medidas de protección.

A continuación, se detallan algunas estadísticas actuales sobre la Ciberseguridad a nivel global:

a) Aumento de los ciberataques. - Según "Cybersecurity Ventures", los costos globales por ciberataques se dispararán de $3 billones (2025) a $10.5 billones anuales para los próximos años. (eSentire Inc., 2024).

b) Impacto de las violaciones de datos. - El Informe de Brechas de Datos de IBM 2024, indicó que el costo promedio global de una violación de datos aumentó de 4,45 millones de dólares en 2023 a 4,88 millones en 2024, lo que representa un incremento del 10%, el mayor aumento desde la pandemia. Este incremento se atribuye al aumento del costo de la pérdida de negocio, incluyendo el tiempo de inactividad operativa y la pérdida de clientes, y al costo de las respuestas posteriores a la vulneración, que incluyen la dotación de personal para atención al cliente y el pago de multas más elevadas (Cost Of A Data Breach 2024 | IBM, s. f.)

c) Ciberseguridad y pequeñas empresas. - Según un informe de Veeam, más del 50% de las pequeñas y medianas empresas (PYMES) han sido víctimas de un ataque cibernético en los últimos 12 meses. Se estima que el 60% de las pequeñas empresas cierren dentro de los seis meses después de sufrir un ataque cibernético grave (2024 Data Protection Trends Report - VEEAM, s. f.). Asimismo, el 70% de los ciberataques son dirigidos a empresas medianas y pequeñas, lo que indica un crecimiento de los ataques dirigidos a organizaciones de menor tamaño.

d) El uso de la Inteligencia Artificial (IA) en Ciberseguridad está en aumento. El uso de esta tecnología emergente experimenta un crecimiento proyectado del 40% anual para los

próximos años.!! La IA generativa está en la caja de herramientas de los adversarios: los adversarios utilizaron cada vez con más frecuencia la IA generativa (genAI) en el 2024 para mejorar la ingeniería social, acelerar las operaciones de desinformación y respaldar actividad maliciosa en la red (Global Threat Report, 2025)

e) Brecha de habilidades en Ciberseguridad. - Según el informe de (ISC[36]), existe una escasez global de más de 3.4 millones de profesionales en Ciberseguridad, lo que dificulta a las empresas y gobiernos responder adecuadamente a las amenazas cibernéticas, ya que el 50% de las organizaciones a nivel mundial afirman que tienen dificultades para cubrir vacantes relacionadas con la Ciberseguridad (Cybersecurity Workforce Study, s. f.).

Estas estadísticas reflejan la creciente amenaza que representan los ciberataques y la necesidad urgente de mejorar la Ciberseguridad a nivel mundial.

3.4. DESAFÍOS ACTUALES RELACIONADOS CON LA CIBERSEGURIDAD EN EL PERÚ

El ciberespacio se ha convertido en un campo de operación clave para actores tanto legítimos como maliciosos. Las amenazas cibernéticas son cada vez más sofisticadas y pueden tener un impacto directo en la seguridad nacional, la economía y la confianza pública.

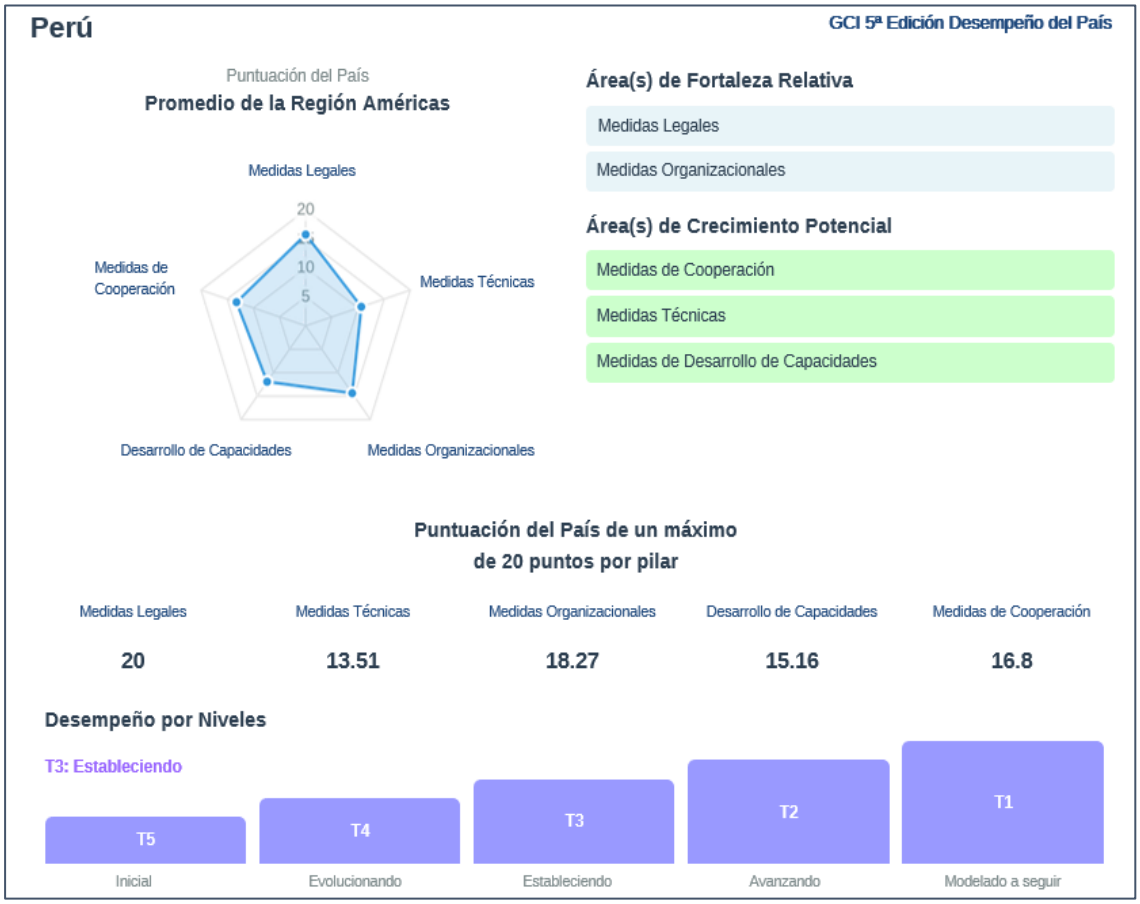
Figura. 20. República del Perú

Perú ha avanzado notablemente en el desarrollo de un marco normativo y políticas públicas robustas en Ciberseguridad, lo que se refleja en su posición relativamente alta en el **Índice Global de Ciberseguridad 2024**. Si bien estos esfuerzos demuestran un compromiso claro con mejorar la resiliencia digital a nivel nacional, no es suficiente ya que el país, al igual que otros países, enfrenta retos significativos debido a estas amenazas especialmente en la protección de infraestructuras críticas y datos personales. El gobierno, desde la **SGTD-PCM, considera que la Ciberseguridad,** continúa siendo una preocupación, pero sobre todo **una prioridad en las agendas de las entidades públicas y privadas en el país**, es por ello que es crucial continuar ampliando la capacitación y la inversión preventiva para consolidar estos logros. En el 2024 y proyectándose hacia el 2025, se han impulsado diversas iniciativas enfocadas en fomentar la cooperación interinstitucional y la sensibilización

[36] ISC: Consorcio internacional de Certificación de Seguridad de Sistemas de Información

ciudadana sobre riesgos cibernéticos, fortaleciendo sus medidas técnicas y afianzado el desarrollo de capacidades en los Oficiales de Seguridad y Confianza Digital y de los especialistas en Ciberseguridad a nivel nacional, buscando consolidar un ecosistema más seguro y resiliente a nivel nacional.

Figura. 21. Ciberseguridad en Perú, desempeño del país, según el IGC 5ta Edición



Fuente: Elaboración propia, adaptada y traducida al español del "Global Cybersecurity Index 2024"

Desde la **SGTD – PCM mediante el Centro Nacional de Seguridad Digital se gestionaron y emitieron 2,320 alertas de Seguridad Digital durante el año 2024**; esto ha generado que se cree una mediana conciencia en cuanto a la protección y los riesgos relacionados con la Ciberseguridad. Hasta el momento, la PCM ha emitido ciento sesenta y seis (166) alertas integradas documento que organiza en coordinación y colaboración con el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú, en el marco de la Seguridad Digital del Estado Peruano, con el fin de que los

responsables de la Seguridad Digital de las entidades públicas y privadas, puedan conocer sobre las amenazas y las vulnerabilidades que aquejan al entorno digital y así advertir las situaciones que pudieran afectar la continuidad de los servicios y operaciones en favor de la población.

Respecto a los ciberataques, en lo que va del 2025, el 62% de los mismos en Perú tuvo su origen en campañas de phishing, una técnica de engaño que sigue siendo altamente efectiva para los ciberdelincuentes; así lo comunica una compañía del sector privado especializada en Ciberseguridad, a través de su telemetría sobre amenazas digitales en el país. Además, según el "Diario Oficial El Peruano", en su artículo ***"Perú Lidera el Ranking de Detecciones de Amenazas Cibernéticas En Latinoamérica"***, menciona que nuestro país encabezó la detección de ciberamenazas en la región durante el primer semestre de 2024, seguido por México, Ecuador, Brasil y Argentina. También, se revela que, en promedio, se registran 2.6 millones de muestras únicas de malware en Latinoamérica. Dentro de este contexto, Perú destacó con 908,803 tipos únicos de archivos maliciosos detectados, la cifra más alta de la región. Entre estas amenazas prevalecen diversas variantes como inyectores, troyanos, downloaders, gusanos, exploits, backdoors, spyware, rootkits y droppers. Estos tipos de malware representan los vectores de ataque más frecuentes en el país.

Siguiendo la perspectiva de observancia en el sector privado, de acuerdo con el documento: "Global threat report" para el 2025, emitido por otra empresa privada, se conoce que los atacantes o ciberdelincuentes, han alcanzado velocidades sin precedentes en su velocidad de ataque; en el 2024, el tiempo promedio de comprometimiento, es decir, el lapso que tarda un atacante en pasar de un equipo inicialmente vulnerado a otro dentro de la organización o entidad objetivo se redujo a solo **48 minutos**. También, se registró el tiempo de comprometimiento más rápido hasta la fecha, alcanzando un récord de apenas **51 segundos**, lo que evidencia una creciente eficiencia operativa por parte del ciberdelincuente, gracias a la automatización y sofisticación de sus técnicas y herramientas.

También se cita en este reporte que, los métodos de acceso utilizados por los ciberdelincuentes han evolucionado rápidamente ya que, en este mismo año, los adversarios recurrieron con mayor frecuencia a técnicas de ingeniería social avanzadas, como el vishing (phishing por voz), el phishing mediante llamadas de devolución y la manipulación de los servicios de asistencia técnica para infiltrarse en redes objetivo.

Además, se apoyaron de forma significativa en credenciales comprometidas, aprovechando un mercado en expansión: los anuncios de "access brokers" que comercializan credenciales válidas robadas aumentaron en un 50% anual.

De hecho, el 52% de las vulnerabilidades observadas en el reporte precedido, durante el año estuvieron vinculadas al acceso inicial, destacando este vector como uno de los principales puntos críticos de la ciberdefensa actual. Grupos avanzados en la ciberdelincuencia emplearon estas técnicas para robar credenciales, mantener acceso persistente y eludir controles de seguridad. Finalmente, también se acota que la inteligencia artificial generativa (GenAI) se ha consolidado como una herramienta clave en el arsenal de los adversarios, su uso se intensificó notablemente en año pasado, para perfeccionar **tácticas de ingeniería social, agilizar campañas de desinformación y potenciar diversas actividades maliciosas en entornos digitales**. Gracias a sus capacidades para generar **contenido convincente de forma automatizada**, **la GenAI, ha permitido a los atacantes operar con mayor velocidad, precisión y escala, representando un desafío creciente para las estrategias de ciberdefensa.**

Este enfoque destaca la creciente sofisticación de los actores maliciosos, que ahora combinan ataques psicológicos con herramientas técnicas para maximizar su impacto.

De igual forma, según datos registrados por la empresa Karspersky, **el país registró más de 64 millones ataques durante el 2024** asimismo, el incremento de sofisticación de ataques y el mal uso de la IA, pone en peligro a las entidades de sufrir daños financieros y de reputación.

Entre los principales retos que el Perú debe afrontar, sobresalen:

- **Aumento de ataques cibernéticos**: Ataques de ransomware, phishing, DDOs, malware en su diferente tipología, entre otros que traen como consecuencia la eliminación de información, robo de datos, distorsión en la data, divulgación y otros, que afectan tanto a entidades del sector público y privado.
- **Falta de cultura en Ciberseguridad**: Muchos usuarios y organizaciones en Perú aún no aplican buenas prácticas de Ciberseguridad, lo que aumenta el riesgo de ser víctimas de incidentes cibernéticos.
- **Ciberdelincuencia organizada**: La proliferación de grupos cibercriminales que operan en el ámbito nacional e internacional con fines financieros, políticos o ideológicos.

A pesar de ello, y de forma progresiva, se está avanzando en términos de legislación en estos ámbitos, especialmente en lo que respecta a la Ciberseguridad y el desarrollo de estrategias de Ciberdefensa. Esto pone de manifiesto la necesidad de contar con una **Estrategia Nacional de Ciberseguridad**, ya que, como se ha señalado, la Ciberseguridad se relaciona estrechamente con la Seguridad Digital, en consecuencia, para enfrentar los ciberataques, es fundamental tomar medidas de protección que involucren una estrecha colaboración entre los

sectores público y privado, garantizando al mismo tiempo que estas acciones sean compatibles con los derechos y libertades individuales consagrados en la Constitución Política del Perú.

3.5. CIBERATAQUES ACTUALES Y TENDENCIAS PARA LOS PRÓXIMOS AÑOS QUE AFECTARÍAN AL PAÍS

Según el Instituto Nacional de Ciberseguridad (INCIBE) y algunas entidades del sector privado, opinan que existe la tendencia de que ciertos ataques perdurarán para los próximos años, incluso haciéndose más sofisticados utilizando las tecnologías emergentes, tales como la IA, la nube, Computación Cuántica, etc. Aquí se presenta un resumen de los principales ciberataques actuales y los que posiblemente serían recurrentes:

Figura. 22. Utilización del MFA para autenticación

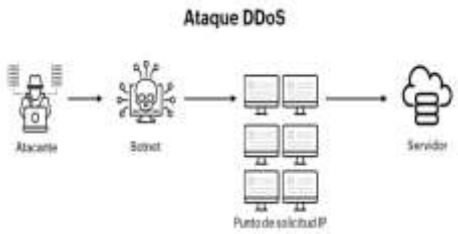
3.5.1 Ransomware

Imagen	Descripción
	Los ataques de ransomware, en los cuales los ciberdelincuentes secuestran los sistemas o datos de una víctima, cifrando los datos para exigir un rescate a cambio de la clave para restaurarlos, se han incrementado en Perú. Este tipo de malware afecta tanto a empresas privadas como a instituciones gubernamentales y servicios esenciales.

3.5.2 Ciberataques a Infraestructuras Críticas

Imagen	Descripción
	La Ciberseguridad en sectores clave, como energía, telecomunicaciones y salud, es cada vez más vulnerable. Los atacantes apuntan a estos sectores para desestabilizar servicios públicos u obtener acceso a información sensible.

3.5.3 Ataque DDOS

Imagen	Descripción
	Un ataque DDoS o denegación de servicio distribuido es un ataque DoS, pero lanzado por múltiples equipos informáticos o tecnológicos. El ciberdelincuente infecta uno o varios equipos informáticos o tecnológicos, a los que denominaremos equipos zombis o botnets, y tras adquirir el control, lanza el ataque DDoS. Este ataque consiste en coordinar a todos los equipos zombi para dirigir un ataque basado en realizar solicitudes sucesivas a una dirección IP, como en el caso anterior, provocando su colapso.

3.5.4 Phishing, Vishing y Smishing

Imagen	Descripción
 	El **Phishing,** sigue siendo una de las principales amenazas. Los atacantes se hacen pasar por organizaciones legítimas para obtener información sensible. El **Vishing (phishing por teléfono)** también está en auge, donde los delincuentes llaman a las víctimas haciéndose pasar por representantes de empresas o bancos para obtener datos personales o financieros. El **Smishing**, es una táctica en la que un ciberdelincuente envía un mensaje de texto (SMS) a un usuario, haciéndose pasar por una entidad legítima, como una red social, banco o institución pública, con la intención de robar información personal o realizar un cargo económico. Usualmente, el mensaje incita al usuario a llamar a un número con tarifas especiales o a ingresar en un enlace que lleva a un sitio web fraudulento bajo un falso pretexto.

3.5.5 Fraude digital y estafas en línea

Imagen	Descripción
	El aumento de las compras y transacciones en línea ha conllevado a un crecimiento del fraude digital, impactando tanto a consumidores como a empresas. Entre los fraudes más comunes se encuentran las compras no autorizadas, el robo de identidad y la creación de sitios web falsos destinados a obtener información personal.

3.5.6 Ciberataques a dispositivos IoT

Imagen	Descripción
	Con el crecimiento del Internet de las Cosas (IoT), los dispositivos conectados se han transformado en objetivos codiciados para los ciberdelincuentes. Muchos de estos dispositivos presentan fallos de seguridad que pueden ser aprovechados para infiltrarse y atacar redes más amplias.

3.5.7 Ingeniería social

Imagen	Descripción
	Las técnicas de manipulación psicológica para obtener información sensible continúan siendo un problema importante. Los atacantes utilizan el perfil público de las personas en redes sociales para diseñar ataques altamente específicos.

3.5.8 Ciberataques impulsados por la IA (AI-powered cyberattacks):

Figura. 23. IA pensando como un humano y más

Un ciberataque utilizando la IA es un tipo de ataque malicioso en el que se utiliza inteligencia artificial para automatizar, optimizar o evadir medidas de seguridad, permitiendo a los atacantes realizar acciones más sofisticadas, rápidas y difíciles de detectar.

Estos ataques pueden ser:

- **Phishing Generativo con IA**.
- **Ataques de fuerza bruta optimizados por IA.**
- **Deepfakes para suplantación de identidad**.
- **Malware adaptativo que evade detección**.

