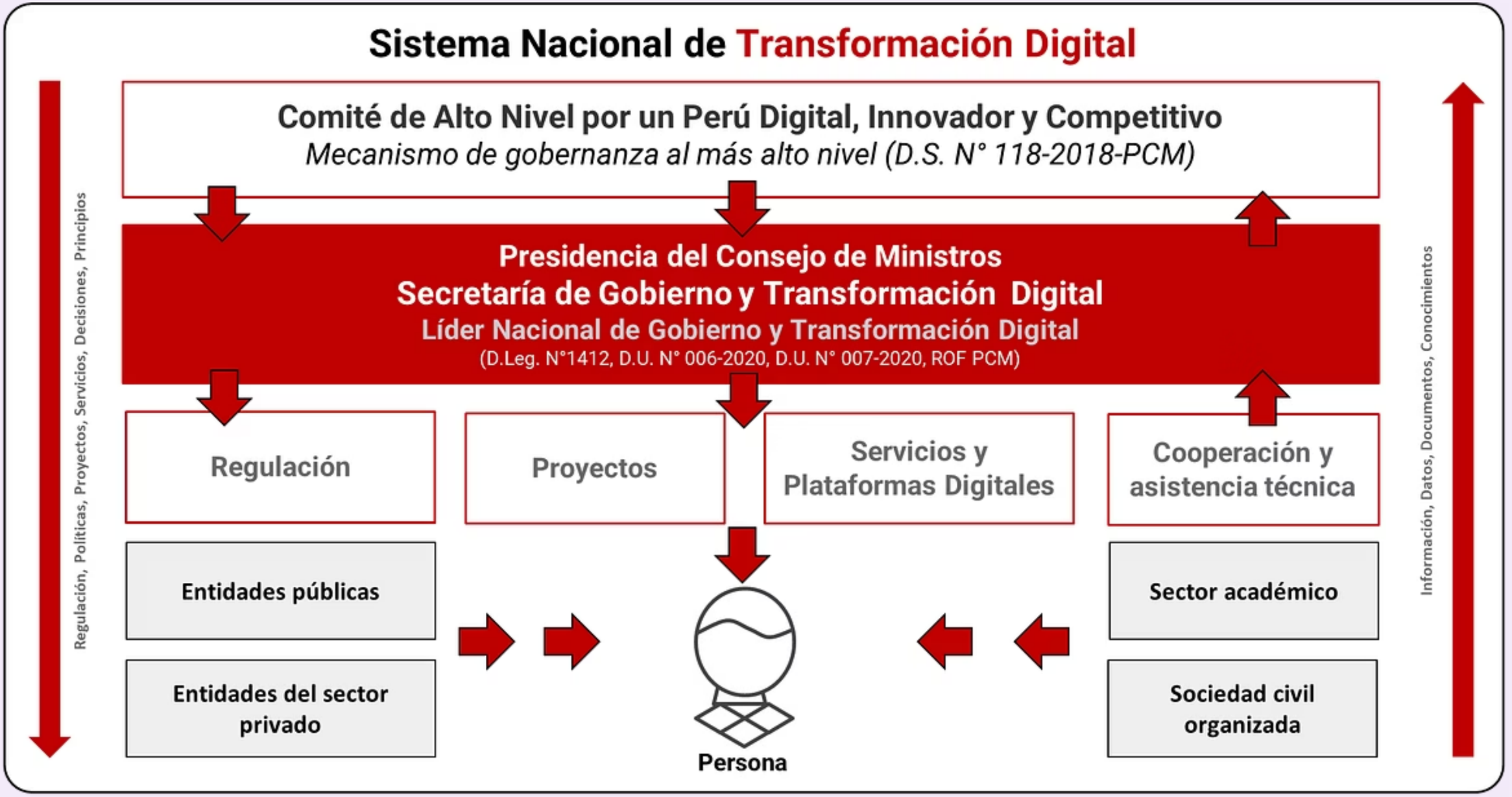
PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Avances en Ciberseguridad y Ciberdefensa

Ing. Orlando Vásquez Rubio
Secretaría de Gobierno y Transformación Digital
Presidencia del Consejo de Ministros

#PorUnPerúDigital



OECD/LEGAL/0475: Recommendation of the Council on International Regulatory Co-operation to Tackle Global Challenges

Marco Normativo

Nivel Base

Política de Estado 35 del Acuerdo Nacional y Decreto Supremo N° 103-2023 (Plan Estratégico de Desarrollo Nacional al 2050).