A continuación, se mostrará los impactos de la IA en la Ciberseguridad:

Figura. 24. El triángulo de impactos de la IA en la Ciberseguridad

Nota: Adaptada al español por la SGTD – PCM, fuente: Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards

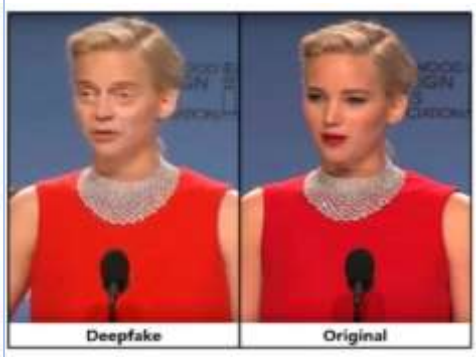
a) Phishing Generativo con IA

Imagen	Descripción
	Se refiere al uso de modelos de inteligencia artificial generativa, como los LLM (modelos de lenguaje), para crear contenido de phishing más creíble, personalizado y contextualizado, generando mensajes hiperrealistas según el objetivo que se persigue, comúnmente se utiliza para robar credenciales bancarias, pero también lo pueden utilizar bajo otro propósito. Estos son algunos ejemplos: • Correos que imitan el estilo de escritura de una persona específica. • Creación de conversaciones en tiempo real para ataques por chat (vishing, smishing). • Generación de mensajes personalizados basados en perfiles públicos (LinkedIn, redes sociales). **Cómo funciona:** 1. Los atacantes usan modelos de lenguaje (como GPT) para generar correos o mensajes de phishing altamente personalizados, imitando el estilo de comunicación de una empresa o contacto conocido. 2. La IA analiza redes sociales y datos públicos para hacer los mensajes más convincentes. 3. El ataque se escala masivamente, con cada mensaje adaptado a la víctima. **Ejemplo:** *"Hola [Nombre], soy [Gerente de tu Banco]. Hemos detectado actividad sospechosa en tu cuenta. Por seguridad, verifica tu identidad aquí: [Enlace Malicioso]. Atentamente, Soporte al Cliente."* **Objetivo:** Robar credenciales bancarias.

b) Ataques de fuerza bruta optimizados por IA

Imagen	Descripción
	Es una variante mejorada del ataque tradicional de fuerza bruta, donde la inteligencia artificial (IA) se utiliza para acelerar y optimizar el proceso de adivinación de credenciales, contraseñas o claves criptográficas. **a) Aprendizaje automático (ML):** La IA analiza patrones en contraseñas comunes, comportamientos de usuarios o estructuras de datos para priorizar intentos más probables. ***Ejemplo:*** *Si un sistema bloquea intentos fallidos, la IA puede ajustar la estrategia para evitar detección.* **b) Reducción del espacio de búsqueda:** En lugar de probar todas las combinaciones posibles, la IA filtra opciones poco probables basándose en bases de datos de contraseñas filtradas o hábitos de los usuarios. **c) Ataques adaptativos:** La IA puede cambiar dinámicamente su enfoque según las respuestas del sistema (Ej.: tiempos de respuesta, mensajes de error). **d) Uso de redes neuronales y modelos generativos:** Modelos como GPT o GANs pueden generar contraseñas realistas basadas en datos entrenados. ***Ejemplos de aplicación:*** • Desarrollo de diccionarios inteligentes: Listas de contraseñas priorizadas por probabilidad. • Ataques a CAPTCHAs: Uso de visión por computadora para resolver desafíos de forma automatizada. • Credential stuffing: Mejorar la eficiencia al probar credenciales robadas en múltiples servicios.

c) Deepfakes para suplantación de identidad

Imagen	Descripción
	Es un ataque cibernético que utiliza en su técnica la inteligencia artificial (IA) la cual utiliza algoritmos de aprendizaje profundo (deep learning) para crear contenido multimedia falso pero muy realista, como imágenes, videos o audios. Estos algoritmos permiten manipular o generar rostros, voces o acciones de personas de manera convincente, haciendo parecer que alguien dijo o hizo algo que nunca ocurrió. El Impacto que tiene este ataque es a la confianza pública y la seguridad nacional de materializarse, en especial pueden generar: • Desinformación: Los deepfakes pueden usarse para manipular la opinión pública o difundir noticias falsas. • Pérdida de confianza: La existencia de deepfakes hace que sea más difícil confiar en la autenticidad de los contenidos. • Violación de privacidad: Pueden usarse para crear contenido íntimo falso sin consentimiento. • Ciberacoso: Facilitan el acoso o la difamación.

d) Malware adaptativo que evade detección

Imagen	Descripción
	Es un tipo de software malicioso que modifica su comportamiento, estructura o apariencia en tiempo real para evadir los mecanismos de detección de seguridad, como los antivirus, EDR (Endpoint Detection and Response), o sandboxes.

	Este malware no es estático: puede detectar entornos de análisis, cambiar su código (polimorfismo/metamorfismo), o retrasar su ejecución hasta que esté fuera de entornos controlados.

3.5.9 Ciberataques sustentados en la computación cuántica

La computación cuántica representa un avance revolucionario en el procesamiento de información, pero también introduce riesgos significativos para la Ciberseguridad, el uso inadecuado de la misma representaría una amenaza significativa respecto a los métodos y técnicas tradicionales de salvaguarda, especialmente en lo que respecta a la criptografía.

Un atacante con una computadora cuántica suficientemente potente podría descifrar comunicaciones cifradas, robar datos bancarios, secretos corporativos o incluso documentos clasificados.

A medida que la computación cuántica avance, también se podrían diseñar nuevas formas de malware optimizadas para este entorno, capaces de evadir técnicas de detección actuales. Por ello, es crucial el desarrollo de criptografía post-cuántica, que resista ataques tanto clásicos como cuánticos. La transición debe comenzar pronto para evitar una crisis de seguridad global futura.

A continuación, se mencionan que posibles ataques pudieran darse al momento de utilizar dicha tecnología:

i) Ataques a Criptografía Actual (Romper Algoritmos Clásicos)

Imagen	Descripción
	Las computadoras cuánticas (especialmente con el **algoritmo de Shor**) pueden factorizar números grandes y resolver problemas de logaritmos discretos de manera eficiente, rompiendo sistemas como: • **RSA** (basado en factorización). • **ECC** (Elliptic Curve Cryptography) entre otros.

	Ejemplo: Un atacante con acceso a una computadora cuántica podría: • **Descifrar comunicaciones almacenadas:** Si hoy se interceptan datos cifrados con RSA (ejm: tráfico HTTPS, VPN), en el futuro podrían descifrarse cuando la computación cuántica esté disponible. • **Falsificar firmas digitales:** Romper firmas RSA/ECC para suplantar identidades en contratos o actualizaciones de software. **Impacto:** Colapso de la confianza en comunicaciones, banca, blockchain (Bitcoin usa ECC), y sistemas gubernamentales.

ii) Ataques a protocolos de internet

Imagen	Descripción
	Protocolos como **TLS/SSL** (usados en HTTPS) dependen de RSA o ECC para el handshake inicial. Un atacante cuántico podría: • **Romper el handshake** y establecer conexiones falsas (MitM). • **Descifrar sesiones antiguas** si se almacenaron registros cifrados. **Ejemplo:** Un atacante podría espiar comunicaciones "seguras" entre un banco y un usuario, o gestionar servidores de actualización de software para distribuir malware.

iii) Ataques a Sistemas de Seguridad Nacional

Imagen	Descripción
	Ciberdelincuentes o ciberterroristas que contratan algunos países, con conocimientos avanzados en este tipo de tecnología, podrían usar computación cuántica para: • **Descifrar inteligencia clasificada** interceptada años atrás. • **Comprometer sistemas militares** que dependen de criptografía clásica. **Ejemplo:** Si un país almacena comunicaciones cifradas de otro país durante décadas, con computación cuántica podría descifrarlas y obtener secretos de estado.

En los próximos años, las amenazas de Ciberseguridad en Perú se volverán cada vez más sofisticadas y específicas, impulsadas por la creciente digitalización, la adopción de tecnologías emergentes como la Inteligencia Artificial (IA), la computación cuántica entre otras y el aumento de la interconexión de dispositivos. En el 2024, los ciberataques experimentaron un incremento del 60%, destacándose casos como los ataques de ransomware, y no hay duda de que seguirán aumentando de manera exponencial. El sector más impactado fue el de banca y finanzas, representando el 45% de los incidentes reportados, mientras que las pequeñas y medianas empresas (PYMEs) peruanas sufrieron pérdidas promedio de $25,000 USD por cada ciberataque. (Fuente: Cámara de Comercio de Lima).

Este escenario subraya la necesidad de fortalecer las medidas respecto a la Ciberseguridad en todos los sectores, especialmente en aquellos más vulnerables como las PYMEs, para mitigar los riesgos y minimizar las pérdidas económicas, y no solo eso, también la protección de la infraestructura crítica y la privacidad de los datos personales se convertirán en áreas prioritarias en los próximos años. Tanto las organizaciones como los usuarios deberán mantenerse alerta y reforzar sus medidas de Ciberseguridad para enfrentar estas amenazas en constante evolución. La estrategia nacional en Ciberseguridad busca responder de manera proactiva a estos desafíos, promoviendo una cultura de prevención y resiliencia en un entorno digital cada vez más complejo.

3.6. IMPORTANCIA DE CONTAR CON UNA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD EN EL PERÚ

En respuesta a la creciente sofisticación de las ciberamenazas y a la acelerada Transformación Digital (TD), es esencial contar con una ESNACIB, que establezca las iniciativas trazando el camino para avanzar en dirección a un país ciberseguro, que fomente un esfuerzo coordinado y multidisciplinario entre todos los sectores, adoptando un enfoque integral, robusto y flexible, capaz de adaptarse con agilidad a un ciberespacio en constante evolución. Para construir un entorno digital seguro, abierto, resiliente y confiable, es crucial implementar aspectos de la Ciberseguridad, Aquí se detallan algunas razones de la importancia de implementar la ESNACIB:

a) **Protección para las Infraestructuras Críticas**: Muchos servicios esenciales, como los sistemas de salud, energía, transporte y banca, dependen de infraestructuras digitales. Una estrategia de Ciberseguridad ayuda a proteger estos sistemas contra ciberataques que podrían tener consecuencias devastadoras.

b) **Seguridad Nacional**: Los ciberataques pueden ser utilizados como herramientas de espionaje o sabotaje por parte de diferentes actores. Una estrategia de Ciberseguridad es vital para coadyuvar en proteger la soberanía y seguridad nacional.

c) **Confianza en el Entorno Digital**: Para que la economía digital crezca, es esencial que los ciudadanos y las empresas confíen en la seguridad de las transacciones y comunicaciones en línea. Una estrategia de Ciberseguridad fomenta esta confianza, promoviendo el comercio electrónico y la innovación tecnológica.

d) **Protección de Datos Personales**: Con el aumento del uso de internet y servicios digitales, la protección de los datos personales se ha vuelto crucial. Una estrategia de Ciberseguridad ayuda a prevenir el robo de identidad y otras formas de fraude.

e) **Cumplimiento Normativo**: Muchas regulaciones internacionales y acuerdos comerciales requieren que los países tengan medidas de Ciberseguridad adecuadas. Implementar una estrategia nacional asegura que el Perú cumpla con estas obligaciones y mantenga relaciones comerciales y diplomáticas sólidas.

f) **Resiliencia ante Ciberamenazas**: Los ciberataques son cada vez más sofisticados y frecuentes. Una estrategia de Ciberseguridad permite al país estar mejor preparado para prevenir, detectar y responder a estos ataques, minimizando su impacto.

g) **Desarrollo Económico**: La Ciberseguridad es un componente fundamental para el desarrollo económico sostenible. Proteger la información y los sistemas de las entidades, atrae inversiones y permite un entorno más seguro para los acuerdos y negocios.

IV. DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD (ESNACIB)

4.1. VISIÓN

Figura. 25. Un Perú ciberseguro para todos

Al 2028, el Perú será un país fortalecido en su Ciberseguridad en la región Latinoamérica, con un ecosistema digital resiliente, confiable y capaz de proteger eficazmente su información y los activos digitales que la soportan, infraestructuras críticas, y derechos ciudadanos frente a las amenazas cibernéticas. Contará con un marco normativo robusto, capacidades tecnológicas avanzadas y una cultura de conciencia digital en todos los sectores, impulsando la colaboración público-privada, la innovación y la formación de talento especializado. Esta visión promoverá la confianza en el uso de las TIC, garantizando un desarrollo socioeconómico sostenible y seguro, alineado con las principales políticas y estándares internacionales y los intereses nacionales.

4.2. OBJETIVO GENERAL DE LA ESTRATEGIA

Establecer un marco de acciones estratégicas destinadas a proteger la infraestructura crítica, las plataformas y/o infraestructuras tecnológicas, los sistemas de información, datos sensibles y todo ente o activos de información digitales, que se encuentre o relacione en el ciberespacio, así como determinar ámbitos que busquen fortalecer la capacidad de respuesta ante las amenazas cibernéticas que impactan negativamente en las entidades.

4.3. PRINCIPIOS RECTORES DE LA ESTRATEGIA

La ESNACIB, refleja el compromiso de los actores del ecosistema de Ciberseguridad para proteger al país, a sus ciudadanos y a las instituciones en el ciberespacio. A través de una gestión proactiva y coordinada, se busca fortalecer la resiliencia frente a los desafíos del entorno digital y construir un futuro seguro y confiable para todos. Con este propósito de salvaguardar la soberanía digital del país, se han establecido los principios rectores que fundamentan la presente estrategia. Cada pilar, junto con sus respectivas líneas de acción, debe garantizar el cumplimiento de estos principios. Estos se aplican tanto al sector público como al privado, la academia, la sociedad civil y la ciudadanía en general, adaptándose al contexto, los roles, las obligaciones y las responsabilidades específicas de cada actor, en

concordancia con el marco jurídico vigente. Los siguientes principios rectores orientan el desarrollo e implementación de esta Estrategia Nacional de Ciberseguridad:

1. **Liderazgo y responsabilidades:** La Ciberseguridad representa un reto que requiere un esfuerzo conjunto, con la participación del gobierno, sector privado, las instituciones académicas, la sociedad civil y cada ciudadano, una responsabilidad compartida entre todos los actores involucrados, asegura una colaboración y cooperación óptimas contribuyendo activamente a la salvaguarda del ciberespacio.
2. **Proteger los derechos digitales y de la privacidad de las personas en el ciberespacio:** En el contexto digital, la información personal y los datos privados están continuamente expuestos a riesgos que pueden ser aprovechados de forma ilícita, por ende, es fundamental asegurar que todas las personas, cuenten con un nivel de Ciberseguridad que les permita salvaguardar su identidad digital y realizar actividades en el ciberespacio con confianza en las tecnologías digitales, asegurando la confidencialidad, integridad y disponibilidad de esta información es fundamental para mantener la confianza y así seguir promoviendo el uso seguro del ciberespacio.

   Por ello, toda iniciativa debe respetar la diversidad y enfatizar la importancia de los derechos humanos como la libertad de expresión, el acceso a la información, la protección de la privacidad y la propiedad como cimientos fundamentales de la Ciberseguridad. De este modo, se busca construir una sociedad digital inclusiva y segura, basada en principios de equidad y justicia social, donde la tecnología sea un elemento clave para el desarrollo integral de las personas en todos sus ámbitos y roles sociales.
3. **Enfoque Holístico:** La Ciberseguridad abarca un amplio ecosistema de actores y elementos que interceptan diversas disciplinas y campos del conocimiento. Su impacto va más allá del ámbito tecnológico, dando lugar a estructuras complejas que demandan enfoques metodológicos sustentado en estándares internacionales y sistemas eficaces para su gobernanza. La definición de una estrategia en materia de Ciberseguridad requiere, de manera indispensable, la participación y colaboración de todas las partes interesadas, lo que implica un alto grado de coordinación y consenso para lograr decisiones efectivas y sostenibles.
4. **Proactividad en la gestión de riesgos y resiliencia cibernética:** La ESNACIB destaca la importancia de adaptarse continuamente a un ciberespacio en constante cambio, caracterizado por ciberamenazas cada vez más sofisticadas y variadas. Para enfrentar estos retos, propone un enfoque proactivo y dinámico centrado en identificar, evaluar y tratar los ciberriesgos, asegurando la integridad, confidencialidad y disponibilidad de la

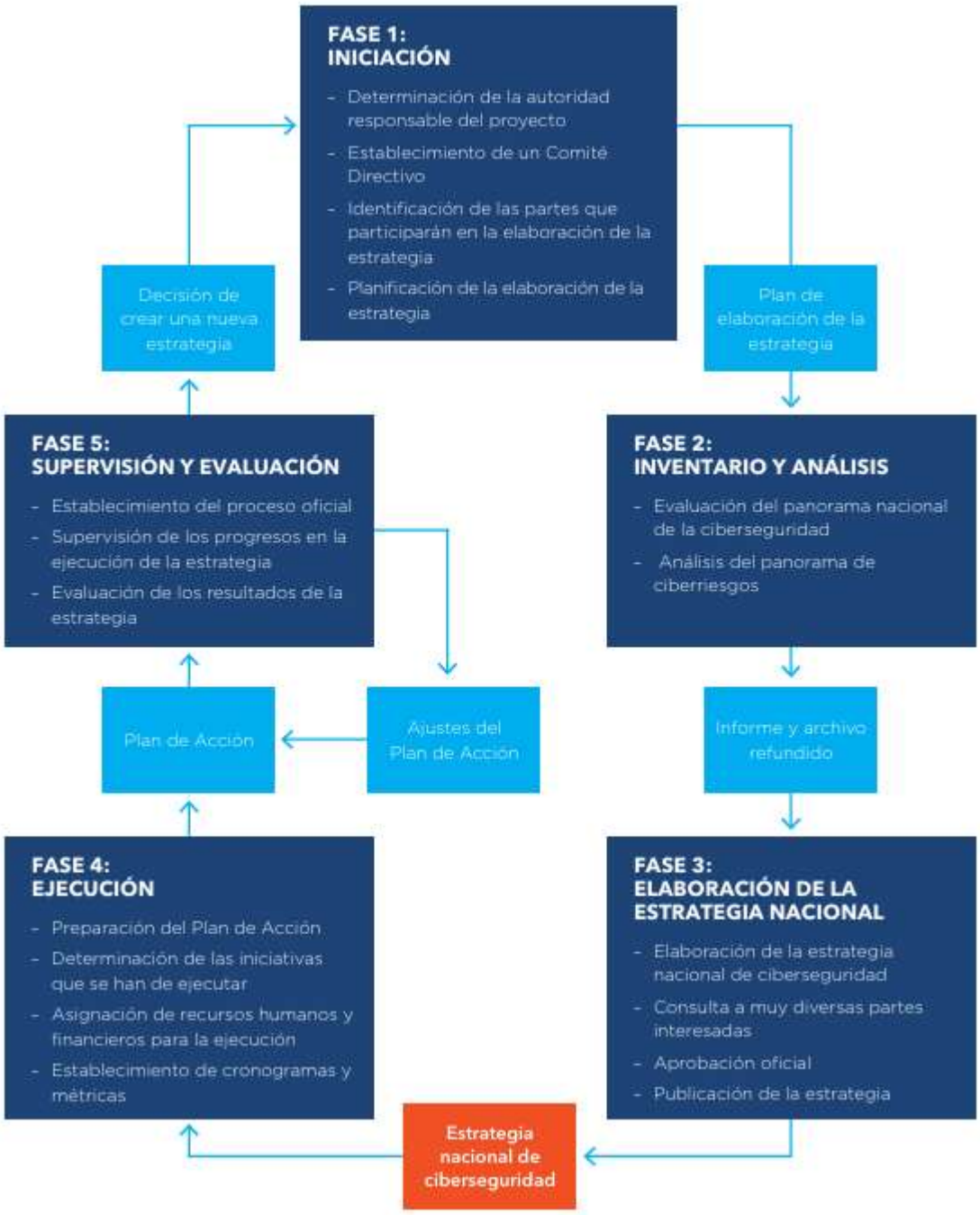
información, así como la continuidad de los servicios críticos gubernamentales. Esto implica adoptar tecnologías emergentes, fomentar una innovación tecnológica segura y mantener herramientas, políticas y procesos actualizados.

5. **Visión inclusiva y de colaboración:** La Ciberseguridad demanda un esfuerzo coordinado tanto a nivel nacional como internacional. A nivel nacional, es crucial fomentar la articulación y colaboración entre todos los actores esto implica al sector público y privado academia y sociedad civil, a fin de compartir información y recursos, fortaleciendo la resiliencia digital del país. A nivel internacional, Perú debe involucrarse activamente en foros y/u organizaciones multilaterales y regionales, contribuyendo al desarrollo de un ecosistema global de Ciberseguridad.
6. **Responsabilidades y asignación de recursos:** La Ciberseguridad debe ser una prioridad estratégica que se fomente y sostenga desde los más altos niveles de gobierno. Para asegurar la transparencia y el avance en este campo, es esencial designar coordinadores en las diversas áreas de acción y garantizar que todas las partes interesadas comprendan de manera clara sus roles y responsabilidades. Además, es crucial fomentar la inversión en investigación, desarrollo e innovación, así como promover la formación de profesionales altamente capacitados en Ciberseguridad, con el fin de fortalecer las capacidades del país frente a los desafíos digitales actuales y futuros.
7. **Entorno de Confianza:** Fomentar la confianza en el ecosistema digital nacional, protegiendo los derechos e intereses de los usuarios y garantizando la seguridad de los activos de información digitales, para aprovechar las oportunidades sociales, políticas y económicas que ofrecen las TIC, es crucial. La ESNACIB, impulsa políticas, procesos y medidas a nivel nacional para proteger servicios esenciales como las Infraestructuras críticas, Comercio Electrónico, entre otros relacionados con el Gobierno y la Transformación Digital; estas acciones promueven la confianza tanto en la ciudadanía como en las organizaciones públicas y privadas que ofrecen servicios basados en las TIC, asegurando su integridad y fiabilidad.

4.4. PROCESO DE LA ESNACIB

El ciclo de vida de la ESNACIB se sustenta en el proceso que sugiere la Guía para la elaboración de una estrategia nacional de Ciberseguridad de la UIT, el cual contempla las siguientes fases:

Figura. 26. Ciclo de vida de la ESNACIB



Fuente: "Guía para la elaboración de una estrategia nacional de Ciberseguridad - Participación estratégica en la Ciberseguridad" de la UIT. Enlace Web: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf

4.4.1. Fase 1.- Iniciación

La fase inicial de la ESNACIB establece los fundamentos necesarios para su desarrollo efectivo. Durante esta etapa, es prioritario definir los procesos, los tiempos de ejecución y los actores clave involucrados en su formulación. Como resultado, se obtiene un plan de preparación que marca el cierre de esta primera etapa.

4.4.2. Fase 2.- Inventario y análisis

El objetivo de esta fase es recopilar y analizar datos que permitan evaluar el estado actual y futuro de la Ciberseguridad a nivel global y en el país, identificando riesgos clave para fundamentar la elaboración de la ESNACIB. Cómo resultado de este ejercicio se detalló un informe dirigido al Secretario de la SGTD - PCM sobre el estado de la Seguridad Digital actual, en donde se describió la postura estratégica nacional en materia de Ciberseguridad y la situación en cuanto a los riesgos.

Asimismo, antes de empezar a elaborar el documento de la estrategia, analizó y evaluó la recopilación de información, asegurándose de que:

a) Se hayan detectado las falencias y/o deficiencias en la capacidad de Ciberseguridad y proponer soluciones para mitigarlas.

b) Determinar el alineamiento de los marcos políticos, regulatorios y operativos con los objetivos estratégicos de los pilares propuestos en la ESNACIB y/o en los componentes del documento.

c) Identificar problemas críticos, como falencias en las infraestructuras crítica, en educación y formación especializada, entre otros.

d) Evaluar todos los resultados pertinentes y deseados para la ESNACIB.

Este proceso garantizó que la estrategia se base en un diagnóstico sólido y aborde los desafíos prioritarios de manera efectiva.

4.4.3. Fase 3.- Elaboración de la Estrategia Nacional

El propósito de esta fase es elaborar el texto de la estrategia con la participación activa de los principales actores del sector público, el sector privado, la academia y la sociedad civil, a través de una serie de consultas públicas enviadas a través de documentos y grupos de trabajo que se formaron, coordinado por la SGTD - PCM, se encargó de definir la visión general, la finalidad, el alcance y el ámbito de aplicación de la estrategia, se establecieron los pilares y dentro de los mismos los objetivos estratégicos generales y específicos junto con sus acciones estratégicas, previa determinación de la situación

actual (detallado en la fase 2), en función de su impacto en la sociedad, la ciudadanía y la economía, previendo la disponibilidad de los recursos financieros necesarios.

4.4.4. Fase 4.- Ejecución

La fase de ejecución representa el componente más crítico en todo el ciclo de vida de la ESNACIB. Su éxito depende de una implementación estructurada, que contemple desde el inicio la asignación adecuada de recursos humanos y financieros. Esta planificación debe integrarse como parte esencial del diseño estratégico. Generalmente, la ejecución se guía mediante un Plan de Acción elaborado, el cual proporciona una hoja de ruta clara para coordinar y llevar a cabo las actividades previstas después que se ha aprobado el documento de la ESNACIB.

4.4.5. Fase 5.- Supervisión y evaluación

Durante esta fase, la SGTD, debe establecer un proceso formal de supervisión y evaluación de la estrategia. En la etapa de supervisión, el gobierno debe garantizar que la implementación se realice conforme al Plan de Acción establecido. Posteriormente, en la fase de evaluación, tanto el gobierno como la SGTD, deben analizar si la estrategia continúa siendo relevante ante la evolución de los riesgos, si sigue alineada con los objetivos gubernamentales y cuáles ajustes o mejoras son necesarios para su efectividad.

Finalmente, contar con este proceso integral es esencial para que la ESNACIB, no solo sea un documento estático, sino una herramienta dinámica y adaptativa que fortalezca la resiliencia del país frente a las amenazas digitales emergentes.

4.5. PILARES DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

El contemplar un pilar en el contexto de la ESNACIB, es tener un eje fundamental que sostiene y estructura la implementación de medidas de seguridad para proteger los activos de información digitales de la nación. Estos pilares son esenciales para construir una estrategia holística y robusta que aborde y articule diversos aspectos de la Ciberseguridad cuyo fin sea garantizar una protección integral, los cuales se detallan a continuación:

Figura. 27. Ocho pilares de la Estrategia Nacional de Ciberseguridad (ESNACIB)

Fuente: Elaboración propia

4.5.1 GOBERNANZA Y LIDERAZGO

La Ciberseguridad es un desafío global que demanda una respuesta coordinada y eficaz a nivel nacional, donde una gobernanza sólida es esencial para proteger la infraestructura crítica, la estabilidad económica y la privacidad de los ciudadanos. La colaboración entre todos los actores clave (individuos, sociedad civil, academia, sector público y privado), es fundamental para construir una postura de Ciberseguridad robusta, resiliente y adaptada a los retos actuales. Este primer pilar estratégico se enfoca en fortalecer la gobernanza nacional, estableciendo una visión clara y objetivos definidos que guíen los esfuerzos hacia una Ciberseguridad integral. Para lograrlo, es necesario desarrollar un marco de gobernanza que delimite roles, responsabilidades y mecanismos de cooperación, así como revisar y actualizar los documentos de gestión, normativos, riesgos entre otros, para la toma de decisiones en los temas relacionados con la Ciberseguridad y de gestionar los recursos para la gobernanza sólida y sostenible de la misma a nivel nacional. Este enfoque no solo mitigará los riesgos cibernéticos, sino que también impulsará un desarrollo digital seguro y confiable, posicionando la

Ciberseguridad como un eje prioritario en los dispositivos y/o documentos de gestión. Para lograr esto se ha determinado:

OEGC1: Establecer un marco holístico de gobernanza de la Ciberseguridad nacional, dotada de capacidades de dirección y operativas, que permita definir lineamientos, políticas y mecanismos claros para que el Ecosistema Nacional de Ciberseguridad, opere de manera coordinada y efectiva.

Este enfoque asegura la protección de los intereses nacionales y fomenta el desarrollo seguro y confiable del ciberespacio en el Perú, fortaleciendo así la resiliencia y la competitividad del país en el ámbito digital.

OEEC1.1: Determinar un modelo de gobernanza multinivel en Ciberseguridad, que defina una estructura clara y eficiente para distribuir responsabilidades entre los niveles: estratégico (qué hacer), táctico (cómo hacerlo) y operacional (ejecución), con un enfoque sectorial que garantiza una gobernanza integral.

Al establecer un modelo de gobernanza multinivel sólido y eficiente, se fortalece la Ciberseguridad y se garantiza una respuesta coordinada y efectiva ante las ciberamenazas, a la par que se fomenta una cultura de sensibilización y comportamientos seguros en Ciberseguridad a nivel nacional.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC1.1

AEC1.1.1: Determinar la autoridad competente y designar responsabilidades ejecutivas de alto nivel, según la estructura organizativa definida en materia de Ciberseguridad con el fin de fortalecer la coordinación, supervisión y aplicación de las políticas y otros dispositivos de gestión y normativos nacionales relacionados con esta materia.

En lo que respecta a la autoridad competente y la designación de responsabilidades ejecutivas de alto nivel en materia de Ciberseguridad, en el marco de la ESNACIB, implica designar a autoridades del más alto nivel del Poder Ejecutivo para liderar y coordinar acciones estratégicas que garanticen la seguridad digital del país. Esta función recae principalmente en la Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital (SGTD), la SGTD - PCM, es el Ente Rector en materia de Gobierno Digital, tal y como lo señala el Artículo 8 de la Ley de

Gobierno Digital y el Artículo 5 y 6 del Decreto de Urgencia Nº 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento[37], la misma que delega funciones a nivel táctico al Centro Nacional de Seguridad Digital (CNSD)[38], el cual constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano denotadas en el Artículo 32 de la Ley de Gobierno Digital[39].

Asimismo, el "Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo", mencionado en el artículo 8 del D.S. 157-2021-PCM, en el ámbito de la Ciberseguridad, actúa como instancia responsable de la articulación intersectorial, brindando gobernanza estratégica y seguimiento a la implementación de la ESNACIB. Así, se asegura una dirección política coherente y transversal en Ciberseguridad.

En cuanto a la Estructura Organizativa Nacional de Ciberseguridad se establece la siguiente:

A. Nivel Estratégico

Objetivo: Definir políticas, lineamientos, monitorear y supervisar el cumplimiento de la ESNACIB

A.1. Secretaría de Gobierno y Transformación Digital (SGTD)

Es el ente rector del Sistema Nacional de Transformación Digital dicta las normas, lineamientos, principios, técnicas, instrumentos y establece los procedimientos en materia de Transformación Digital, mediante el cual se organizan y promueven las actividades de los miembros del sistema. Es responsable de su operación y correcto funcionamiento[40]. Asimismo, tendrá a cargo la elaboración, diseño, monitoreo, seguimiento y actualización de la ESNACIB, así como de los temas relacionados con la Ciberseguridad dentro del ámbito de su competencia según designe y corresponda.

[37] "Artículo 5. Ente Rector del Marco de Confianza Digital" y "Artículo 6. Atribuciones del Ente Rector" del "Capítulo II: Marco de Confianza Digital" del "Decreto de Urgencia Nº 007-2020. Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento." En concordancia con el "Artículo 8.- Ente Rector en Materia de Gobierno Digital" del "Capitulo I. Gobierno Digital" del "Título II. Gobierno Digital" del Decreto Legislativo Nº1412. Decreto Legislativo que aprueba la Ley de Gobierno Digital.

[38] "Artículo 7. Centro Nacional de Seguridad Digital" del "Capitulo II. Marco de Confianza Digital" del "Decreto de Urgencia Nº 007-2020. Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento", de conformidad con el "Art. 32" del "Decreto Legislativo Nº1412. Decreto Legislativo que aprueba la Ley de Gobierno Digital".

[39] "Artículo 32. Gestión del Marco de Seguridad Digital del Estado Peruano" del "Capítulo VI. Seguridad Digital" del "Título II. Gobierno Digital" del "Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital".

[40] Artículo 5: Ente rector del Sistema. Decreto Supremo Nª 157-2021-PCM. Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia Nº006-2020 Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

A.2. Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo

Es el órgano de carácter político – estratégico, constituyéndose en el mecanismo de coordinación y articulación multisectorial entre el gobierno, sector público, organizaciones del sector privado, sociedad civil, academia y la ciudadanía para el impulso desarrollo y consolidación de las materias del Sistema Nacional de Transformación Digital y de una sociedad digital, dentro de esta temática la Ciberseguridad.

B. Nivel Táctico

Objetivo: Implementar y gestionar planes, programas y proyectos alineados a la ESNACIB

B.1. Centro Nacional de Seguridad Digital (CNSD)

Responsable de la operación del Sistema Nacional de Ciberseguridad. Se encarga de analizar las ciberamenazas, gestión y respuesta ante incidentes así como de velar sobre el cuidado y de tener actualizado el Registro Nacional de Incidentes de Seguridad Digital, de realizar Ciberinteligencia, análisis forense, criptología entre otros a nivel nacional en coordinación con todas las entidades del Estado Peruano, según lo enfatiza el D.U. 007-2020 en espacial cuando se refieran a entidades que cuenten con infraestructuras críticas soportados en TIC.

B.2. Entidades responsables de la Ciberseguridad del Estado Peruano (ERCIB)

Refiere a las entidades que tiene responsabilidad directa con los pilares de la ESNACIB, para lo cual serán representados por Coordinadores establecidos formalmente y/ o representantes, según el ámbito de competencia.

B.2. Oficinas de Ciberseguridad Sectoriales (OCS)

Cada ministerio o entidad tiene una oficina o unidad encargada que coordina con el CNSD sobre la temática de Ciberseguridad. Asimismo, se encargan de implementar planes sectoriales, reporte de incidentes, capacitación, planificar los ethical hacking de las entidades de forma prioritaria de las entidades con infraestructura crítica en cada sector y llevar a cabo auditorías internas y externas al año según correspondan.

B.3. Equipo de Respuesta ante Incidentes de Ciberseguridad (CSIRT Nacionales)

Coordina la respuesta inmediata y las acciones de mitigación ante incidentes de seguridad digital, asegurando su adecuada documentación y registro conforme a los lineamientos del Registro Nacional de Incidentes de Seguridad Digital, para su posterior reporte al CNSD. Participa activamente en ejercicios de *ethical hacking*, programas de capacitación, y simulacros periódicos con el fin de fortalecer la postura de Ciberseguridad de la entidad.

B.4. Comunidad de expertos en Ciberseguridad

Unidad de apoyo estratégico, que integra a los expertos en Ciberseguridad de las demás entidades gubernamentales, el sector privado, ONG, la sociedad civil y el mundo académico, en coordinación con el CNSD. Los roles, funciones y responsabilidades de cada actor se definirán de manera clara, respaldados por instrumentos y capacidades operativas adecuadas a través de dispositivos normativos que se establezca. Esta colaboración estructurada fomentará una comunidad activa y comprometida, facilitando el intercambio de conocimientos, la cooperación estratégica y el fortalecimiento de capacidades, asimismo, contribuirá con el CNSD en aportes, sugerencias y otros relacionados a esta temática en relación a la parte táctica o técnica cuando se requiera.

C. Nivel Operacional

Objetivo: Ejecución directa de acciones técnicas, monitoreo, respuesta y protección de activos de información digitales.

C.1. Equipos Técnicos de Seguridad (SOC – Security Operations Center)

Monitorización continua de redes y sistemas conectados, así como la detección, análisis y respuesta a incidentes de Ciberseguridad.

C.2. Analistas y Especialistas en Ciberseguridad

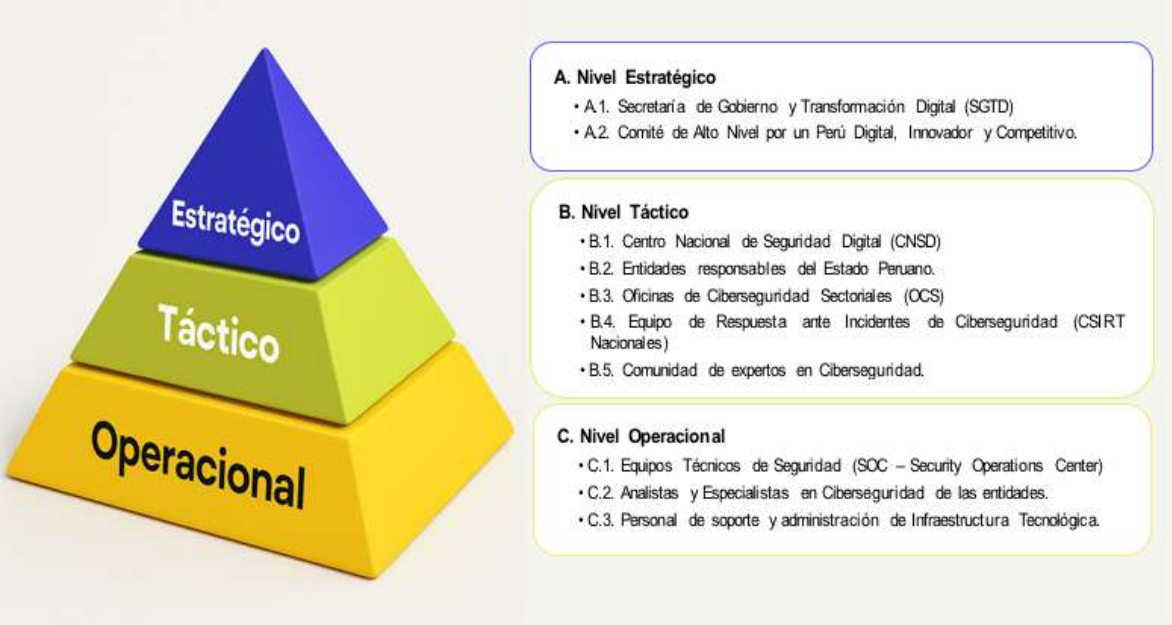
Encargados de realizar la gestión de vulnerabilidades, actualización de sistemas, pruebas de penetración, participan de los ethical hacking cuando se

realicen y de las auditorias relacionadas proporcionando la información previamente recaudada, ordenada y sistematizada.

C.3. Personal de soporte y administración de Infraestructura Tecnológica

Implementación de controles técnicos, configuración segura, mantenimiento preventivo, detectivo y correctivo.

Figura. 28. Estructura Organizativa Nacional de la Ciberseguridad



Fuente: Elaboración propia

AEC1.1.2: Fomentar el liderazgo y la asignación de recursos adecuados para la implementación de los temas relacionados con la Ciberseguridad.

Esta acción, implica promover la participación activa de altos responsables para guiar estratégicamente las iniciativas en esta área, asegurando la asignación de recursos técnicos, humanos y financieros necesarios. Esto es clave para garantizar una implementación efectiva y sostenida de las políticas y medidas de protección digital, fortaleciendo así la resiliencia y seguridad de la infraestructura crítica nacional.

AEC1.1.3: Establecer y optimizar mecanismos de coordinación para el modelo implementado, así como elaborar lineamientos, protocolos y procedimientos claros que promuevan una comunicación efectiva, el flujo ágil de información y la

colaboración estratégica entre los diversos actores nacionales involucrados en el ámbito de la Ciberseguridad.

Esto indica crear estructuras y procesos claros que faciliten una comunicación eficiente y un intercambio rápido de información entre los actores nacionales utilizando diferentes medios y herramientas que permitan una comunicación más fluida (por ejemplo, la implementación de una plataforma de comunicación formal). Además, implica desarrollar lineamientos, protocolos y procedimientos precisos que impulsen la colaboración estratégica, asegurando una respuesta conjunta y coherente frente a las amenazas digitales en el país.

AEC1.1.4: Establecer la supervisión de la implementación de la ESNACIB e implantar mecanismos regulares de seguimiento y notificación de los indicadores de Ciberseguridad.