Nivel Estratégico

Decreto Supremo N.° 042-2023-PCM (Política General de Gobierno) y Decreto Supremo N.° 085-2023-PCM (Política Nacional de Transformación Digital).

Marco Operativo

Decreto Legislativo N° 1412 (Ley de Gobierno Digital) y Decretos de Urgencia para Sistema Nacional de Transformación Digital.

Innovación Tecnológica

Ley N.° 31814 promueve el uso de inteligencia artificial para desarrollo económico y social del país.

Política Nacional de Transformación Digital

Uso Ético de la Tecnología

Acceso Inclusivo

Seguridad Digital

Economía Sostenible

Talento Digital

Servicios Públicos Digitales

6 Objetivos Prioritarios

26 Lineamientos de acción

82 Servicios de política

Duplicar el ejercicio de la ciudadanía digital al 2030

Fortalecimiento de la Ciberseguridad y Ciberdefensa en Perú

Políticas de Ciberdefensa

Desarrollo de marcos legales y estratégicos para la defensa cibernética.

Colaboración Internacional

Asociarse con naciones extranjeras para compartir inteligencia y recursos.

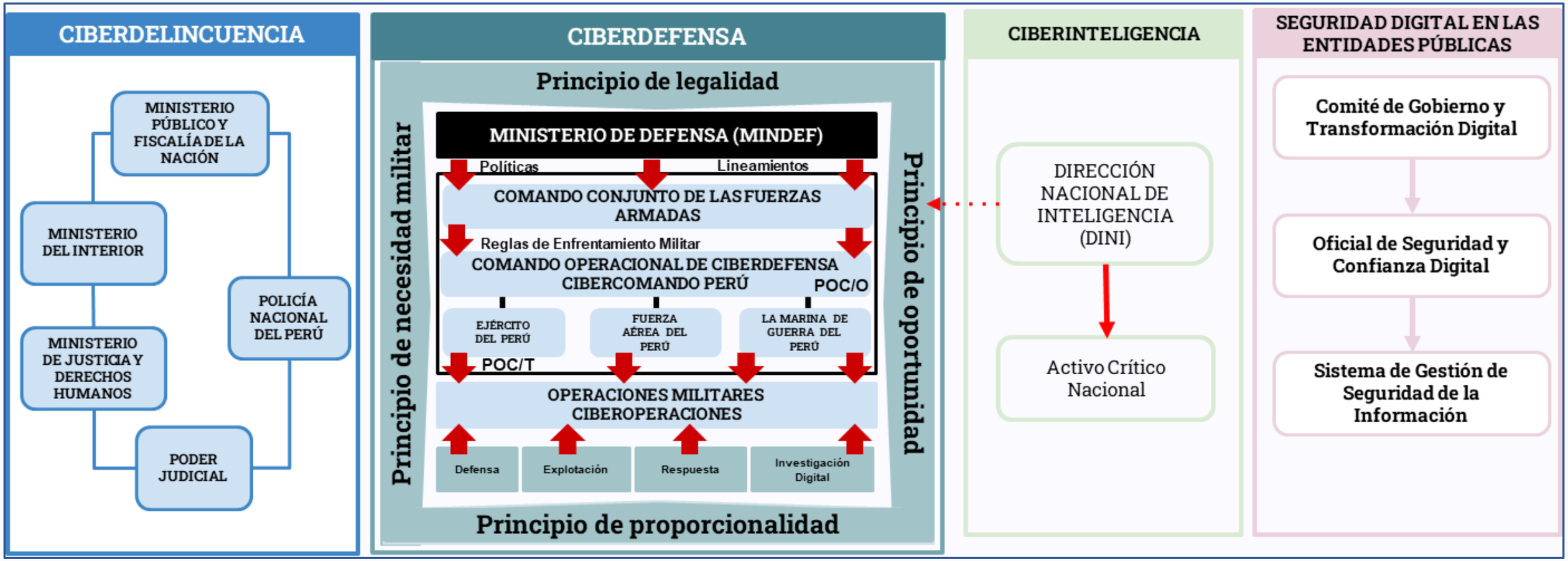
Infraestructura de Ciberseguridad

Mejora de los sistemas y redes para una mejor protección.

Capacitación en Ciberseguridad

Capacitar a los profesionales en las últimas técnicas y herramientas.