Implica monitorear de forma continua el cumplimiento de sus objetivos, asegurando que las acciones se ejecuten según lo planificado, Además, se deben implementar mecanismos periódicos para el seguimiento y reporte de indicadores clave, por ejemplo para difundir los indicadores de compromiso el CNSD, se agenciará de un servicio automático en ayuda de reportar por parte de las entidades los ataques que se hayan perpetrado en ellas y de ser detectadas por el centro, informar de forma automática para que dicha información lo conozcan los entes involucrados para priorizar la solución, lo que permite evaluar el avance, identificar brechas y tomar decisiones informadas para fortalecer la Ciberseguridad nacional.

OEEC1.2.- Promover la formación de una comunidad cohesionada y colaborativa, integrada por expertos en Ciberseguridad provenientes de los diversos sectores y actores involucrados.

La participación activa del sector público y privado, la academia y la sociedad civil es esencial para asegurar la eficacia de las medidas y promover una cultura de Ciberseguridad. Esta comunidad, integrada por expertos de múltiples sectores, impulsará el desarrollo estratégico y la resiliencia nacional. A través de ejercicios prácticos conjuntos y redes de intercambio, se formarán expertos altamente capacitados, preparados para responder de manera rápida y coordinada ante crisis cibernéticas graves. Este enfoque colaborativo no solo fortalecerá la preparación y

respuesta ante ciberamenazas, sino que también contribuirá a construir un ecosistema digital más seguro y sostenible.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC1.2

AEC1.2.1: Establecer la comunidad de expertos en Ciberseguridad para enfrentar de manera conjunta los desafíos comunes en materia de Ciberseguridad, fortaleciendo así la capacidad de respuesta y la resiliencia nacional.

La gobernanza de la Ciberseguridad se basará en una coordinación inclusiva y articulada liderada por la SGTD – PCM como ente rector, el cual promoverá la **conformación de una comunidad teniendo como líder a un Coordinador(a) General de Ciberseguridad**[41], **el cual integrará a los expertos en Ciberseguridad de las demás entidades gubernamentales, el sector privado, ONG, la sociedad civil y el mundo académico, en coordinación con el CNSD.** Los roles, funciones y responsabilidades de cada actor se definirán de manera clara, respaldados por instrumentos y capacidades operativas adecuadas a través de dispositivos normativos que se establezca. Esta colaboración estructurada fomentará una comunidad activa y comprometida, facilitando el intercambio de conocimientos, la cooperación estratégica y el fortalecimiento de capacidades, asimismo, contribuirá con el CNSD en aportes, sugerencias y otros relacionados a esta temática en relación a la parte táctica o técnica cuando se requiera.

AEC1.2.2: Se crearán espacios de consulta y participación para integrar a las partes interesadas clave, en el diseño y ejecución de la ESNACIB.

Esto indica que se implementará un mecanismo de colaboración efectivo y seguro, que involucre a instituciones gubernamentales, el sector privado, el ámbito académico y otros, con el objetivo de establecer una plataforma integral para su participación activa. Esta plataforma facilitará: a) la consulta y recopilación de información; b) el intercambio de conocimientos y datos; c) la coordinación de acciones; y d) la cooperación operativa.

[41] El/la coordinador(a) formará parte del "Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo", debiendo asumir funciones claramente definidas y diferenciadas dentro de dicho espacio. Para preservar la segregación de funciones y evitar posibles conflictos de interés, sus responsabilidades no deben coincidir ni superponerse con las del Coordinador del CNSD. Esta separación funcional es clave para asegurar una gestión eficiente, transparente y alineada con los principios de gobernanza digital.

OEEC1.3.- Optimizar la comunicación en Ciberseguridad para una mayor eficacia y coordinación.

Una comunicación eficaz es fundamental para la Ciberseguridad, comprendiendo desde la promoción de una cultura de Ciberseguridad hasta la gestión transparente y clara de incidentes.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC1.3

AEC1.3.1: Elaborar y coordinar un plan de comunicación integral en Ciberseguridad que esté alineado con los objetivos de la estrategia actual, enfocándose en la sensibilización, prevención y respuesta frente a las ciberamenazas.

Diseñar plan de comunicación articulado, que refuerce los objetivos de la estrategia nacional vigente, promoviendo la conciencia y preparación frente a riesgos digitales. Este plan debe enfocarse en sensibilizar a los actores clave, fomentar prácticas preventivas y establecer protocolos de respuesta ante ciberamenazas y/o ciberataques. La comunicación clara y oportuna es esencial para una gestión eficaz de incidentes y una cultura de Ciberseguridad sólida en el país.

AEC1.3.2: Desarrollar un programa de difusión para garantizar una comunicación eficaz ante incidentes de Ciberseguridad, dirigido a los responsables de la toma de decisiones y a los colaboradores de las entidades públicas.

Desarrollar un programa de difusión en Ciberseguridad implica diseñar e implementar estrategias de comunicación claras y oportunas, orientadas a informar y capacitar a los responsables de la toma de decisiones en las entidades públicas y a los colaboradores. Este programa debe asegurar que, ante incidentes cibernéticos, exista una comprensión adecuada de los protocolos de respuesta y se facilite una acción coordinada y eficaz.

AEC1.3.3: Brindar formación en Ciberseguridad a los equipos de comunicación y difusión, enfocándose en cómo gestionar incidentes utilizando herramientas de comunicación efectivas.

Considera capacitar al equipo de comunicación para que se puedan manejar y entender adecuadamente los incidentes digitales, usando herramientas y técnicas comunicativas efectivas. Esto asegura que puedan transmitir información clara, precisa y oportuna,

facilitando una gestión adecuada de crisis y minimizando el impacto de los ciberataques en la percepción pública y la coordinación institucional.

AEC1.3.4: Fomentar o generar oportunidades de diálogo y colaboración con los medios de comunicación a fin de transmitir noticias y/o temática referida a Ciberseguridad.

Fomentar el diálogo y la colaboración con los medios de comunicación busca fortalecer la concientización pública sobre los riesgos y buenas prácticas en el entorno digital. Esta acción permite difundir información precisa y oportuna sobre incidentes, amenazas y medidas de prevención. Además, contribuye a construir una cultura de Ciberseguridad en la sociedad, al facilitar el acceso a contenidos educativos y alertas relevantes. Los medios actúan como aliados estratégicos en la tarea de sensibilizar y empoderar a la ciudadanía digitalmente. En suma, esta colaboración refuerza la resiliencia nacional frente a amenazas cibernéticas.

4.5.2 SALVAGUARDAR LAS INFRAESTRUCTURAS CRÍTICAS Y ACTIVOS DE INFORMACIÓN DIGITALES.

Las infraestructuras críticas del país conforman a los sistemas, plataformas, instalaciones, redes, servicios y activos físicos o virtuales, que son esenciales para el funcionamiento de una sociedad, economía y seguridad nacional. Su interrupción o daño puede tener graves consecuencias, afectando la seguridad pública, la salud, la economía y la estabilidad del estado. Estas Infraestructuras criticas comprenden a las entidades que brindan suministro de energía, agua, transporte, comunicaciones, salud, refinación y abastecimiento de combustibles, banca y finanzas[42] y seguridad. Su interrupción o destrucción tendría un impacto grave en la economía, la seguridad nacional y el bienestar social. Por su importancia, suelen estar protegidas por marcos legales y medidas de seguridad reforzadas para prevenir ataques, desastres naturales o fallos técnicos que puedan comprometer su operatividad.

[42] El sector bancario y financiero se considera una infraestructura crítica, debido a su papel fundamental en la economía y la estabilidad social. Este sector garantiza el funcionamiento de los pagos, el crédito, los ahorros y las transacciones comerciales, por lo que su interrupción podría provocar crisis económicas, pérdida de confianza en el sistema y desestabilización social. Por ello, los gobiernos y organismos reguladores implementan medidas de seguridad física y cibernética, resiliencia operativa y planes de contingencia para protegerlo frente a ciberataques, fraudes, fallos técnicos o desastres naturales. Su protección es clave para la seguridad nacional y el bienestar económico.

Los activos de información digitales esenciales en las entidades también son cruciales, en especial, los Activos Críticos Nacionales (ACN) cuyo funcionamiento es vital para el mantenimiento de servicios clave en una sociedad.

OEGC2: Fomentar la protección y resiliencia de las infraestructuras críticas del país y los activos de información digitales.

Esto se realizará mediante un enfoque integral de Ciberseguridad que minimice riesgos, asegure la continuidad operativa y fortalezca la capacidad de respuesta ante ciber amenazas, y/o ciberataques en coordinación con los responsables directos (DINI) y sectores público y privado.

OEEC2.1.- Definir un marco de objetivos y acciones de gestión en favor de la Ciberseguridad que sea aplicable a todas las entidades que conformen los sectores o cuenten con servicios críticos del país.

Definir un marco de objetivos y acciones de gestión en favor de la Ciberseguridad implica establecer lineamientos o sustentos claros y acciones estandarizadas en los documentos de gestión, procedimientos e instructivos que orienten la protección, detección, respuesta y recuperación ante incidentes digitales en las infraestructuras críticas. Este marco debe ser obligatorio y adaptable para todas las entidades públicas y privadas que operen infraestructuras o servicios críticos en el país. Su finalidad es asegurar una postura común de ciberresiliencia que garantice la continuidad y seguridad nacional.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC2.1

AEC.2.1.1: Consolidar la Ciberseguridad en un objetivo estratégico dentro de los documentos de gestión de alto nivel en las entidades que operan y/o tienen servicios o sectores críticos del país, fomentando un compromiso institucional sólido para su implementación y la asignación de recursos necesarios.

Esta acción es clave para incorporar la Ciberseguridad en la planificación institucional. Dicho objetivo deberá estar reflejado en el Plan Estratégico Institucional (PEI) o documento equivalente, así como en otros instrumentos de gestión que se encuentren

articulados. Asimismo, los planes, proyectos y otros documentos que la entidad del sector crítico desarrolle, deberá alinearse a este documento de gestión de alto nivel; dicho marco de objetivos debe ser aplicable y coherente con las responsabilidades de las entidades que gestionan servicios o sectores críticos del país, asegurando la protección y continuidad de infraestructuras esenciales. Así, se fortalece la coordinación interinstitucional y se impulsa una cultura organizacional orientada a mitigar riesgos cibernéticos y responder eficazmente ante incidentes. Esto contribuye directamente al cumplimiento de la ESNACIB y al fortalecimiento del ecosistema digital nacional.

AEC 2.1.2: Identificar y categorizar a las entidades que tengan infraestructuras críticas y/o que tengan activos críticos nacionales (ACN)[43] digitales que salvaguardar, evaluando la naturaleza de los mismos, su exposición ante las ciberamenazas (nivel de vulnerabilidad), el nivel de riesgo y su impacto potencial ante incidentes, el contexto operativo en el que se desempeñan, así como sus interconexiones y dependencias con otros actores.

Esto implica reconocer qué entidades poseen activos críticos nacionales (ACN) digitales para el funcionamiento del país. Este proceso requiere evaluar su vulnerabilidad, nivel de riesgo, impacto potencial ante incidentes y su entorno operativo. También implica analizar las interdependencias tecnológicas con otros actores para priorizar acciones de protección coordinada.

AEC 2.1.3: Implementación de protocolos de seguridad y gestión de riesgos en infraestructuras críticas y activos de información digitales del estado peruano.

Esta acción está enfocada en aplicar la adopción de estándares y mejores prácticas internacionales (ISO 27001, NIST CSF, CIS Controls, etc.), mejorar la configuración de firewalls, cifrado de comunicaciones, segmentación de redes, y controles de acceso multifactor (MFA), así como la respuesta a incidentes contra amenazas como ransomware o ataques APT junto con la alineación a marcos legales como la Ley N° 30999, todo esto Incluye gestión de riesgos para priorizar vulnerabilidades y mitigar impactos, especialmente en infraestructuras sensibles (energía, transporte, datos estatales) y activos digitales gubernamentales. El objetivo es garantizar la continuidad operativa y prevenir brechas que afecten la seguridad nacional, requiriendo coordinación

[43] Decreto Supremo N.° 106-2017-PCM aprobado el 9 de noviembre de 2017. Enlace web: https://cdn.www.gob.pe/uploads/document/file/535679/DS_N_106-2017-PCM.pdf?v=1582930272

interinstitucional, inversión en SOCs y concientización en Ciberseguridad para funcionarios públicos.

4.5.3 REGULACIÓN Y CUMPLIMIENTO

Un entorno legal bien estructurado, no solo fortalecerá el ecosistema de Ciberseguridad, sino que también servirá como herramienta fundamental para la implementación de políticas públicas en esta materia. Entre las áreas prioritarias que requieren atención inmediata se encuentran la Ciberseguridad nacional, la protección de infraestructuras críticas digitales y los activos de información digitales, la gestión de incidentes cibernéticos y la lucha contra la ciberdelincuencia. Estas áreas deben ser abordadas con normativas específicas que definan claramente los deberes y derechos de todos los actores involucrados, promoviendo así un entorno digital seguro y confiable para el desarrollo del país.

OEGC3: Robustecer el marco legal y regulatorio en Ciberseguridad, asegurando que sea firme, coherente, actualizado, completo, aprobado y difundido en el país.

En el contexto de la realidad peruana, la implementación de un marco legal y regulatorio integral en materia de Ciberseguridad se presenta como una necesidad urgente y primordial para enfrentar los desafíos del mundo digital.

OEEC3.1.- Revisar, elaborar y/o actualizar y fomentar el marco normativo en Ciberseguridad, alineándolo con estándares internacionales y buenas prácticas para garantizar su eficacia y robustez.

Este marco normativo debe ser transparente y actualizado, basado en un análisis legislativo exhaustivo que permita identificar las brechas y necesidades específicas del país. No se trata solo de crear normas por el hecho de legislar, sino de entender y abordar las demandas reales que surgen de los objetivos estratégicos enmarcados en los pilares de la ESNACIB. Es crucial evitar la sobre regulación, garantizando que las disposiciones sean proporcionales y estén alineadas con los principios de eficacia y claridad.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC3.1

AEC3.1.1: Desarrollar un marco legal holístico de Ciberseguridad, que fomente la colaboración entre el sector público, sector privado, la academia y la sociedad civil en general para el fortalecimiento de la Ciberseguridad nacional

Crear e implementar una legislación integral en Ciberseguridad, alineada con los desafíos actuales, que regule de forma transversal los aspectos clave a nivel nacional. Este marco debe garantizar seguridad jurídica, prevenir delitos informáticos, proteger los derechos digitales y definir responsabilidades claras para todos los actores del entorno digital.

AEC3.1.2: Desarrollar normatividad específica en Ciberseguridad, para la protección de infraestructuras críticas.

Diseñar regulaciones tanto sectoriales como transversales enfocadas en la protección de infraestructuras críticas nacionales y activos de información críticos digitales, atendiendo los riesgos específicos de cada sector estratégico. Estas normativas deben incluir requisitos mínimos de seguridad, gestión de incidentes, continuidad operativa y resiliencia. El objetivo es asegurar la prestación ininterrumpida y segura de los servicios esenciales. Así se fortalece la capacidad de respuesta ante amenazas y se protege el funcionamiento del país.

AEC3.1.3: Establecer un mecanismo formal y periódico para la actualización continua, de normativa y estándares internacionales relacionados con la Ciberseguridad y/o temática conexa.

Implementar un mecanismo formal y periódico para evaluar, optimizar y actualizar los estándares técnicos, normativas y protocolos nacionales de Ciberseguridad. Este procedimiento garantizará su continua adaptación a los avances tecnológicos, las nuevas amenazas digitales y los estándares globales, manteniendo así una postura de Ciberseguridad robusta y actualizada. La institucionalización de este sistema asegurará su sostenibilidad y aplicación consistente, fortaleciendo la resiliencia del país frente a riesgos cibernéticos. Además, incorporará un enfoque proactivo para anticipar vulnerabilidades emergentes y alinear las políticas locales con marcos internacionales reconocidos.

AEC3.1.4: Promoción de la aceptación y adopción de estándares internacionales de Ciberseguridad

Esa acción, indica alinear el marco normativo nacional con la adopción progresiva de estándares internacionales de Ciberseguridad (como ISO/IEC 27001, 27032 y demás ISOs relacionadas, NIST CSF, CIS Controls entre otros) aplicable al sector público en especial. Esta iniciativa busca incrementar la madurez en Ciberseguridad del país, potenciar las competencias técnicas institucionales y fomentar la interoperabilidad con esquemas globales, mejorando así la postura de Seguridad Digital peruana en el contexto internacional."

AEC3.1.5: Garantizar que el marco normativo nacional promueva y proteja la Ciberseguridad a nivel supraterritorial, alineándose con los estándares internacionales y cumpliendo con los compromisos adquiridos por el país en el ámbito internacional.

Este planteamiento se refiere a la necesidad de desarrollar un marco legal nacional en Ciberseguridad con dos ejes estratégicos: (1) efectividad supranacional (aplicable más allá de fronteras físicas, crucial para delitos transnacionales y protección de datos transfronterizos), y (2) armonización global, asegurando que las leyes locales incorporen estándares y convenios internacionales, además de honrar acuerdos bilaterales/multilaterales del Perú. El objetivo final es crear un ecosistema jurídico que fortalezca la soberanía digital mientras facilita la cooperación internacional contra ciberamenazas.

OEEC3.2.- Alinear el accionar de las entidades al cumplimiento de la normativa que se adapte referido a estándares internacionales, así como asesorar en la certificación y conformidad relacionados con la Ciberseguridad.

Fomentar que tanto las entidades públicas como privadas, así como los sistemas y procesos vinculados a la Ciberseguridad, cumplan los estándares internacionales y requisitos relacionados a la Ciberseguridad del Perú.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC3.2

AEC3.2.1: Establecer un sistema de acreditación y/o certificación que permita validar el cumplimiento de Ciberseguridad en las entidades u organizaciones

Esta acción demuestra su adherencia a las mejores prácticas de Ciberseguridad y/o Seguridad Digital en el Perú. Esta certificación será un sello de confianza para las entidades, su entorno, clientes o ciudadanos y socios.

AEC3.2.2: Establecer mecanismos para garantizar el cumplimiento de los requisitos normativos en Ciberseguridad.

Esta acción permitirá identificar posibles brechas o vulnerabilidades en el marco normativo y fomentar la mejora continua en la gestión de riesgos cibernéticos en las entidades del Sector Público de carácter mandatorio y en el sector privado de manera sugerida o a solicitud.

4.5.4 GESTIÓN DE RIESGOS, RESILIENCIA Y RESPUESTA A INCIDENTES

La gestión de riesgos es un componente esencial en cualquier proceso de desarrollo, incluyendo la Transformación Digital, la cual ofrece importantes beneficios en innovación, competitividad, crecimiento socioeconómico y mejora de los servicios públicos en Perú, sin embargo, también introduce amenazas complejas y un nuevo perfil de riesgos. La creciente dependencia de las tecnologías digitales, sumada a un entorno de amenazas externas cada vez más sofisticado, incrementa la vulnerabilidad frente a incidentes cibernéticos provocados por ciberdelincuentes, hacktivistas entre otros, si no se gestionan adecuadamente los riesgos de Ciberseguridad, pueden causar daños físicos a los activos de información digitales, interrumpiendo su disponibilidad que impactan a toda la sociedad peruana. Por ello, es crucial:

OEGC4: Gestionar de manera integral los Ciberriesgos asociados a los activos de información digitales del país, fortaleciendo las capacidades de resiliencia y respuesta ante incidentes cibernéticos, con un enfoque proactivo y sostenible.