Seguridad Digital



Indicadores Internacionales

3

Nivel

Perú en "Estableciendo la ciberseguridad" según ITU 2024

9°

Posición Mundial

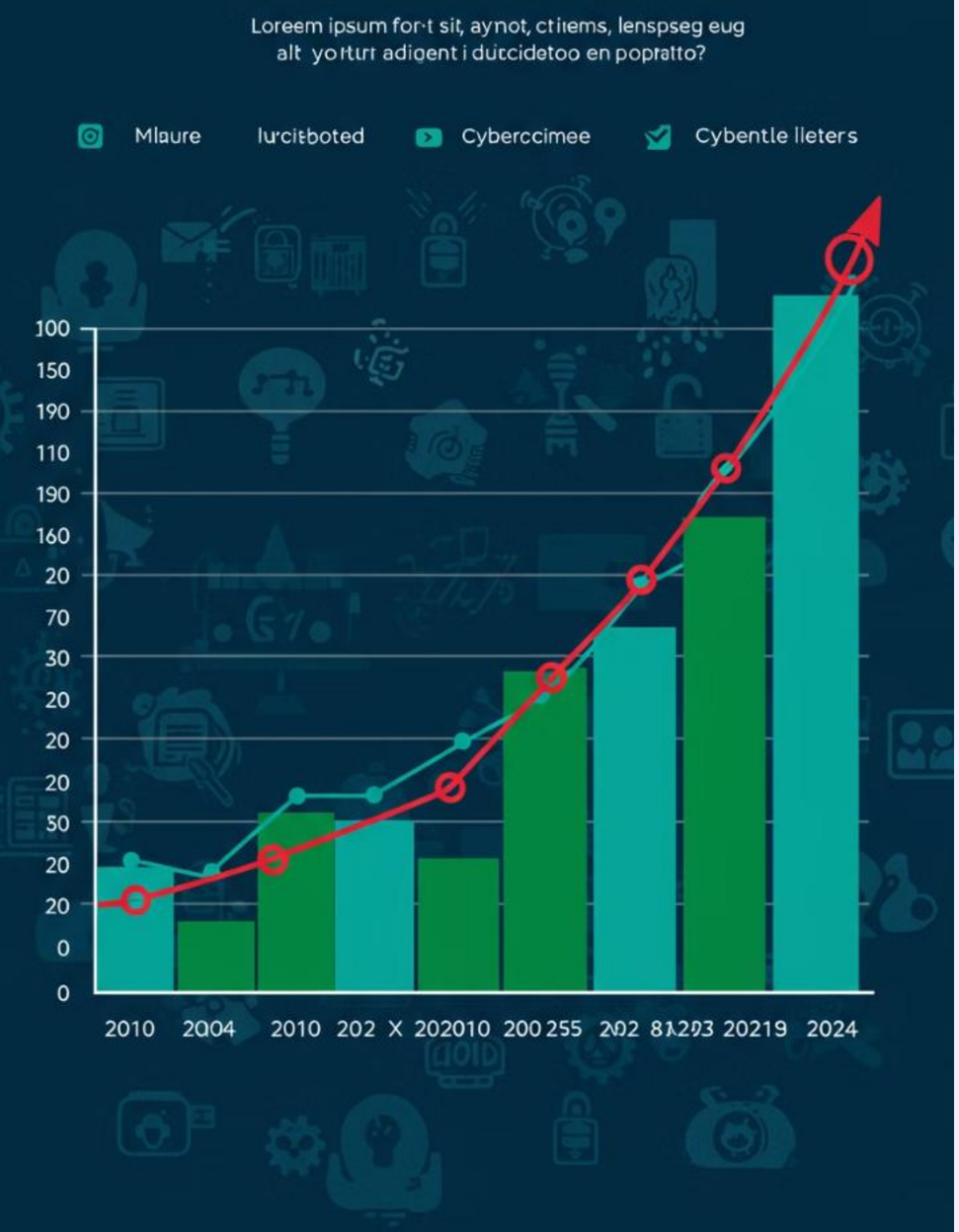
Entre los 49 países de la capa 3

7°

Posición América

Entre 35 países del continente

Brasil lidera en Latinoamérica (capa 1), seguido por Ecuador, México y Uruguay (capa 2). Perú integra la capa 3 junto con Chile, Colombia y otros países en desarrollo de capacidades.



El Desafío Digital

40%

Aumento de Delitos

Incremento en denuncias por ciberdelitos entre 2023 y 2024

1,685

Alertas Emitidas

Advertencias de seguridad digital generadas en 2024

4,269

Personas Capacitadas

Funcionarios formados en prácticas de seguridad digital

Coordinación y Articulación

Esta colección corresponde a un análisis técnico periódico realizado por 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 y la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en el marco del Centro Nacional de Seguridad Digital (CNSD).

Articulación en Ciberdefensa

Fuerza Aérea

Vigilancia del espacio aéreo digital y respuesta a amenazas emergentes

DINI

Inteligencia sobre amenazas cibernéticas y actores hostiles

PCM

Coordinación interinstitucional y articulación de políticas nacionales

PNP

Investigación forense digital y persecución de ciberdelincuentes

La articulación entre entidades permite una respuesta coordinada ante incidentes de seguridad que afecten la infraestructura crítica nacional.

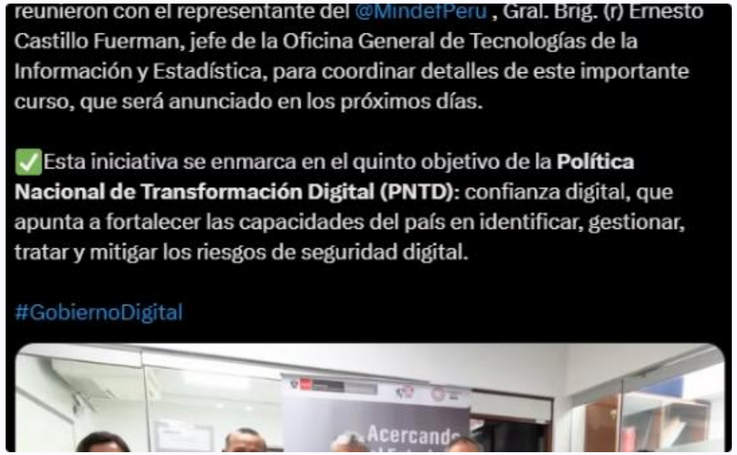
Articulación en Ciberdefensa

Comando Conjunto FFAA

Coordinación estratégica de operaciones de ciberdefensa a nivel nacional.

Ejército del Perú

Protección de infraestructuras críticas y respuesta táctica ante ciberataques.



Marina de Guerra

Seguridad de sistemas navales y protección del espacio marítimo digital.

Articulación con el MININTER

Video vigilancia

Grupo de Trabajo Multisectorial en apoyo a la Seguridad Ciudadana

Llamadas Prohibidas

Mesa de trabajo para prohibir las llamadas desde centros penales

Plan de Seguridad Digital APEC 2024

Elaboración de Estrategia

Plan integral con diversas entidades especializadas en ciberseguridad para reforzar la seguridad del foro.

Despliegue Operativo

400 especialistas en seguridad digital y ciberdefensa monitoreando eventos en el ciberespacio.

Resultados Exitosos

Plataformas y servicios digitales del Estado funcionaron con normalidad 24/7 durante la cumbre.

Coordinación efectiva entre SGTD, Ministerios, Fuerzas Armadas, DIVINDAT, Fiscalía, FBI y Centro de Ciberseguridad de USA.

Centro Nacional de Seguridad Digital

Gestión

Dirección estratégica de iniciativas de seguridad digital a nivel nacional.

Articulación

Coordinación entre entidades públicas y privadas para respuesta integrada.

Supervisión

Monitoreo constante del ecosistema digital nacional.

Punto de Contacto

Representación única en comunicaciones con organismos internacionales similares.

Red Nacional de Seguridad Digital

+800 Oficiales

Distribuidos en igual número de entidades públicas para vigilancia constante.

Monitoreo 24/7/365

Vigilancia permanente del ciberespacio nacional sin interrupciones.

Articulación Estratégica

Integración con PNP, Sector Defensa y entidades clave de protección digital.

Cooperación Internacional

Miembro activo de la Red de CSIRT Américas para colaboración regional.