Este objetivo se enfoca en la identificación, evaluación y mitigación proactiva de Ciberriesgos, asegurando la resiliencia de los activos de información digitales de forma especial de los sistemas críticos, e indica optimizar la capacidad de respuesta ante incidentes. Incluye la implementación de marcos o estándares internacionales para gestionar amenazas de manera estructurada. Además, promueve la adopción de planes de continuidad operativa (DRP/BCP) y la realización de simulacros periódicos para fortalecer la preparación. La coordinación con CSIRTs nacionales e internacionales

garantiza una reacción ágil y efectiva frente a ciberataques, así como es crucial establecer una respuesta nacional coordinada e integral, que articule a todos los sectores públicos y privados, asegurando una gestión sostenible y resiliente frente a las amenazas del ciberespacio.

OEEC4.1.- Establecer un proceso integral para gestionar y tratar los Ciberriesgos

Este objetivo promueve la adopción de buenas prácticas que aborden la Ciberseguridad desde un enfoque preventivo y adaptativo. Dado que los Ciberriesgos no pueden eliminarse por completo, es fundamental identificarlos, comprender sus interdependencias, incluidas las de alcance transfronterizo, y gestionarlos a lo largo de todo el ciclo de vida de los sistemas. Este enfoque debe actualizarse periódicamente debido a la naturaleza cambiante de las amenazas, e incluir mecanismos de monitoreo y evaluación para asegurar mejoras continuas. Así, se fortalece la resiliencia nacional frente a riesgos digitales emergentes.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC4.1

AEC4.1.1: Definir un mecanismo de gestión de riesgos.

La ESNACIB establece un mecanismo obligatorio de gestión de riesgos para todas las entidades gubernamentales y/u operadores de forma especial de infraestructura crítica del país, integrando: (1) identificación estandarizada de activos y servicios esenciales de acuerdo a los procesos misionales de las entidades; (2) evaluación de amenazas basada en probabilidad/impacto (NIST, ISO 27005); (3) un registro nacional centralizado con datos cifrados y acceso controlado; (4) asignación explícita de responsabilidades sectoriales en mitigación y aceptación de riesgos; y (5) auditorías periódicas para garantizar efectividad. Es decir, el objetivo es crear un sistema dinámico de inteligencia de riesgos, para tener en primera instancia un registro nacional de riesgos junto con las soluciones adoptadas, almacenado y comunicado de manera segura (a través de una plataforma o sistema web), que permita al ente rector, a su equivalente o a la entidad que se designe, facilitar su monitoreo continuo y supervisión gubernamental; además, se establecerá un sistema de priorización basado en la probabilidad de que los riesgos se materialicen tomando en consideración sus impactos, con el único fin de gestionarlos permitiendo la toma de decisiones basadas en datos y resiliencia nacional coordinada.

AEC4.1.2: Identificar una metodología común para gestionar los riesgos para la Ciberseguridad.

La metodología debe proporcionar directrices claras sobre la asignación de funciones y responsabilidades en diversos aspectos de la gestión de riesgos, incluyendo la valoración de activos de los procesos críticos o misionales de las diferentes entidades, así como la identificación y evaluación de amenazas y vulnerabilidades, la implementación del tratamiento a los riesgos y mantenimiento de medidas de mitigación y la aceptación de riesgos residuales. Además, debe incluir un programa de certificación y de calidad de resultados en su aplicación que facilite la evaluación y posterior mejora del cumplimiento.

Para el Estado Peruano, se manejará un híbrido de las reguladas por las ISO/IEC tanto la 27001, 27005, 31000 y el marco de trabajo de NIST para la preparación, resiliencia y respuesta a incidentes de Ciberseguridad y otros estándares o buenas prácticas que aporten a lo concerniente.

Es importante señalar que, para la adquisición y el desarrollo de infraestructuras o servicios, la metodología de gestión de riesgos debe dar además orientación sobre cómo minimizar el riesgo mediante una arquitectura y un diseño seguro, reconociendo que se obtiene mayor salvaguarda, cuando ésta es parte integrante del proceso de diseño de un producto, proceso o servicio (seguridad desde la fase de diseño).

AEC4.1.3: Determinar perfiles de riesgos específicos por sector en el ámbito de la Ciberseguridad.

Una vez seleccionada o creada la metodología a utilizar, se deberá identificar en todas las entidades del país los activos de información digitales clave que sustentan sus procesos críticos, si bien se tiene identificado a los Activos Críticos Nacionales (ACN) que corresponde a las infraestructuras críticas, es crucial tener mapeados todos los activos críticos de las diferentes entidades del Estado Peruano por sector, esto deberá supervisarse por el CNSD en coordinación con las entidades que tienen a cargo los ACN, con el fin de intercambiar información relevante ante la mitigación de riesgos preponderantes para el país, así como mantener la ciberresiliencia ante las ciberamenazas y/o ciberataques que se propaguen.

La utilización de perfiles de riesgos sectoriales sienta las bases para efectuar evaluaciones de riesgos más específicas de distintas entidades, aumenta la coherencia dentro y a través de todos los sectores a escala nacional y reduce los recursos

necesarios para evaluar los riesgos que corren las entidades. Los perfiles deben actualizarse periódicamente para garantizar que se mantengan actualizados.

AEC4.1.4: Monitorear continuamente y supervisar a las entidades del sector público por parte de la SGTD - PCM, respecto al cierre eficaz de las acciones establecidas en los planes del tratamiento al riesgo en especial de los Ciberriesgos determinados.

Se deberá monitorear continuamente por parte del equipo SGTD – PCM, según los planes de tratamiento al riesgo y/o planes de acción, a las entidades del sector público a fin de que las mismas, aborden las acciones relacionadas al cierre eficaz de los planes de tratamiento al riesgo, con el fin de tener una gestión apropiada de cara al fortalecimiento de la Ciberseguridad a nivel nacional.

OEEC4.2.- Elaborar mecanismos y/o procedimientos para fortalecer capacidades de resiliencia y respuesta ante incidentes relacionados con la Ciberseguridad.

Esto incluye la creación de protocolos de respuesta estandarizados, el fortalecimiento de los equipos de gestión de incidentes (CSIRT), y la realización periódica de simulacros y ejercicios de cibercrisis. Además, es fundamental establecer canales de comunicación eficaces entre entidades públicas, privadas y operadores críticos. Estas acciones deben estar acompañadas de procesos de mejora continua y actualización constante frente a amenazas emergentes.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC4.2

AEC4.2.1 Establecer e implementar protocolos y procedimientos unificados y sistemáticos para la prevención, detección, análisis, contención, respuesta y recuperación ante incidentes cibernéticos fortaleciendo la ciberresiliencia.

Se requiere para esta acción, además de adoptar una metodología para la gestión de riesgos que se ha visto en el pilar anterior, es necesario implementar procedimientos estandarizados tomando como base a los estándares internacionales (ISO/IEC 27001, 27002, 27035, NIST SP 800-61 Rev. 3, entre otros) que permita y facilite la interoperabilidad entre instituciones y promueva una respuesta eficaz, alineada a fin de garantizar una actuación coordinada, oportuna y eficaz frente a amenazas digitales.

Asimismo, se necesita elaborar mecanismos y procedimientos óptimos y eficaces, dentro de estos mecanismos es necesario implementar un sistema integral y automatizado de alerta temprana nacional basado en inteligencia de amenazas (Threat Intelligence) y análisis predictivo, así como realizar un monitoreo continuo de incidentes con el control respectivo y bajo el orden jurídico, que permita detectar y comunicar de forma proactiva amenazas cibernéticas emergentes, también considerar la realización de ethical hacking en las entidades al menos una vez por año y si agregamos la colaboración público-privada en ejercicios de Red Team/Blue Team. La mejora continua mediante lessons learned[44] y auditorías también fortalece la madurez del proceso. Este enfoque no solo reduce el impacto de incidentes, sino que también alinea la estrategia peruana con estándares globales como el IGC y las mejores prácticas de organismos como ENISA y OEA, todo esto con el fin de anticipar incidentes y reducir su impacto.

Finalmente, se debe determinar y fortalecer la capacidad de recuperación, adaptación y continuidad de los activos de información digitales estratégicos del país ante estos ciberataques o incidentes disruptivos, mediante la implementación de mecanismos de gestión de respaldo y restauración, redundancia, planes de continuidad operativa y pruebas periódicas de resistencia cibernética.

AEC4.2.2: Establecer capacidades de monitoreo y respuesta a incidentes

Las capacidades de monitoreo y respuesta ante incidentes en Ciberseguridad deben incluir la formación y fortalecimiento de equipos especializados, como los CERTs y/o CSIRTs, esenciales para la atención eficiente de emergencias y/o incidentes en el entorno digital. En Perú, el D.U. 007-2020 establece la creación de CSIRTs a nivel nacional que responde a ambos eventos, aunque aún no están plenamente constituidos en todas las entidades públicas, (mientras que, en el sector privado, académico y otras organizaciones en su mayoría ya existen), es crucial fortalecerlos con recursos humanos, tecnológicos y financieros adecuados para asegurar una respuesta rápida y coordinada esto implica de agenciarse de las tecnologías emergentes como soluciones de inteligencia artificial y/u otra tecnología, para la detección de amenazas y respuesta ante incidentes de forma rápida. Asimismo, es prioritario conformar estos equipos en todas las instancias locales, regionales y nacionales donde aún no se han establecido, garantizando así una defensa integral frente a emergencias e incidentes cibernéticos.

[44] Lessons learned (lecciones aprendidas), se refiere al proceso de revisión, análisis y documentación de lo ocurrido tras un incidente de seguridad, con el fin de identificar errores, aciertos y oportunidades de mejora.

AEC4.2.3: Elaborar un Plan Nacional de Continuidad o de Contingencia para gestionar crisis de Ciberseguridad con la debida resiliencia

Se elaborará un Plan Nacional de Continuidad para situaciones de emergencia y crisis en Ciberseguridad del país, que considere diversos escenarios de riesgo, con la colaboración de las entidades del sector público, privado, la academia y la sociedad civil. Este plan prestará especial atención a las entidades que gestionen infraestructuras críticas esenciales, como las del sector salud, energía, saneamiento, entre otros. El plan Nacional de continuidad o contingencia en Ciberseguridad tomará en cuenta los resultados de las evaluaciones nacionales de riesgos y cualquier factor intersectorial que pueda afectar la operación de estas infraestructuras, así como los protocolos y mecanismos de respuesta rápida ante incidentes de Ciberseguridad recuperación ante desastres. Además, deberá proporcionar una visión integral de los mecanismos nacionales de respuesta ante incidentes y clasificar los incidentes de Ciberseguridad según su impacto en los activos y servicios críticos de las entidades del Estado Peruano.

AEC4.2.4: Promover el intercambio de información

Esta acción permitirá establecer un sistema y medios de comunicación para el intercambio de información entre el CNSD, la Comunidad Nacional de Ciberseguridad (CNC) y demás actores del ecosistema digital que permitan compartir inteligencia e información útil sobre las últimas amenazas, vulnerabilidades, buenas prácticas y otro tema de interés relacionado con la Ciberseguridad.

Los programas de intercambio de información facilitan la coordinación y comunicación durante el restablecimiento y respuesta a incidentes. Permiten el rápido intercambio de inteligencia sobre amenazas, mejorando la comprensión de los sectores afectados y divulgando métodos para mitigar riesgos. Esto ayuda a reducir vulnerabilidades, nivel de exposición y los riesgos asociados.

El Plan Nacional de Continuidad, precisará las estructuras institucionales responsables de transmitir información útil entre el CNSD, la CNC y otros, incluyendo los sectores público y privado. El intercambio de información será un proceso bidireccional, donde si los gobiernos comparten sus datos y/o información, demostrarán a las entidades su compromiso como socios en la lucha contra las ciberamenazas. Este sistema o mecanismos que se implemente permitirán una toma de decisiones informada, la

prevención proactiva de riesgos y la generación de sinergias para fortalecer la resiliencia nacional frente a ataques cibernéticos.

AEC4.2.5: Realizar simulacros de ataques de Ciberseguridad para fortalecer la capacitación continua de los responsables, equipos CSIRTs dirigidos a las audiencias técnicas del sector público y privado.

Se fomentará la organización y coordinación de programas de formación continua y ejercicios prácticos que simulen escenarios reales de ciberataques y respuesta a incidentes a escala nacional, en especial lo contemplado en el Plan Nacional de Continuidad con el propósito de optimizar la preparación, la coordinación o comunicación interinstitucional y los tiempos de respuesta frente a incidentes relacionados con los ataques cibernéticos. Estos simulacros pueden seguir diferentes formatos (por ejemplo, simulaciones o ejercicios en tiempo real, off line, etc.)

AEC4.2.6: Creación de un Sistema Nacional de Gestión de Cibercrisis

Se fomentará la creación del Sistema Nacional de Gestión de Cibercrisis (SNGC) tal y como lo indica el lineamiento 8 del Plan Estratégico Nacional 2050. Este sistema implica establecer un marco coordinado a nivel país para prevenir, detectar, responder y recuperarse de incidentes cibernéticos de gran escala que afecten infraestructuras críticas, instituciones públicas o la seguridad nacional en relación incluso con otros países. Este sistema debe integrar al CNSD, organismos gubernamentales, sector privado y fuerzas de seguridad, con protocolos claros de actuación y comunicación. También requiere una infraestructura tecnológica robusta, centros de respuesta a incidentes (CSIRTs) a nivel de todo el país y tener capacidades de análisis e inteligencia cibernética. Su objetivo principal es minimizar el impacto de las cibercrisis y garantizar la continuidad operativa del país. En esencia, fortalece la resiliencia nacional ante amenazas digitales emergentes.

4.5.5 CONTRARESTAR LA CIBERDELINCUENCIA

La evolución constante del ciberdelito representa una amenaza creciente para la seguridad de las personas, la protección de sus derechos y la estabilidad de las naciones en la era digital. Una prevención y respuesta efectivas son fundamentales para salvaguardar los activos de información digitales, la identidad, la privacidad individual y

la integridad institucional. Fortalecer las capacidades de Ciberseguridad es clave para enfrentar estos desafíos.

OEGC5: Abordar los ciberdelitos de manera proactiva y colaborativa para la seguridad y prosperidad del país.

Plantea la necesidad de enfrentar los ciberdelitos con un enfoque proactivo y colaborativo, lo que implica anticiparse a las amenazas mediante inteligencia utilizando las tecnologías emergentes, monitoreo constante y medidas preventivas alineadas al marco normativo vigente, en lugar de solo reaccionar ante incidentes. Además, resalta la importancia de la cooperación entre entidades gubernamentales, sector privado, academia y organismos internacionales para compartir información, recursos y buenas prácticas. Este enfoque integral busca no solo proteger los sistemas y datos en entornos nacionales o transfronterizos (entorno nube), sino también garantizar un entorno digital seguro que favorezca el desarrollo económico, la confianza ciudadana y la estabilidad nacional. En resumen, es una estrategia orientada a la resiliencia y la prosperidad del país frente a riesgos cibernéticos.

OEEC5.1.- Optimizar las capacidades técnicas, la infraestructura de apoyo y los sistemas de monitoreo y vigilancia digital debidamente controlada bajo el marco legal, para gestionar eficazmente las denuncias, su procesamiento, soluciones respectivas y la aplicación de sanciones referidas a la ciberdelincuencia.

Para combatir eficazmente la ciberdelincuencia, es esencial optimizar las capacidades técnicas, infraestructura tecnológica y fortalecer los sistemas de monitoreo digital dentro del marco legal. Esto resulta crítico para proteger la identidad digital, los datos personales y la privacidad de los usuarios, con especial atención a niños(as) y demás población vulnerable, salvaguardando su integridad y derechos fundamentales en el entorno digital.

Asimismo, se debe mejorar la formación del personal especializado y establecer canales eficientes para la recepción y gestión de denuncias. Además, se requiere una articulación clara entre los procesos de investigación, análisis forense, solución y aplicación de sanciones, garantizando siempre el respeto a los derechos fundamentales.

La vigilancia digital debe operar bajo estrictos marcos legales que aseguren el equilibrio entre seguridad y privacidad. Esta estrategia fortalece la confianza ciudadana y la eficacia del sistema de justicia en el entorno digital. Por ello, se pondrá especial atención al apoyo de la sinergia de instituciones que velan por la Ciberseguridad del país.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC5.1

AEC5.1.1: Robustecer el marco regulatorio y fortalecer las capacidades para la lucha contra los ciberdelitos.

Esto implica reforzar al Perú en marcos normativos, así como afianzar las capacidades de los actores directos de los tres poderes del estado peruano conformantes del ecosistema digital, para prevenir, investigar y sancionar los ciberdelitos mediante un enfoque integral que promueva la cooperación internacional, el desarrollo de habilidades especializadas, la colaboración interinstitucional y la formación de profesionales en Ciberseguridad en todo su contexto.

Cabe resaltar la especial atención a la protección de la identidad digital y los datos personales, pues constituyen derechos fundamentales en un entorno digital crecientemente expuesto a ciberamenazas. El volumen masivo de información recolectada por entidades públicas y privadas amplía los riesgos de brechas de seguridad, pudiendo derivar en fraudes, suplantación de identidad o discriminación si no se gestiona con los controles adecuados. Implementar marcos robustos de seguridad y prepararnos en el conocimiento y concientización, no solo mitiga estos peligros, sino que fortalece la confianza ciudadana en los servicios digitales y fomenta una gestión responsable de los datos, esencial en la era de la hiperconectividad.

AEC5.1.2: Fortalecer las Infraestructuras tecnológicas para hacer frente a los ciberdelitos.

La protección de la identidad digital y los datos personales a nivel nacional requiere la implementación de controles de seguridad robustos, incluyendo medidas técnicas para la evaluación previa, durante y posterior mediante inteligencia OSINT, HUMINT y otros métodos. Es esencial fortalecer las capacidades organizativas y tecnológicas de las entidades públicas y privadas, garantizando la confidencialidad, integridad, disponibilidad y trazabilidad de la información, conforme a los niveles de riesgo y estándares internacionales. En este contexto, de modo particular, el RENIEC debe

seguir liderando el desarrollo de medios seguros de identificación digital, como el DNI digital, ID Perú, firma digital remota y gestión de atributos, alineados con el Decreto Supremo 029-2021-PCM. La certificación de los sistemas de firma digital debe contar con el respaldo de INDECOPI a través de la IOFE, asegurando su fiabilidad, así como El MINJUSDH en lo que respecta a protección de datos personales.

AEC5.1.3: Proveer al Centro Nacional de Seguridad Digital y los Centros conexos que se habiliten, de las herramientas y protocolos necesarios para respaldar las actividades de lucha contra los ciberdelitos, garantizando la trazabilidad y transparencia en todo el proceso.

Esto propone dotar al CNSD y a los centros conexos de soluciones tecnológicas avanzadas relacionadas con la Ciberseguridad, de plataformas de monitoreo continuo, sistemas de gestión y respuesta a incidentes (SIEM/SOAR) y herramientas de rastreo y/o análisis forense digital con capacidades de trazabilidad robusta. Asimismo, se implementará protocolos estandarizados para la recolección, custodia y análisis de evidencias digitales, garantizando transparencia e integridad en todo el proceso. Estas capacidades deben integrarse con mecanismos de auditoría automatizada, interoperabilidad entre entidades y una política de capacitación técnica permanente. Todo ello alineado a estándares internacionales y a la ESNACIB.

AEC5.1.4: Generar capacidades para la investigación y gestión de la evidencia digital.

Es prioritario fortalecer las capacidades nacionales en investigación, innovación y gestión de evidencia digital, mediante la creación de laboratorios de informática forense que cumplan con estándares internacionales. Estos centros de referencia deberán brindar soporte técnico especializado a las entidades competentes, en estrecha coordinación con el CNSD, la Policía, el Ministerio Público, la Fiscalía de la Nación, el Poder Judicial y demás organismos del Estado. Su funcionamiento debe regirse por protocolos unificados y alineados a marcos internacionales, en articulación con la SGTD–PCM y los centros especializados en referencia a contrarrestar la ciberdelincuencia.