Logros del CNSD en 2024

Asistencia Técnica

1,513 entidades recibieron soporte especializado

Capacitación

4,269 funcionarios formados en seguridad digital

Protección APEC

Seguridad digital para evento internacional clave

Simulacro Internacional

Más de 100 entidades participaron en ejercicios de ciberdefensa

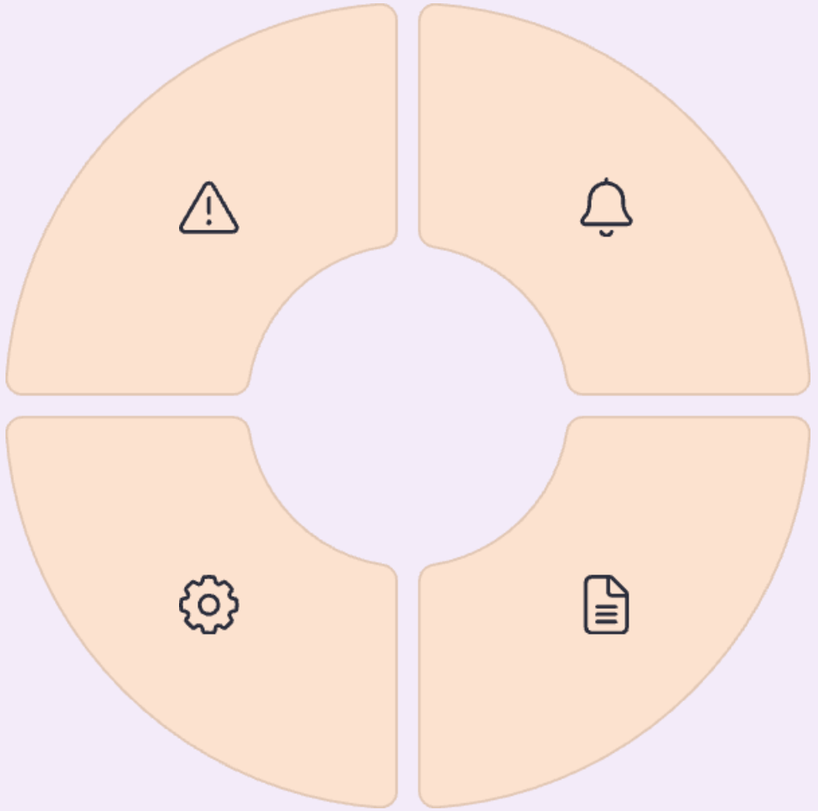
Avances 2025

Incidentes Atendidos

164 situaciones críticas resueltas

Alertas Emitidas

223 notificaciones de seguridad digital



Implementación de Herramientas

20 entidades con soluciones de seguridad actualizadas

Informes de Vulnerabilidades

36 análisis técnicos generados

Resultados: Gestión de Incidentes y Alertas

800+

Incidentes Gestionados

Con asistencia técnica especializada

1,180

Alertas Emitidas

Para prevención de intrusiones

90

Casos Derivados

30 a PNP-DIVINDAT y 60 a ANPDP

Resultados: Coordinación y Respuesta

185 Equipos Conformados

Equipos de respuesta ante incidentes de seguridad digital en entidades públicas nacionales.

Cooperación Internacional

Intercambio de información sobre amenazas con CSIRT de países miembros de la OEA.

Protección de Datos

Eliminación de 60 publicaciones en foros de hacking con datos personales filtrados.

Resultados: Capacitación y Concientización

Capacitación Ciudadana

6,766 ciudadanos formados en ciberseguridad, defensa, prevención e inteligencia artificial durante 2024.

Enfoque en desarrollo de competencias técnicas y conocimientos prácticos.

Alianza Nacional

Once sesiones sobre seguridad digital y protección de datos personales entre 2024-2025.

Más de 1,400 ciudadanos sensibilizados en gestión de riesgos digitales.

Programa SHE SECURES

Iniciativa con OEA para impulsar participación femenina en ciberseguridad.

Desarrollo de habilidades técnicas en seguridad digital para mujeres peruanas.

Simulacro Internacional de Ataques Cibernéticos

Objetivo Principal

Medir y fortalecer capacidad de reacción institucional ante ciberataques

Metodología

Simulación de ciberataques y evaluación de respuesta CSIRT

Dirección

Secretaría de Gobierno y Transformación Digital a través del CNSD

El simulacro se alinea con el quinto objetivo prioritario de la Política Nacional de Transformación Digital: garantizar la seguridad y confianza digital en el país.

Programa de Ciberseguridad y Ciberdefensa 2025

Objetivo Superior

Fortalecer capacidades digitales y resguardar el ciberespacio nacional

Alcance

Capacitación gratuita para más de 15 mil peruanos

Articulación

Iniciativa conjunta PCM y Ministerio de Defensa

Metodología

Formación virtual en dos fases complementarias

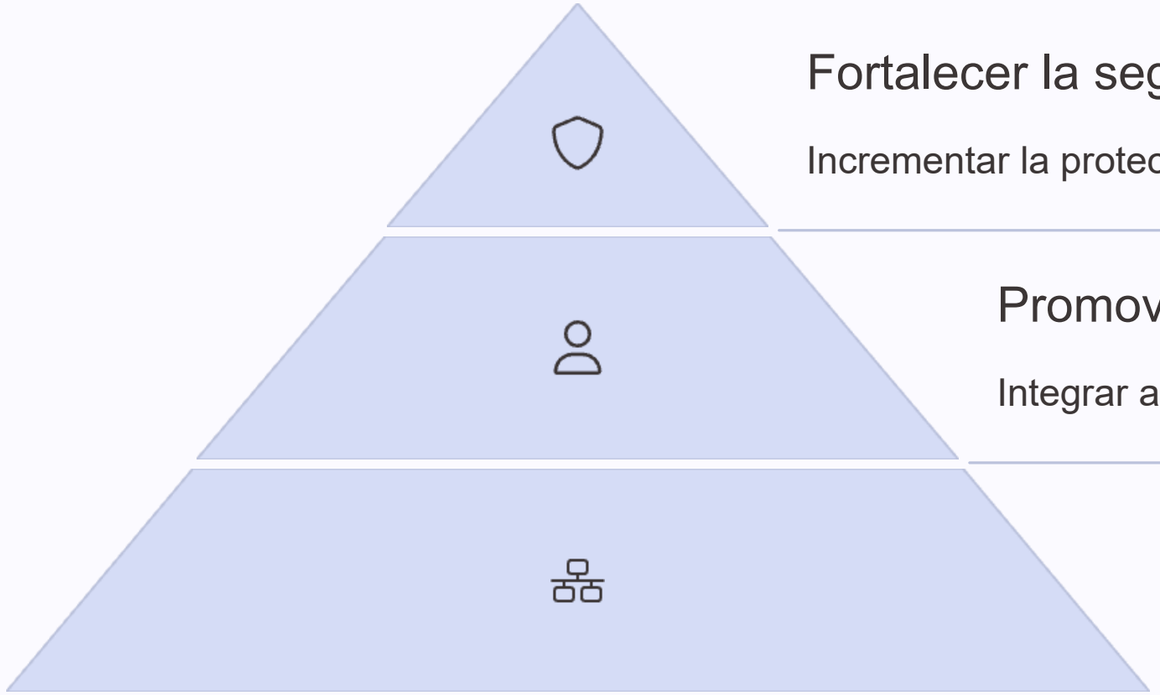
El programa responde a la creciente necesidad de proteger la información de entidades públicas, privadas y de la población en general frente a las amenazas digitales.