AEC5.1.5: Establecer mecanismos de supervisión y control para el cumplimiento del marco normativo referido a neutralizar la ciberdelincuencia.

Es decisivo diseñar e implementar mecanismos eficaces de supervisión y control que aseguren el cumplimiento de las normativas relacionadas con la identidad digital, la protección de datos personales, contrarrestar los ciberdelitos y fraude informático y el uso indebido de la inteligencia artificial. Las entidades encargadas de proteger a la ciudadanía en el ciberespacio y administrar justicia deben fortalecer sus capacidades de fiscalización y respuesta ante el incumplimiento de dicho marco. Asimismo, es fundamental impulsar una cultura de cumplimiento normativo entre las organizaciones que manejan datos personales y/o confidenciales o sensibles, promoviendo la corresponsabilidad en la lucha contra la ciberdelincuencia. Esto permitirá detectar, prevenir y sancionar conductas delictivas digitales de forma más eficiente.

AEC5.1.6: Promover una gestión más eficiente de la justicia mediante contribuciones y propuestas relacionadas con la legislación actual.

Esto implica, reforzar el marco normativo actual mediante la actualización y armonización de leyes con un enfoque técnico-jurídico especializado en delitos digitales emergentes. Es esencial fomentar una colaboración interinstitucional efectiva entre el Poder Ejecutivo, Congreso, Fiscalía, Poder Judicial y entes reguladores, mediante mesas técnicas permanentes y espacios de diálogo multisectorial. También se debe incorporar evidencia técnica en los procesos legislativos y judiciales, garantizando que las decisiones estén basadas en la realidad operativa del cibercrimen. Esto permitirá una respuesta legal más ágil, coherente y efectiva frente a las nuevas amenazas digitales.

OEEC5.2.- Monitoreo y seguimiento del ciberdelito o del cibercrimen a fin de implementar estrategias para su comunicación y posterior extinción.

La recolección y análisis de datos clave brindará una visión completa de la situación de los ciberdelitos en el país, proporcionando información esencial para el diseño e implementación de estrategias efectivas en la lucha contra este fenómeno.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC5.2

AEC5.2.1: Facilitar el acceso de las personas a un mecanismo ágil que permita realizar la denuncia de los ciberdelitos.

Se fomentará la creación de una plataforma digital unificada, integrando de ser posible, con el observatorio de delitos que tiene el Ministerio del Interior, la información relacionada con los delitos vinculados a las TIC, como los ciberdelitos y/o delitos informáticos actuales, dicha plataforma tiene que ser accesible desde diversos dispositivos, que permita a la ciudadanía reportar ciberdelitos de manera rápida, segura y con trazabilidad garantizada. Esta herramienta debe estar integrada con las entidades competentes, como la Policía, Fiscalía y el CNSD, para una atención inmediata y coordinada. Además, incluiría funcionalidades de autodiagnóstico, orientación legal básica y seguimiento en tiempo real del caso. La plataforma debe cumplir con altos estándares de Ciberseguridad y protección de datos personales. Todo ello debe ser respaldado por campañas de difusión y educación digital.

AEC5.2.2: Incorporar al país, a los convenios internacionales y otros organismos relacionados a fin de hacer frente a la ciberdelincuencia.

Con el objetivo de realizar las adaptaciones normativas y protocolares necesarias para asegurar el cumplimiento efectivo de las acciones contra la ciberdelincuencia, se tendrá que fortalecer la cooperación internacional en la identificación, persecución y sanción de ciberdelincuentes, incluso cuando operen desde fuera del territorio nacional. Para ello, es fundamental establecer alianzas estratégicas, así como suscribir convenios bilaterales o multilaterales que permitan el intercambio ágil y seguro de información en procesos de investigación. Estos acuerdos deben garantizar obligaciones claras para los Estados firmantes respecto a la colaboración judicial y técnica. Además, deben contemplar mecanismos estandarizados para la solicitud y entrega de datos digitales en fases preliminares de investigación. Todo ello contribuirá a una respuesta transnacional más eficaz frente al cibercrimen.

4.5.6 CONSOLIDAR LA CIBERDEFENSA

El país debe estar preparado para enfrentar eventos sistémicos derivados de posibles ciberataques. En este pilar solo se mencionará el objetivo que se relaciona con la contribución que realizaría la Ciberseguridad en apoyo de la ciberdefensa, el cual en su

liderazgo está a cargo del Ministerio de Defensa y el Comando Conjunto de las Fuerzas Armadas, todo ello enmarcado dentro de la Ley Nº 30999. Ley Ciberdefensa del Perú y su reglamento, sin embargo, es importante la coordinación con el CNSD – SGTD – PCM, ya que su interrelación con la salvaguarda de infraestructuras críticas ante una posible ciberguerra coadyuva a la protección de soberanía digital nacional.

OEGC6: Anticipar y gestionar escenarios de incidentes masivos que puedan impactar las operaciones nacionales y afectar a la población de forma total o parcial por causa de una ciberguerra.

En el siguiente gráfico se observa la evolución que ha tenido la ciberdefensa en el Perú hasta el año 2021, según lo manifestado por la Política Sectorial de Ciberdefensa:

Figura. 29. Evolución de la Ciberdefensa al 2021

Fuente: Política Sectorial de Ciberdefensa: una necesidad impostergable. Enlace Web: https://ebiz.pe/noticias/politica-sectorial-de-ciberdefensa-una-necesidad-impostergable/

En consecuencia, es importante anticipar, gestionar y simular escenarios de ciberguerra que puedan desencadenar incidentes masivos, disruptivos o catastróficos, capaces de comprometer operaciones críticas nacionales (infraestructuras, servicios esenciales) y afectar a la población de manera generalizada o localizada. Implica desarrollar y reforzar capacidades proactivas de inteligencia, resiliencia y respuesta coordinada entre sectores: público y privado para mitigar daños, garantizar la continuidad del Estado y proteger a la ciudadanía frente a ataques cibernéticos de gran escala estratégica.

OEEC6.1.- Robustecer el ecosistema de ciberdefensa del país mediante el refuerzo de capacidades institucionales para prevenir, detectar y responder a incidentes de Ciberseguridad que amenacen la seguridad nacional.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC6.1

AEC6.1.1: Desarrollar una Estrategia Nacional de Ciberdefensa basada en prevención, detección temprana, respuesta coordinada y resiliencia, reforzada con formación continua y una cultura de Ciberseguridad en las Fuerzas Armadas y Comando Conjunto, para proteger la soberanía digital y contrarrestar ciberataques de escala estratégica o bélica.

Esto implica determinar entidades responsables de prevenir y mitigar cibercrisis, con mecanismos de coordinación público-privada para respuestas ágiles frente a ciberataques masivos. Se establecerán protocolos de guerra cibernética para proteger infraestructuras críticas (energía, defensa, finanzas, etc.), integrando inteligencia artificial, threat hunting militar y doctrinas de retaliación controlada, todo bajo un marco de gobernanza nacional alineado con estándares OTAN y resiliencia soberana.

4.5.7 INVESTIGACIÓN, INNOVACIÓN Y CULTURA EN CIBERSEGURIDAD

Con este pilar se busca impulsar la investigación e innovación en Ciberseguridad mediante alianzas estratégicas entre universidades, sector privado y agencias estatales, priorizando áreas como inteligencia artificial aplicada a detección de amenazas, análisis forense avanzado y resiliencia de infraestructuras críticas. Paralelamente, desarrollar campañas masivas de concienciación ciudadana para todo nivel educativo y programas de formación especializada (ej. hacking ético, ciberdefensa nacional) a fin de crear una cultura proactiva de Ciberseguridad, reduciendo brechas técnicas y humanas frente a ataques sofisticados.

OEGC7: Promover la innovación y avances tecnológicos en Ciberseguridad mediante inversión estratégica en I+D+i, impulsando soluciones disruptivas, así como empoderar a las entidades y demás actores del ecosistema digital, para usar las TIC de manera segura y responsable, protegiendo sus derechos y libertades en el ciberespacio.

OEEC7.1.- Impulsar I+D+i en Ciberseguridad para desarrollar tecnologías disruptivas.

Este objetivo busca fortalecer la investigación e innovación respecto a los avances tecnológicos emergentes, como la inteligencia artificial defensiva y criptografía post-cuántica, blockchain, el aprendizaje automático y otras tecnologías disruptivas, para desarrollar soluciones innovadoras que fortalezcan la Ciberseguridad. El desarrollo tecnológico en esta temática, permitirá a las instituciones públicas y privadas estar mejor preparadas para prevenir, detectar y mitigar ataques cibernéticos, fomentar la creación de nuevas herramientas y plataformas de protección contribuirá a mejorar la resiliencia del país frente a las amenazas digitales.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC7.1

AEC7.1.1: Incentivo a la innovación y la investigación en Ciberseguridad

Con esta acción se busca articular a los sectores público, privado y sociedad civil para fortalecer la protección colectiva contra ciberamenazas, impulsando un ecosistema de innovación en Ciberseguridad mediante incentivos clave. Se promoverán startups y empresas tecnológicas a través de participación de subvenciones, beneficios tributarios, becas, programas de incubación y fondos concursables, con el objetivo de desarrollar soluciones tecnológicas nacionales y potenciar el talento especializado. Todo ello con el respaldo estratégico de instituciones como CONCYTEC, la Cámara de Comercio, PRONABEC, universidades, centro de investigación, etc., que fomentan la I+D+i para consolidar una industria digital segura y competitiva.

AEC7.1.2: Creación de centros de investigación y capacitación en Ciberseguridad

Crear centros de investigación y capacitación descentralizados (por macro regiones) en Ciberseguridad con enfoque multidisciplinario, dotados de la infraestructura tecnológica correspondiente, que funcionen como polos de innovación, formación especializada y desarrollo de talento orientados a impulsar el desarrollo científico y tecnológico en esta materia estratégica, para generar soluciones adaptadas al contexto nacional, estudiar amenazas emergentes y diseñar herramientas de defensa digital. Además, facilitarían la colaboración entre el Estado, el sector privado, la academia y sociedad civil. Su existencia fortalecería la soberanía tecnológica y la capacidad de respuesta ante

ciberriesgos. Serían fundamentales para posicionar al país como referente regional en investigación en Ciberseguridad.

OEEC7.2: Fomentar una cultura de Ciberseguridad que promueva la higiene digital como una práctica habitual.

Implica crear conciencia continua sobre los riesgos digitales y promover hábitos responsables entre todos los usuarios. La higiene digital debe integrarse en la rutina diaria, como actualizar contraseñas, evitar enlaces sospechosos y usar autenticación multifactor. Propondría programas de capacitación periódicos, campañas internas y políticas claras que refuercen buenas prácticas. Además, es clave que el liderazgo implemente estas prácticas en las instituciones del Estado Peruano y apoye estas iniciativas de forma activa.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC7.2

AEC7.2.1: Impulsar programas especializados de capacitación y sensibilización dirigidos a operadores de infraestructuras críticas y usuarios estratégicos, promoviendo una cultura robusta de Ciberseguridad.

Con esta acción se busca promover una sólida cultura de Ciberseguridad mediante la implementación de un programa integral y sistemático de formación continua y evaluación periódica, orientado a operadores de infraestructuras críticas y usuarios clave. Este programa debe fortalecer sus capacidades normativas, técnicas y operativas para anticipar, identificar y responder eficazmente a incidentes cibernéticos. La capacitación debe adaptarse a las amenazas emergentes y a los avances tecnológicos. Así se garantiza una respuesta coordinada y resiliente frente a riesgos que comprometan la seguridad digital del entorno crítico.

AEC7.2.2. Implementación de cursos de formación continua y certificaciones profesionales en Ciberseguridad promovidos por el estado peruano.

Elaborar e implementar programas de formación continua y certificación profesional respaldados por el Estado, orientados tanto a especialistas del sector tecnológico como a profesionales de áreas estratégicas, con especial énfasis en el Sector Público y en la ciudadanía. Estas iniciativas, como las impulsadas por el CNSD, la “Alianza por una Internet Segura”, y los cursos dirigidos a PYMES, Gobiernos Regionales y locales,

deben fortalecer las competencias del talento humano nacional, especialmente de quienes lideran la Ciberseguridad en las entidades públicas y privadas. Es fundamental que estos programas incluyan contenidos actualizados, prácticas avanzadas y certificaciones con reconocimiento nacional e internacional, contando con el respaldo de instituciones como PRONABEC, SUNEDU y universidades acreditadas. El objetivo es elevar el nivel de preparación técnica del país, cerrar brechas de especialización y fomentar un ecosistema digital más seguro, resiliente e innovador frente a amenazas cibernéticas emergentes.

AEC7.2.3: Suscitar una cultura de Ciberseguridad en el Sistema Educativo Nacional.

Promover la educación en Ciberseguridad desde todos los niveles del sistema educativo peruano[45], con el compromiso articulado del MINEDU, SUNEDU, SERVIR, PRONABEC, Gobierno Regionales, Municipalidades, entre otros, de forma progresiva, es esencial para desarrollar competencias digitales sólidas en la población. Esta formación debe adaptarse a las características y necesidades de diversos grupos (niños(as), jóvenes, personas adultas mayores y sectores vulnerables en especial con habilidades diferentes y otras). La comunicación y los contenidos educativos deben ser inclusivos, relevantes y accesibles. Las iniciativas deben priorizar temas como la protección de datos, privacidad y seguridad en el entorno digital, asegurando el uso adecuado y seguro de las tecnologías. consolidando una cultura de Ciberseguridad responsable y resiliente.

4.5.8 COOPERACIÓN INTERNACIONAL

En este ámbito prioritario, se fortalecerán los compromisos de Ciberseguridad a nivel regional e internacional. La Ciberseguridad adquiere una relevancia creciente en múltiples dimensiones de las relaciones internacionales, incluyendo la protección de la privacidad y de los derechos humanos, el impulso al desarrollo económico, las transacciones comerciales, el control de armamentos, la seguridad global, la estabilidad, la paz y la resolución de conflictos.

OEGC8: Fortalecer los mecanismos de cooperación internacional posicionando al Perú como un actor clave y confiable en la gobernanza del ciberespacio, tanto a nivel regional como internacional.

[45] Sistema educativo peruano incluye a nivel primario, secundario, superior y programas para la población vulnerable.

Fortalecer los mecanismos de cooperación internacional con la Organización de Estados Americanos (OEA), Unión Europea (UE), la ONU, INCIBE, INTERPOL, EUROPOL, y otros organismos globales, lo que permitirá al Perú integrarse activamente en iniciativas globales orientadas a fortalecer la Ciberseguridad, facilitando el intercambio de buenas prácticas, el acceso a tecnología avanzada y la suscripción de acuerdos para proteger la información y sus activos especialmente los correspondientes a infraestructuras críticas. Asimismo, incluirá asistencia técnica, formación especializada y el intercambio de inteligencia cibernética, elevando significativamente la capacidad del país para afrontar desafíos complejos y así conservar la soberanía en el entorno digital.

OEEC8.1.- Fomentar la cooperación bilateral y multilateral, contribuyendo al desarrollo de la confianza entre naciones y al aumento de la resiliencia global frente a amenazas digitales crecientes.

El Perú debe proyectarse como un socio comprometido, transparente y técnicamente sólido, que fomente el intercambio sustancial en este ámbito, alineado con los intereses nacionales.

ACCIONES ESTRATÉGICAS DE CIBERSEGURIDAD DEL OEEC8.1

AEC8.1.1: Participar en foros regionales e internacionales y tratados sobre Ciberseguridad lo cual permita alinear al Perú con estándares internacionales y fomentar una cooperación eficaz ante amenazas cibernéticas globales.

Fortalecer la presencia activa del país en foros, conferencias de organismos internacionales de Ciberseguridad es clave para intercambiar experiencias, adoptar buenas prácticas y acceder a asistencia técnica especializada. Esta participación estratégica permitirá alinear al Perú con estándares internacionales y promover una cooperación efectiva frente a ciberataques globales. Además, potenciará la capacidad nacional para prevenir y responder a incidentes transfronterizos. Así, el país se consolida como un actor confiable en la gobernanza del ciberespacio.

AEC8.1.2: Establecer protocolos y mecanismos de colaboración internacional para una respuesta coordinada y oportuna ante ciberataques.

Esta acción conllevará a mejorar las capacidades de respuesta frente a los ciberataques que puedan afectar a múltiples naciones, así como fomentará el intercambio de

información sobre ciberamenazas y técnicas de defensa para fortificar la seguridad cibernética global. Este mecanismo de operabilidad tendrá que darse en tiempo real buscando la asistencia mutua y la articulación de esfuerzos entre países para contener y mitigar amenazas digitales de alcance transnacional.

AEC8.1.3: Promover la cooperación internacional en el desarrollo de estrategias de prevención y en la investigación de cibercrímenes y ciberterrorismo, en la lucha contra la ciberdelincuencia.

Se promoverá alianzas estratégicas con organismos multilaterales, países aliados, redes de expertos, centros y/o agencias de Ciberseguridad, autoridades judiciales y fuerzas de seguridad de diferentes países, mediante el establecimiento de acuerdos bilaterales y multilaterales y redes de cooperación que faciliten el desarrollo conjunto de estrategias preventivas y el intercambio de información relacionado al modus operandi de cibercriminales y grupos ciberterroristas. Además, se deben establecer canales seguros y ágiles para la investigación transfronteriza de cibercrímenes y ciberterrorismo, con apoyo técnico y legal mutuo. La articulación con organismos especializados permitirá acceder a capacidades avanzadas de análisis forense digital. Estas acciones contribuirán a una respuesta más efectiva y coordinada frente a estas temáticas.

4.6. INDICADORES DE LA ESNACIB

Corresponde a la ESNACIB, agenciarse de Indicadores Clave de Rendimiento (KPIs) (*Key Performance Indicators, por sus siglas en inglés*), indicadores que se utilizan para medir el progreso, el desempeño o la eficacia de una actividad, proceso, proyecto o estrategia.

En relación con los objetivos establecidos en los pilares, dichos indicadores se reflejarán en el Plan de Acción que tiene el Perú.

4.6.1. Características clave de los KPIs:

a) Cuantificables: se expresan en métricas concretas (porcentaje, tiempo, cantidad, etc.)
b) Relevantes: están alineados con los objetivos estratégicos de la organización.
c) Medibles en el tiempo: permiten hacer seguimiento periódico (diario, mensual, anual).
d) Accionables: ofrecen información útil para tomar decisiones o corregir el rumbo.

Ejemplos:

- Reducción de Incidentes relacionados con la Ciberseguridad al año.
- Número de incidentes de seguridad detectados trimestralmente.
- Tiempo promedio de respuesta ante un incidente (MTTR).
- Porcentaje de colaboradores y/o usuarios entrenados en prácticas seguras por entidad.
- Porcentaje de la población capacitada cada bimestre en conferencias realizadas por la Alianza de una Internet Segura u otro evento masivo.
- Duración promedio para detectar y mitigar eventos de Ciberseguridad.
- Porcentaje de sistemas actualizados con parches de seguridad.
- Tasa de éxito en pruebas realizadas mediante ethical hacking.
- Progreso en la adopción de tecnologías como MFA y sistemas de monitoreo.

En resumen, los KPIs permiten evaluar si se están cumpliendo los objetivos y metas de Ciberseguridad de forma clara, medible y orientada a la mejora continua.