Marco de Confianza Digital:

Reglamento del Decreto de Urgencia N° 007-2020

Esta presentación detalla los elementos fundamentales del Marco de Confianza Digital, diseñado para garantizar interacciones seguras y transparentes en el entorno digital.

Objetivos y Principios Fundamentales



Fortalecer la seguridad

Incrementar la protección en todos los sectores digitales

Promover participación

Integrar actores públicos y privados en la estrategia

Articular marco

Implementar estructura coherente de confianza digital

Los principios rectores incluyen colaboración, gestión de riesgos, integridad y privacidad desde el diseño. El respeto a derechos humanos y transparencia completan estos pilares.

Estructura Institucional

SGTD-PCM

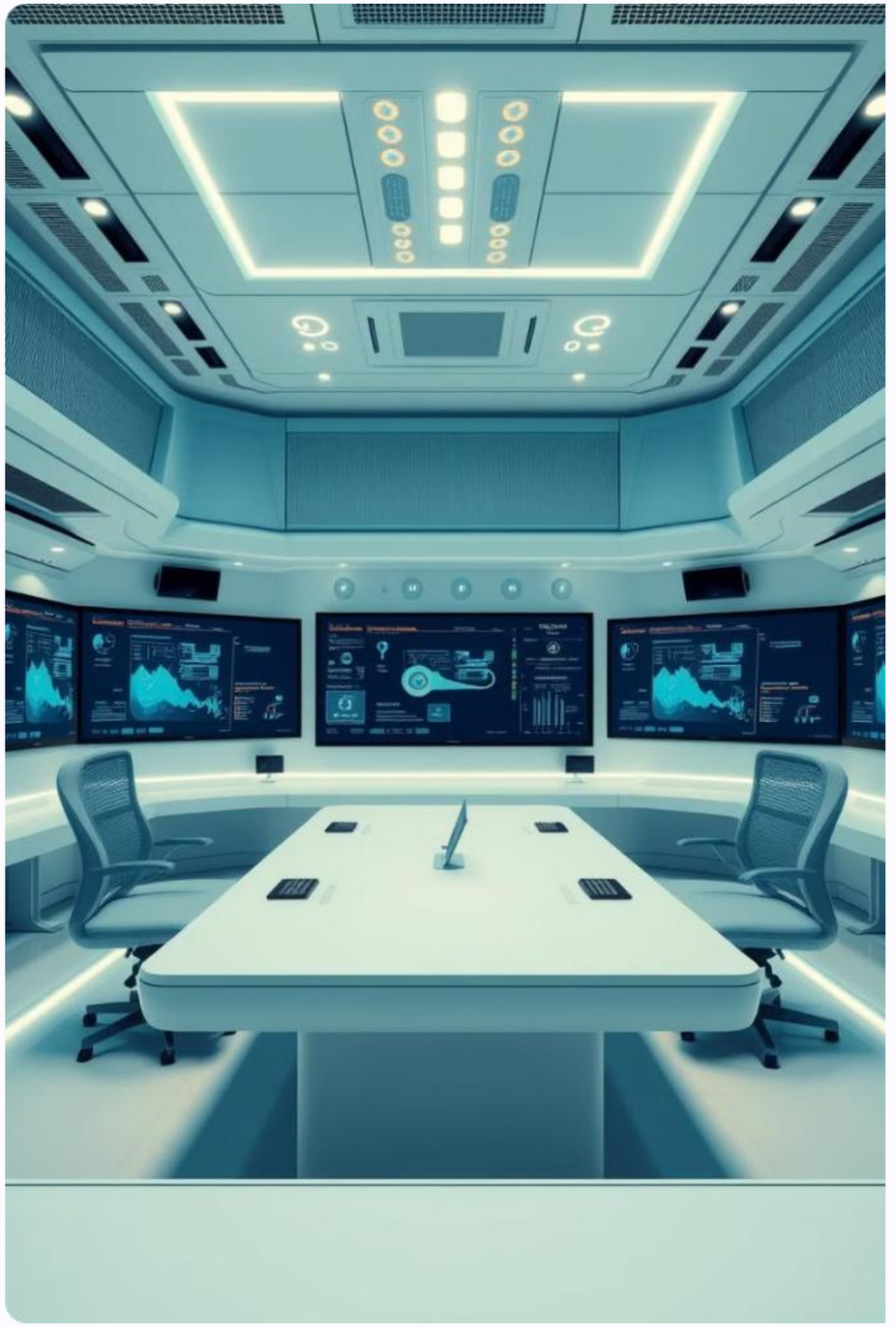
Ente rector del Marco de Confianza Digital. Articula políticas y supervisa implementación.