4.7. SEGUIMIENTO A LAS RESPONSABILIDADES ASUMIDAS POR LAS ENTIDADES RESPECTO A LOS PILARES DE LA ESNACIB

4.6.1. DESCRIPCIÓN DE ENTIDADES PARTICIPANTES

Se detallan las principales entidades comprometidas con la protección, prevención, respuesta y coordinación del Estado peruano. Estas instituciones desempeñan un rol clave en el fortalecimiento de la seguridad digital nacional y en la protección de los Activos Críticos Nacionales (ACN):

a) Presidencia del Consejo de ministros (PCM)

Lidera y coordina las políticas de gobierno digital y Ciberseguridad a través de la Secretaría de Gobierno y Transformación Digital (SGTD).

b) Secretaría de Gobierno y Transformación Digital (SGTD) de la PCM

Actúa como la autoridad nacional competente en Ciberseguridad, responsable de la formulación, implementación, supervisión y evaluación de la ESNACIB-Perú.

c) Centro Nacional de Seguridad Digital (CNSD) de la SGTD

Es el centro de coordinación táctica - operativa para la prevención, detección, respuesta y recuperación ante incidentes de Ciberseguridad a nivel nacional.

d) Dirección Nacional de Inteligencia (DINI):

Contribuye con inteligencia estratégica para la identificación y análisis de ciberamenazas a la seguridad nacional.

e) Ministerio de Defensa (MINDEF) y el Comando Conjunto de las Fuerzas Armadas (CCFFAA)

Responsables de la ciberdefensa del Estado y la protección de los activos críticos militares y estratégicos. Sus órganos ejecutores (Ejército, Marina de Guerra y Fuerza Aérea) implementan acciones específicas en este ámbito.

f) Ministerio del Interior y la Policía Nacional del Perú (PNP)

Encargados de la prevención, investigación y persecución de los ciberdelitos a través de sus unidades especializadas.

g) Ministerio Público – Fiscalía de la Nación

Responsable de la dirección de la investigación del delito y el ejercicio de la acción penal en casos de cibercrimen. Cabe resaltar que la Fiscalía Especializada en Cibercriminalidad tiene la responsabilidad de investigar y llevar a cabo procesos judiciales relacionados con ciberdelitos, como fraudes informáticos, delitos contra la privacidad, y otros crímenes tecnológicos.

h) Sectores Responsables (Ministerios y Reguladores Sectoriales)

Son responsables de implementar medidas de Ciberseguridad específicas en los sectores bajo su competencia (e.g., Ministerio de Energía y Minas para el sector energético, Ministerio de Transportes y Comunicaciones para el sector de telecomunicaciones y transporte, Superintendencia de Banca, Seguros y AFP para el sector financiero, SUNAT, SUSALUD, etc.).

i) Autoridad Nacional de Protección de Datos Personales (ANPDP)

Esta entidad, parte del Ministerio de Justicia y Derechos Humanos, se encarga de velar por la protección de los datos personales, lo cual incluye la lucha contra ciberdelitos que involucren el robo o uso indebido de información personal.

j) Operadores de los Activos Críticos Nacionales (ACN)

Entidades públicas y privadas identificadas como responsables del funcionamiento de infraestructuras y servicios esenciales, con obligaciones específicas en materia de Ciberseguridad.

k) Academia y Centros de Investigación:

Contribuyen a la formación de profesionales, la investigación y el desarrollo de soluciones en Ciberseguridad, lo conforman las universidades, institutos, colegios y demás centros de formación e investigación.

l) Sociedad Civil Organizada:

Desempeña un rol en la concientización, la promoción de buenas prácticas y la vigilancia ciudadana en el ámbito de la Ciberseguridad.

Asimismo, se presenta el siguiente cuadro resumen de los pilares, objetivos y acciones estratégicas, así como su temporalidad de implementación:

Cuadro resumen respecto a los pilares, objetivos estratégicos generales y específicos y acciones estratégicas en relación a la ESNACIB

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
4.5.1. GOBERNANZA Y LIDERAZGO	**OEGC1:** Establecer un marco holístico de gobernanza de la Ciberseguridad nacional, dotada de capacidades de dirección y operativas, que permita definir lineamientos, políticas y mecanismos claros para que el Ecosistema Nacional de Ciberseguridad, opere de manera coordinada y efectiva	**OEEC1.1:** Determinar un modelo de gobernanza multinivel en Ciberseguridad, que defina una estructura clara y eficiente para distribuir responsabilidades entre los niveles: estratégico (qué hacer), táctico (cómo hacerlo) y operacional (ejecución), con un enfoque sectorial que garantiza una gobernanza integral.	**AEC1.1.1:** Determinar la autoridad competente y designar responsabilidades ejecutivas de alto nivel, según la estructura organizativa definida en materia de Ciberseguridad con el fin de fortalecer la coordinación, supervisión y aplicación de las políticas y otros dispositivos de gestión y normativos nacionales relacionados con esta materia.	*SGTD – PCM (Liderazgo) *Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo (Instancia responsable)	Todas las entidades del Estado Peruano tanto del sector público y privado, así como la academia y sociedad civil.	C
			AEC1.1.2: Fomentar el liderazgo y la asignación de recursos adecuados para la implementación de los temas relacionados con la Ciberseguridad.	MEF	Todas las entidades del Estado Peruano tanto del sector público y privado, así como la academia y sociedad civil.	C
			AEC1.1.3: Establecer y optimizar mecanismos de coordinación para el modelo implementado, así como elaborar lineamientos, protocolos y procedimientos claros que promuevan una comunicación efectiva, el flujo ágil de información y la	*SGTD – PCM (Liderazgo) * CNSD (Nivel Técnico)	Todas las entidades del Estado Peruano tanto del sector público y privado, así como la academia y sociedad civil.	C

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
			colaboración estratégica entre los diversos actores nacionales involucrados en el ámbito de la Ciberseguridad.	*Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo (Instancia responsable)		
			AEC1.1.4: Establecer la supervisión de la implementación de la ESNACIB e implantar mecanismos regulares de seguimiento y notificación de los indicadores de Ciberseguridad.	*Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo (Instancia responsable) * CNSD (Nivel Técnico)	Todas las entidades del Estado Peruano tanto del sector público y privado, así como la academia y sociedad civil.	M
		OEEC1.2.- Promover la formación de una comunidad cohesionada y colaborativa, integrada por expertos en Ciberseguridad provenientes de los diversos sectores y actores involucrados.	**AEC1.2.1:** Establecer la comunidad de expertos en Ciberseguridad para enfrentar de manera conjunta los desafíos comunes en materia de Ciberseguridad, fortaleciendo así la capacidad de respuesta y la resiliencia nacional.	*SGTD – PCM (Liderazgo)	Todas las entidades del Estado Peruano tanto del sector público y privado, así como la academia y sociedad civil.	M
			AEC1.2.2: Se crearán espacios de consulta y participación para integrar a las partes interesadas clave, en el diseño y ejecución de la ESNACIB.	*SGTD – PCM (Liderazgo)	Todas las entidades del Estado Peruano tanto del sector público y privado, así como la academia y sociedad civil.	M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
		OEEC1.3.- Optimizar la comunicación en Ciberseguridad para una mayor eficacia y coordinación.	**AEC1.3.1:** Elaborar y coordinar un plan de comunicación integral en Ciberseguridad que esté alineado con los objetivos de la estrategia actual, enfocándose en la sensibilización, prevención y respuesta frente a las ciberamenazas.	SGTD – PCM, en su arista de comunicación y difusión y el CNSD.	Todas las entidades del Sector público, privado, la academia y otros. En especial los diferentes medios de comunicación del país, como radio, TV, diarios, redes sociales, etc.	C
			AEC1.3.2: Desarrollar un programa de difusión para garantizar una comunicación eficaz ante incidentes de Ciberseguridad, dirigido a los responsables de la toma de decisiones y a los colaboradores de las entidades públicas.	Equipo de difusión de la SGTD – PCM IRTP. Diario Oficial "El Peruano"	Todas las entidades del Sector público, privado, la academia y otros. En especial los diferentes medios de comunicación del país, como radio, TV, diarios, redes sociales, etc.	C

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
			AEC1.3.3: Brindar formación en Ciberseguridad a los equipos de comunicación y difusión, enfocándose en cómo gestionar incidentes utilizando herramientas de comunicación efectivas.	CNSD - SGTD - PCM	Todas las entidades del Sector público, privado, la academia y otros.	C
			AEC1.3.4: Fomentar o generar oportunidades de diálogo y colaboración con los medios de comunicación a fin de transmitir noticias y/o temática referida a Ciberseguridad.	CNSD - SGTD - PCM	Todas las entidades del Sector público, privado, la academia y otros.	M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
4.5.2. SALVAGUARDA A LAS INFRAESTRUCTURAS CRÍTICAS Y ACTIVOS DE INFORMACIÓN DIGITALES	**OEGC2:** Fomentar la protección y resiliencia de las infraestructuras críticas del país y los activos de información digitales.	**OEEC2.1.-**. Definir un marco de objetivos y acciones de gestión en favor de la Ciberseguridad que sea aplicable a todas las entidades que conformen los sectores o cuenten con servicios críticos del país.	**AEC.2.1.1:** Consolidar la Ciberseguridad como un objetivo estratégico dentro de los documentos de gestión en las entidades que operan y/o tienen servicios o sectores críticos del país, fomentando un compromiso institucional sólido para su implementación y la asignación de recursos necesarios.	ANA APN BCRP ELECTRONORTE ELECTROSUR ELECTROCENTRO ESSALUD FONAFE INAIGEM INDECI MEF MINDEF MINCETUR MINCUL MIDAGRI MINEDU MINEM MININTER MINJUSDH MINSA MRE MTC MTPE OEFA OTASS SEDAPAL SENAMHI SERFOR SUNASS SUTRAN SUSALUD	SGTD – PCM	M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
			AEC 2.1.2: Identificar y categorizar a las entidades que tengan infraestructuras críticas y/o que tengan activos críticos nacionales (ACN) digitales que salvaguardar, evaluando la naturaleza de los mismos, su exposición ante las ciberamenazas (nivel de vulnerabilidad), el nivel de riesgo y su impacto potencial ante incidentes, el contexto operativo en el que se desempeñan, así como sus interconexiones y dependencias con otros actores.	MINDEF CNSD – SGTD - PCM Ministerios del Estado Peruano. Superintendencias del Perú. INDECI	Entidades del Estado que tengan Infraestructura Crítica de los Sectores de Salud, Banca y Finanzas, Saneamiento, Transporte y Comunicaciones, etc.	M
			AEC 2.1.3: Implementación de protocolos de seguridad y gestión de riesgos en infraestructuras críticas y activos de información digitales del estado peruano.	Entidades del Estado que tengan Infraestructura Crítica de los Sectores de Salud, Banca y Finanzas, Saneamiento, Transporte y Comunicaciones, etc.	CNSD – SGTD - PCM INDECI Ministerios del Estado Peruano. Superintendencias del Perú.	M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
4.5.3 REGULACIÓN Y CUMPLIMIENTO	**OEGC3:** Robustecer el marco legal y regulatorio en Ciberseguridad, asegurando que sea firme, coherente, actualizado, completo, aprobado y difundido en el país.	**OEEC3.1.-** Revisar, elaborar y/o actualizar y fomentar el marco normativo en Ciberseguridad, alineándolo con estándares internacionales y buenas prácticas para garantizar su eficacia y robustez.	**AEC3.1.1:** Desarrollar un marco legal holístico de Ciberseguridad que fomente la colaboración entre el sector público, sector privado, la academia y la sociedad civil en general para el fortalecimiento de la Ciberseguridad nacional.	SGTD - PCM Congreso de la República Fiscalía de la Nación Poder Judicial MININTER – PNP MINDEF - FFAA	Las demás entidades según el ámbito de su competencia.	M
			AEC3.1.2: Desarrollar normatividad específica en Ciberseguridad, para la protección de infraestructuras críticas	SGTD - PCM Entidades de los diferentes sectores que tienen a cargo infraestructuras críticas.	Todas las demás entidades del Estado según el ámbito de su competencia.	M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
			AEC3.1.3: Establecer un mecanismo formal y periódico para la actualización continua, de normativa y estándares internacionales relacionados con la Ciberseguridad y/o temática conexa.	SGTD - PCM	Demás entidades del Estado, según el ámbito de su competencia.	M
			AEC3.1.4: Promoción de la aceptación y adopción de estándares internacionales de Ciberseguridad	SGTD - PCM	Demás entidades del Estado, según el ámbito de su competencia.	M
			AEC3.1.5: Garantizar que el marco normativo nacional promueva y proteja la Ciberseguridad a nivel supraterritorial, alineándose con los estándares internacionales y cumpliendo con los compromisos adquiridos por el país en el ámbito internacional.	SGTD – PCM Congreso de la República MRE -Superintendencia Nacional de Migraciones. Poder Judicial MINJUS Fiscalía de la Nación	Demás entidades del Estado, según el ámbito de su competencia.	L
		OEEC3.2.- Alinear el accionar de las entidades al cumplimiento de la normativa que se adapte referido a estándares internacionales, así	**AEC3.2.1:** Establecer un sistema de acreditación y/o certificación que permita validar el cumplimiento de Ciberseguridad en las entidades u organizaciones	SGTD – PCM CNSD	Demás entidades del Estado, según el ámbito de su competencia.	M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
		como asesorar en la certificación y conformidad relacionados con la Ciberseguridad.	**AEC3.2.2:** Establecer mecanismos para garantizar el cumplimiento de los requisitos normativos en Ciberseguridad.	SGTD – PCM CNSD	Demás entidades del Estado, según el ámbito de su competencia.	L
4.5.4 GESTIÓN DE RIESGOS, RESILIENCIA Y RESPUESTA A INCIDENTES	**OEGC4:** Gestionar de manera integral los Ciberriesgos asociados a los activos de información digitales del país, fortaleciendo las capacidades de resiliencia y respuesta ante incidentes cibernéticos, con un enfoque proactivo y sostenible.	**OEEC4.1.-** Establecer un proceso integral para gestionar y tratar los Ciberriesgos.	**AEC4.1.1:** Definir un mecanismo de gestión de riesgos.	SGTD – PCM CNSD	Demás entidades del Estado, según el ámbito de su competencia.	M
			AEC4.1.2: Identificar una metodología común para gestionar los riesgos para la Ciberseguridad.	SGTD – PCM CNSD	Demás entidades del Estado, según el ámbito de su competencia.	M
			AEC4.1.3: Determinar perfiles de riesgos específicos por sector en el ámbito de la Ciberseguridad.	SGTD – PCM CNSD	Demás entidades del Estado, según el ámbito de su competencia.	M A L
			AEC4.1.4: Monitorear continuamente y supervisar a las entidades del sector	SGTD – PCM CNSD	Demás entidades del Estado Peruano	M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
			público por parte de la SGTD - PCM, respecto al cierre eficaz de las acciones establecidas en los planes del tratamiento al riesgo en especial de los Ciberriesgos determinados.			
		OEEC4.2.- Elaborar mecanismos y/o procedimientos para fortalecer capacidades de resiliencia y respuesta ante incidentes relacionados con la Ciberseguridad.	**AEC4.2.1** Establecer e implementar protocolos y procedimientos unificados y sistemáticos para la prevención, detección, análisis, contención, respuesta y recuperación ante incidentes cibernéticos fortaleciendo la ciberresiliencia	SGTD – PCM CNSD	Demás entidades del Estado Peruano	L
			AEC4.2.2: Establecer capacidades de monitoreo y respuesta a incidentes.	SGTD – PCM CNSD	Demás entidades del Estado Peruano	C
			AEC4.2.3: Elaborar un Plan Nacional de Continuidad o de Contingencia para gestionar crisis de Ciberseguridad con la debida resiliencia.	SGTD – PCM CNSD	Demás entidades del Estado Peruano	M
			AEC4.2.4: Promover el intercambio de información.	SGTD – PCM CNSD	Demás entidades del Estado Peruano	C

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
			AEC4.2.5: Realizar simulacros de ataques de Ciberseguridad para fortalecer la capacitación continua de los responsables, equipos CSIRTs dirigidos a las audiencias técnicas del sector público y privado.	SGTD – PCM CNSD	Demás entidades del Estado Peruano	C
			AEC4.2.6: Creación un Sistema Nacional de Gestión de Cibercrisis.	SGTD – PCM	Demás entidades del Estado Peruano	M
4.5.5 CONTRARESTAR LA CIBERDELINCUENCIA	**OEGC5:** Abordar los ciberdelitos de manera proactiva y colaborativa para la seguridad y prosperidad del país.	**OEEC5.1.-** Optimizar las capacidades técnicas, la infraestructura de apoyo y los sistemas de monitoreo y vigilancia digital debidamente controlada bajo el marco legal, para gestionar eficazmente las denuncias, su procesamiento, soluciones respectivas y la aplicación de sanciones referidas a la ciberdelincuencia	**AEC5.1.1**: Robustecer el marco regulatorio y fortalecer las capacidades para la lucha contra los ciberdelitos.	SGTD – PCM CONGRESO DE LA REPÚBLICA FISCALÍA DE LA NACIÓN PODER JUDICIAL MINITERIO DE JUSTICIA MININTER	Demás entidades del Estado Peruano	M
			AEC5.1.2: Fortalecer las Infraestructuras tecnológicas para hacer frente a los ciberdelitos.	MEF MININTER MINDEF	Demás entidades del Estado Peruano	M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
			AEC5.1.3: Proveer al Centro Nacional de Seguridad Digital y los Centros conexos que se habiliten, de las herramientas y protocolos necesarios para respaldar las actividades de lucha contra los ciberdelitos, garantizando la trazabilidad y transparencia en todo el proceso.	SGTD – PCM MEF	Demás entidades del Estado Peruano	M
			AEC5.1.4: Generar capacidades para la investigación y gestión de la evidencia digital.	CNSD - SGTD DINI	Demás entidades del Estado Peruano	M
			AEC5.1.5: Establecer mecanismos de supervisión y control para el cumplimiento del marco normativo referido a neutralizar la ciberdelincuencia.	CNSD – SGTD MINISTERIO PÑUBLICO – FISCALÍA DE LA NACIÓN	Demás entidades del Estado Peruano	M
			AEC5.1.6: Promover una gestión más eficiente de la justicia mediante contribuciones y propuestas relacionadas con la legislación actual.	AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS.	Demás entidades del Estado Peruano	M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
		OEEC5.2.- Monitoreo y seguimiento del ciberdelito o del cibercrimen a fin de implementar estrategias para su comunicación y posterior extinción.	**AEC5.2.1:** Facilitar el acceso de las personas a un mecanismo ágil que permita realizar la denuncia de los ciberdelitos	CNSD - SGTD DINI, DIVINDAT	Demás entidades del Estado Peruano	M
			AEC5.2.2: Incorporar al país, a los convenios internacionales y otros organismos relacionados a fin de hacer frente a la ciberdelincuencia.	SGTD – PCM MINISTERIO DEL INTERIOR	Demás entidades del Estado Peruano	M
4.5.6 CONSOLIDAR LA CIBERDEFENSA	OEGC6: Anticipar y gestionar escenarios de incidentes masivos que puedan impactar las operaciones nacionales y afectar a la población de forma total o parcial por causa de una ciberguerra.	OEEC6.1.- Robustecer el ecosistema de ciberdefensa del país mediante el refuerzo de capacidades institucionales para prevenir, detectar y responder a incidentes de Ciberseguridad que amenacen la seguridad nacional.	**AEC6.1.1:** Desarrollar una Estrategia Nacional de Ciberdefensa basada en prevención, detección temprana, respuesta coordinada y resiliencia, reforzada con formación continua y una cultura de Ciberseguridad en las Fuerzas Armadas y Comando Conjunto, para proteger la soberanía digital y contrarrestar ciberataques de escala estratégica o bélica.	MINDEF – COMANDO CONJUNTO DE LAS FUERZAS ARMADAS	PCM y demás entidades del Estado Peruano	M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
4.5.7 INVESTIGACIÓN, INNOVACIÓN Y CULTURA EN CIBERSEGURIDAD	OEGC7: Promover la innovación y avances tecnológicos en Ciberseguridad mediante inversión estratégica en I+D+i, impulsando soluciones disruptivas, así como empoderar a las entidades y demás actores del ecosistema digital, para usar las TIC de manera segura y responsable, protegiendo sus derechos y libertades en el ciberespacio.	OEEC7.1.- Impulsar I+D+i en Ciberseguridad para desarrollar tecnologías disruptivas.	**AEC7.1.1:** Incentivo a la innovación y la investigación en Ciberseguridad	SGTD – PCM CONCYTEC		M
			AEC7.1.2: Creación de centros de investigación y capacitación en Ciberseguridad	SGTD	MEF DINI	M
		OEEC7.2: Fomentar una cultura de Ciberseguridad que promueva la higiene digital como una práctica habitual.	**AEC7.2.1:** Impulsar programas especializados de capacitación y sensibilización dirigidos a operadores de infraestructuras críticas y usuarios estratégicos, promoviendo una cultura robusta de Ciberseguridad.	SGTD – PCM MINITER		M
			AEC7.2.2. Implementación de cursos de formación continua y certificaciones profesionales en Ciberseguridad promovidos por el estado peruano.	SGTD – PCM SUNEDU SECTOR PRIVADO ACADEMIA EN GENERAL	Demás entidades del Estado Peruano	C Y M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
			AEC7.2.3: Suscitar una cultura de Ciberseguridad en el Sistema Educativo Nacional.	SGTD – PCM MINEDU SUNEDU PRONABEC	Demás entidades del Estado Peruano	C, M Y L
4.5.8 COOPERACIÓN INTERNACIONAL	OEGC8: Fortalecer los mecanismos de cooperación internacional posicionando al Perú como un actor clave y confiable en la gobernanza del ciberespacio, tanto a nivel regional como internacional.	OEEC8.1.- Fomentar la cooperación bilateral y multilateral, contribuyendo al desarrollo de la confianza entre naciones y al aumento de la resiliencia global frente a amenazas digitales crecientes.	AEC8.1.1: Participar en foros regionales e internacionales y tratados sobre Ciberseguridad lo cual permita alinear al Perú con estándares internacionales y fomentar una cooperación eficaz ante amenazas cibernéticas globales.	SGTD-PCM MRE	Entidades del Estado Peruano que pudieran colaborar para dicho fin.	C Y M
			AEC8.1.2: Establecer protocolos y mecanismos de colaboración internacional para una respuesta coordinada y oportuna ante ciberataques.	PCM MRE MININTER - FFAA	Entidades del Estado Peruano que pudieran colaborar para dicho fin.	C Y M