CNSD

Gestiona incidentes, monitorea riesgos y promueve cultura de seguridad digital.

ANPDP e INDECOPI

Protección de datos personales y defensa de derechos del consumidor digital.



Medidas de Seguridad Digital

Sector Público

- Identificación de actividades críticas
- Gestión de riesgos anual
- Oficial de Seguridad Digital

Sector Privado

- Estándares ISO y NIST
- Niveles de Confianza (NCA 1-3)
- Notificación de incidentes

Gestión de Incidentes y Fortalecimiento

Detección

Identificación mediante CSIRT Nacional y Registro de Incidentes

Notificación

48 horas para incidentes críticos mediante canales oficiales

Fortalecimiento

Sellos de confianza y Plataforma Nacional de Talento Digital

Respuesta

Aplicación de protocolos específicos según clasificación

Próximas Acciones

Fortalecimiento del CNSD

Implementación del Centro de Operaciones de Seguridad Digital (SOC) con inversión de S/50 millones.

Estrategia Nacional

Aprobación de Estrategia Nacional de Ciberseguridad alineada a la Política Nacional de Transformación Digital 2030.

Protección Electoral

Trabajo conjunto con ONPE, JNE, PNP, DINI y FFAA para resguardar el proceso electoral 2026.

Próximas Acciones

Sector Financiero

Formación de equipo técnico con representantes bancarios para fortalecer seguridad en ecosistema financiero.

Inclusión de Género

Impulso a la participación femenina en tecnología y ciberseguridad mediante programas especializados.

Cooperación Internacional

Fortalecimiento de alianzas con Corea del Sur, China,India, EAU, EE.UU. e Israel.

Protocolos de Respuesta

Desarrollo de protocolos de escalamiento en el Marco de la Ley de Ciberdefensa.

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

BICENTENARIO DEL PERÚ 2021 - 2024

Con Punche Perú

¡Gracias!

- www.gob.pe/transformaciondigital

@PeruPaisDigital

#PorUnPerúDigital