Pilar	Objetivo Estratégico General de Ciberseguridad (OEGC)	Objetivo Estratégico Específico de Ciberseguridad (OEEC)	Acción Estratégica de Ciberseguridad (AEC)	Entidad responsable	Entidades colaboradoras	Implementado en corto (C), mediano (M) o largo plazo (L)
			AEC8.1.3: Promover la cooperación internacional en el desarrollo de estrategias de prevención y en la investigación de cibercrímenes y ciberterrorismo, en la lucha contra la ciberdelincuencia.	PCM MRE MININTER - FFAA	Entidades del Estado Peruano que pudieran colaborar para dicho fin.	C Y M

V. CONCLUSIONES

La Ciberseguridad es un desafío global que requiere un enfoque integral y colaborativo. En el contexto del país, la Presidencia del Consejo de ministros (PCM) a través de su Secretaría de Gobierno y Transformación Digital (SGTD), considera fundamental que, tanto el gobierno como las empresas, la academia y los ciudadanos adopten medidas proactivas para enfrentar las amenazas cibernéticas.

La ESNACIB es esencial para construir un futuro digital seguro, resiliente y confiable, mediante una gestión efectiva de los riesgos cibernéticos y la promoción de una cultura nacional e internacional de seguridad y cooperación. Su alineación con marcos internacionales y principios de gobernanza digital permite articular esfuerzos entre Estado, sector privado, academia y sociedad civil, fortaleciendo la corresponsabilidad, la transparencia y la legitimidad en la protección del ciberespacio nacional.

La ESNACIB, se sustenta en ocho (8) pilares estratégicos, los cuales decantan en objetivos estratégicos generales, específicos y acciones estratégicas. Los ocho pilares propuestos cubren desde el fortalecimiento de capacidades hasta la investigación e innovación, y permiten una respuesta estructurada y adaptativa ante amenazas. Su implementación busca reducir brechas tecnológicas, reforzar la ciberresiliencia y proteger infraestructuras críticas esenciales para el país. Cada objetivo cuenta con entidades responsables —como PCM, MINDEF, MTC y OSIPTEL— que aseguran liderazgo sectorial y ejecución coordinada. Esta arquitectura estratégica está orientada a generar valor público mediante servicios digitales seguros y confiables.

La ESNACIB 2026–2028 busca proteger los derechos digitales, garantizar la confianza en el entorno digital y consolidar un Estado seguro, moderno e inclusivo. Su valor público radica en fortalecer la seguridad ciudadana digital, promoviendo el bienestar común y la sostenibilidad del desarrollo económico y social.

La ESNACIB en el Perú no solo salvaguarda al Estado Peruano, Sector Privado, la sociedad civil, academia, entre otros, sino que también fortalece la economía, la seguridad nacional y la posición del país en el escenario global.

VI. REFERENCIAS

REFERENCIAS

2024 Data Protection Trends Report - VEEAM. (s. f.). Veeam Software. https://go.veeam.com/wp-data-protection-trends-2024

Albarrán, C., & Albarrán, C. (2024, 13 septiembre). *Índice Global de Ciberseguridad 2024: los países redoblan sus esfuerzos, pero no son suficientes*. Redes&Telecom. https://www.redestelecom.es/seguridad/indice-global-de-Ciberseguridad-2024/

Berkman Klein Center for Internet & Society. (2012) Keyword Index and Glossary of Core Ideas. Harvard University. Disponible en: https://cyber.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

Content Studio. (2024, 10 noviembre). ¿Qué es la seguridad cibernética? https://www.purestorage.com/la/knowledge/what-is-cybersecurity.html#:~:text=Seguridad%20cibern%C3%A9tica%3A%20tiene%20como%20objetivo,dominio%20de%20la%20seguridad%20cibern%C3%A9tica.

Centro Criptológico Nacional, C. C. (agosto de 2015). Guía de Seguridad (CCN-STIC-401). Glosario y Abreviaturas. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-determinos/22-401-descargar-glosario/file.html

Diario Oficial "El Peruano". *Perú lidera el ranking de detecciones de amenazas cibernéticas en Latinoamérica*. Noticias. Disponible en: https://elperuano.pe/noticia/255336-peru-lidera-el-ranking-de-detecciones-de-amenazas-ciberneticas-en-latinoamerica

Diccionario de la lengua española (23.ª ed.), [versión en línea]. https://dle.rae.es

Díaz Flores Corrales, Pedro (2012). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. McLean, Virginia, Estados Unidos. ISBN 1-4043-0641-2.

eSentire Inc. (2024, 29 agosto). *Cybersecurity Ventures Report on Cybercrime*. eSentire. https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime

Forrester: The State of Data Security, 2024. (2024, 25 octubre). Forcepoint. https://www.forcepoint.com/resources/industry-analyst-reports/forrester-state-data-security-2024-fb?sf_src_cmpid=7016T000002gGOSQA2&utm_term=prevent%20data%20breaches&utm_campaign=WW.ALL.DV.AD.SeP.VaC.Visibility_and_Control.Ever&utm_source=google&utm_medium=search_pd&hsa_acc=4948252953&hsa_cam=20959854868&hsa_grp=167029014623&hsa_ad=723424142090&hsa_src=g&hsa_tgt=kwd-309167547265&hsa_kw=prevent%20data%20breaches&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=EAIaIQobChMI3K3RuKSWiwMV-Q9ECB1jcBn9EAAYAyAAEgJ2MvD_BwE

Global Cybersecurity Outlook 2025. (s. f.). Foro Económico Mundial. Disponible en: https://es.weforum.org/publications/global-cybersecurity-outlook-2025/in-full/

IBM. (2022a). ¿Qué es un ataque cibernético? Disponible en: https://www.ibm.com/ar-es/topics/cyberattack?mhsrc=ibmsearch_a&mhq=INyeccion%20de%20sql

IBM. (2022b) ¿Qué es la seguridad móvil? Disponible en: https://www.ibm.com/ar-es/topics/mobile-security#:~:text=Phishing,n%C3%BAmeros%20de%20tarjetas%20de%20cr%C3%A9dito

IBM Security. (2020). *What is SOAR? Security Orchestration, Automation and Response Explained*. IBM. Disponible en: https://www.ibm.com/topics/soar

INCIBE, *Instituto Nacional de Ciberseguridad (2021). Glosario de términos de Ciberseguridad: una guía de aproximación para el empresario*. 14 Glosario de Ciberseguridad N°1 - Julio 2022. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

IsecT Ltd. www.isect.com. (s. f.). *ISO/IEC 27032 cybersecurity guideline*. Copyright © IsecT Ltd. 2023. Disponible en: https://www.iso27001security.com/html/27032.html

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Disponible en:

ISO/IEC 27032:2023. Cybersecurity — Guidelines for Internet security (n.d.). ISO. En: https://www.iso.org/standard/76070.html

National Institute of Standards and Technology. (September de 2012). Guide for Conducting Risk Assessments. NIST Special Publication 800-30, Rev. 1. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (mayo de 2015). *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82, Rev 2. Disponible en: http://dx.doi.org/10.6028/NIST.SP.800-82r2

National Institute of Standards and Technology. (September de 2020). Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Rev 5. Disponible en: https://doi.org/10.6028/NIST.SP.800-53r5

National Security Presidential Directive/NSPD-54 and Homeland Security Presidential Directive/HSPD-23. (8 de enero de 2008) Cybersecurity Policy. Disponible en: https://irp.fas.org/offdocs/nspd/nspd-54.pdf

National Institute of Standards and Technology (NIST). (2020). *Zero Trust Architecture (SP 800-207).* U.S. Department of Commerce. Disponible en: https://doi.org/10.6028/NIST.SP.800-207

OCDE (23 de mayo de 2022) Definición de Seguridad Digital, en: https://www.oecd.org/en/topics/digital-security.html

OCDE (2022), Marco de políticas de la OCDE sobre seguridad digital: Ciberseguridad para la prosperidad, Publicaciones de la OCDE, París, Disponible en: https://doi.org/10.1787/a69df866-en

ProInversion https://www.investinperu.pe, Agencia de Promoción de la inversión Privada. (s. f.). OECD evaluates Perú on responsible business conduct as part of accession process. ProInversión. https://www.investinperu.pe/en/pi/detail-news/oecd-evaluates-peru-on-responsible-business-condu?utm_source=chatgpt.com

Pollitt M. M. (1998). Ciberterrorism: Fact or Fancy. Computer Fraud & Security, vol.1998, issue 2. 8-10. Disponible en: https://doi.org/10.1016/S1361-3723(00)87009-8

Real Academia de Ingeniería. (s.f.). En Diccionario Español de Ingeniería 1.0. Recuperado el 19 de diciembre de 2024, de Real Academia Española. (2024). Disponible en: https://diccionario.raing.es/es/lema/ciberataque

Unión Internacional de Telecomunicaciones (UIT). (2021) *Guía para la elaboración de una estrategia nacional de Ciberseguridad. 2da Edición.* *https://ncsguide.org/wp-content/uploads/2024/05/508938S.pdf*

World Economic Forum. (2025). *Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards*. En colaboración con el Global Cyber Security Capacity Centre, University of Oxford. https://www.weforum.org

VII. ANEXO

ANEXO 1: ENTIDADES QUE COLABORARON BRINDANDO SUS COMENTARIOS, OBSERVACIONES Y/O APORTES AL DOCUMENTO

Nº	Nº DE DOCUMENTO	ENTIDAD	TIPO DE ENTIDAD
1	D00240DE2025	CUNA MÁS	A) PÚBLICA
2	002051-2025-MP-FN-SEGFIN	MINISTERIO PÚBLICO	A) PÚBLICA
3	OF. RE (OTI) N° 1-0/81	MINISTERIO DE RELACIONES EXTERIORES	A) PÚBLICA
4	0001-2025-GAF-FONAFE	FONAFE	A) PÚBLICA
5	CORREO ELECTRONICO	AGRORURAL	A) PÚBLICA
6	CORREO ELECTRONICO	INSN	A) PÚBLICA
7	CORREO ELECTRONICO	PRESIDENCIA	A) PÚBLICA
8	CORREO ELECTRONICO	OTASS	A) PÚBLICA
9	CORREO ELECTRONICO	ANIN	A) PÚBLICA
10	CORREO ELECTRONICO	SUNEDU	A) PÚBLICA
11	CORREO ELECTRONICO	PRONACEJ	A) PÚBLICA
12	CORREO ELECTRONICO	SANIPES	A) PÚBLICA
13	CORREO ELECTRONICO	MUNICIPALIDAD DE PIURA	A) PÚBLICA
14	CORREO ELECTRONICO	CONIDA	A) PÚBLICA
15	CORREO ELECTRONICO	MUNICIPALIDAD DE ASIA	A) PÚBLICA
16	CORREO ELECTRONICO	DRE CAJAMARCA	A) PÚBLICA
17	CORREO ELECTRONICO	INAGEIM	A) PÚBLICA
18	CORREO ELECTRONICO	PJ	A) PÚBLICA
19	CORREO ELECTRONICO	PROYECTO ESPECIAL DE INVERSION PUBLICA ESCUELAS BICENTENARIO	A) PÚBLICA
20	CORREO ELECTRONICO	SBS	A) PÚBLICA
21	000474-2025-FONCODES-DE	FONCODES	A) PÚBLICA
22	000079-2025-SENAMHI-GG	SENAMHI	A) PÚBLICA
23	000158-2025-IGP/PE	IGP	A) PÚBLICA
24	000001-2025-ITP/OTI	ITP	A) PÚBLICA
25	D000219-2025-IPEN-PRES	IPEN	A) PÚBLICA
26	CORREO ELECTRONICO	UNPRG	A) PÚBLICA
27	109-2025/GG/PATPAL-FBB	PARQUE DE LAS LEYENDAS	A) PÚBLICA
28	D000303-2025-CONADIS-PRE	CONADIS	A) PÚBLICA

Nº	Nº DE DOCUMENTO	ENTIDAD	TIPO DE ENTIDAD
29	000146-2025-SG-ACFFAA	ACFFAA	A) PÚBLICA
30	000146-2025-MIDAGRI-SENASA-OPDI	SENASA	A) PÚBLICA
31	000153-2025-BNP-GG	BNP	A) PÚBLICA
32	000381-2025-MIDIS-SG	MIDIS	A) PÚBLICA
33	D000003-2025-MIDAGRI-SERFOR-GG-OTI	MIDAGRI- SERFOR	A) PÚBLICA
34	000133-2025-IRTP-GG	IRTP	A) PÚBLICA
35	OFICIO N°D000120-2025-SUTRAN-GSF	SUTRAN	A) PÚBLICA
36	OFICIO N° 0333-2025-ANA-GG	ANA	A) PÚBLICA
37	D00155-GG-INAIGEM-2025	INAGEM	A) PÚBLICA
38	114-2025-GEG/INDECOPI	INDECOPI	A) PÚBLICA
39	OFICIO N° 00641-2025-MINAM/SG	MINAN	A) PÚBLICA
40	OFICIO N°186-2025-DV-GG	Comisión Nacional para el Desarrollo y Vida sin Drogas	A) PÚBLICA
41	OFICIO N°GSTI-87-2025/OS-OS	OSINERMING	A) PÚBLICA
42	OFICIO Nª000119-2025-INACAL/GG	INACAL	A) PÚBLICA
43	00077-2025-OSINFOR/01.1	OSINFOR	A) PÚBLICA
44	003-2025-MIDAGRI-INIA-GG-UI	MIDAGRI INIA	A) PÚBLICA
45	000033-2025-OTI-ONP	ONP	A) PÚBLICA
46	000374	INEI / OTIN	A) PÚBLICA
47	000008	ONPE	A) PÚBLICA
48	00007-2025-OEFA/OTI	OEFA / OTI	A) PÚBLICA
49	OFICIO Nº 273-2025-MINEDU/VMGI-PRONABEC	PRONABEC	A) PÚBLICA
50	00004-2025-JTI-GA-OSITRAN	OSITRAN	A) PÚBLICA
51	000103-2025-AGN/SG	AGN	A) PÚBLICA
52	1505 -2025-JUS/SG	MINJUS	A) PÚBLICA
53	000319-2025-MIDIS/PNADP-DE	MIDIS PNAD	A) PÚBLICA
54	OFICIO Nº 000085-2025-03.00/SENCICO	SENCICO	A) PÚBLICA
55	OFICIO Nº 1522-2025-GR.CAJ/DRE-DGA-DIR	GORE CAJAMARCA	A) PÚBLICA

Nº	Nº DE DOCUMENTO	ENTIDAD	TIPO DE ENTIDAD
56	OFICIO SIED Nro. 008-2025/8300/BN	BANCO DE LA NACIÓN	A) PÚBLICA
57	CARTA N°000258.- 2025.GG. OSIPTEL	OSIPTEL	A) PÚBLICA
58	786-2025-DG/INR	INR - DOCTORA ADRIANA REBAZA	A) PÚBLICA
59	304-2025-OGTI-MINSA	MINSA	A) PÚBLICA
60	000159-2025-SG-ACFFAA	ACFFAA	A) PÚBLICA
61	058-2025-DG-JNJ	JNJ	A) PÚBLICA
62	GCAD-1145-2025	PETROPERU	A) PÚBLICA
63	00955-2025-MINEDU/SG	MINEDU	A) PÚBLICA
64	000597-2025/SGEN/RENIEC	RENIEC	A) PÚBLICA
65	000005-2025-AGN/SG-OTIE	AGN	A) PÚBLICA
66	352-2025-SUNARP/ZRXI/JEF	SUNARP-ZRXI	A) PÚBLICA
67	000384-2025-FONDEPES/J	FONDEPEZ	A) PÚBLICA
68	193-2025-INBP/IN	BOMBEROS DEL PERÚ	A) PÚBLICA
69	001735-2025-SECRE/FAP	FAP	A) PÚBLICA
70	234-2025-CONCYTEC-P	CONCYTEC	A) PÚBLICA
71	108-2025-GG-ADINELSA	ADINELSA	A) PÚBLICA
72	003085-2025/SGTD	SUNARP	A) PÚBLICA
73	ENSA-GR-APG-0503-2025	DISTRILUZ	A) PÚBLICA
74	Carta G-0704-2025-EU	ELECTRO UCAYALI	A) PÚBLICA
75	0085-2025-INGEMMET-GG	INGEMMET	A) PÚBLICA
76	OFICIO No 00449-2025-SUNARP/ZRI/JEF	SUNARP2	A) PÚBLICA
77	395-2025-DG/DIRIS-LC	DIRIS LIMA - CENTRO	A) PÚBLICA