UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

CONPES 3995

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

Resumen Ejecutivo: CONPES 3995

Política Nacional de Confianza y Seguridad Digital de la República de Colombia

1. Resumen Ejecutivo y Visión General

El documento **CONPES 3995** constituye la Hoja de Ruta de Política Pública de Colombia orientada a consolidar la **Confianza y Seguridad Digital**. En el contexto de la Cuarta Revolución Industrial (4RI) y la creciente dependencia sistémica de las infraestructuras de tecnologías de la información y comunicación (TIC), el Estado colombiano identifica que la falta de capacidades técnicas, la fragmentación de la gobernanza institucional y la lenta adopción de marcos de ciberseguridad representan un riesgo directo para la estabilidad económica, la soberanía nacional y el bienestar ciudadano.

A diferencia de sus antecesores (CONPES 3701 de 2011 y CONPES 3854 de 2016) que enfocaron sus esfuerzos primordialmente en el fortalecimiento de capacidades militares y del gobierno central, el CONPES 3995 adopta una perspectiva integral y holística basada en las recomendaciones de la OCDE, el Foro Económico Mundial (FEM) y la Unión Internacional de Telecomunicaciones (UIT). Su meta central es construir un entorno digital resiliente, inclusivo y competitivo mediante tres ejes fundamentales: **fortalecimiento de capacidades operativas y humanas**, **modernización de la gobernanza institucional** y **adopción acelerada de estándares tecnológicos ante tecnologías emergentes**.

2. Contexto Estratégico y Justificación del Diagnóstico

El diagnóstico formulado en el documento revela vulnerabilidades estructurales en la postura de ciberseguridad del país, sustentado en métricas internacionales de referencia:

- **Índice de Evolución Digital (Tufts/Mastercard):** Colombia ocupó el puesto 32 entre 42 países en confianza digital (puntaje 2,33 vs. promedio global de 2,78), catalogando su entorno como 'moderado a débil'.
- **Índice Global de Ciberseguridad (UIT 2018):** Colombia descendió del puesto 46 (en 2017) al puesto 73 (en 2018) entre 175 naciones, evidenciando un rezago en la efectividad operativa y la velocidad de respuesta institucional.

- **Índice Nacional de Ciberseguridad (NCSI):** Puntuación de 46,75/100, identificando severas falencias en la protección de servicios digitales (0%), protección de servicios esenciales (17%) y gestión de crisis cibernéticas (20%).
- **Protección Infantil (COSI 2020):** Puesto 20 entre 30 países (34 puntos vs. 42 de promedio global), mostrando baja competencia digital y alta exposición de menores a ciberamenazas.
- **Sector Privado y Protección de Datos:** El 44% de 31.410 empresas evaluadas por la SIC presentaban un cumplimiento de medidas de ciberseguridad menor o igual al 25%. Solo el 15% superaba el 76% de implementación requerida.

EVALUACIÓN TÉCNICA DE CIBERSEGURIDAD
Las métricas evidenciaron que la superficie de ataque del país creció exponencialmente frente al aumento acelerado de ataques web e intentos de autenticación maliciosa (más de 536 millones de eventos registrados en Colombia entre 2017 y 2019 según Akamai), mientras que la preparación técnica y los marcos normativos se mantenían estáticos.

3. Objetivos Estratégicos y Plan de Acción Detallado

OE 1: Fortalecimiento de Capacidades (Ciudadanía, Sector Público y Privado)

- **Estrategia Nacional de Formación y Ciberhigiene:** Articulación entre DAPRE, MinTIC, MinDefensa, MinEducación, SIC y SENA para unificar campañas de concientización y diseñar currículos de uso seguro de TIC en toda la trayectoria escolar.
- **Inclusión y Enfoque Diferencial:** Programas específicos para reducción de brecha de género (potenciando talento femenino en ciberseguridad) y protección de comunidades vulnerables y líderes sociales.
- **Formación Especializada SENA y Marco NICE:** Creación de programas técnicos y profesionales alineados con el marco NICE (National Initiative for Cybersecurity Education) de EE.UU.
- **Infraestructuras Críticas y Sector Salud:** Definición de planes de mejora en seguridad digital para el Sistema de Seguridad Social Integral (SSSI),

considerando su condición de infraestructura crítica cibernética nacional. Creación del CSIRT del Sector de la Seguridad Social Integral y del CSIRT del Sector Inteligencia.
- **Registro Central Único de Incidentes:** Diseño de una plataforma unificada para el reporte obligatorio de incidentes y recolección normalizada de evidencia digital bajo el Código de Procedimiento Penal.

OE 2: Actualización del Marco de Gobernanza Institucional

- **Unidad de Política de Ciberseguridad:** Estructuración formal de la gobernanza de ciberseguridad bajo el Coordinador Nacional de Seguridad Digital (DAPRE) y el Comité de Seguridad Digital.
- **Sistema Nacional de Gestión de Incidentes Cibernéticos:** Liderado por MinDefensa para articular la respuesta ante ataques complejos, estandarizar estadísticas oficiales y servir de soporte a la toma de decisiones del Gobierno Nacional.
- **Modelo de Divulgación Responsable de Vulnerabilidades:** Protocolos de notificación entre descubridores de fallas, operadores de infraestructuras críticas e instancias del gobierno.
- **Sistema de Intercambio de Información Cibernética:** Plataforma para compartir Indicadores de Compromiso (IoCs) en tiempo real entre actores públicos, privados e internacionales.

OE 3: Adopción de Modelos y Estándares para la 4RI

- **Decreto Reglamentario de Gestión de Riesgos:** Expedición de normatividad vinculante bajo el Artículo 147 de la Ley 1955 de 2019 (PND).
- **Guías de Riesgo para Tecnologías Emergentes:** Desarrollo de metodologías de análisis de riesgo por MinTIC, MinDefensa y DNI para Inteligencia Artificial, IoT, Cloud Computing, Big Data y Blockchain.
- **Obsolescencia Tecnológica:** Lineamientos técnicos obligatorios para la actualización y deconstrucción segura de activos de TI obsoletos en el sector público.

4. Esquema Financiero e Inversión Presupuestal

La implementación de la política contó con un presupuesto estimado indicativo de **$8.342 Millones de Pesos Colombianos (COP)** distribuidos entre 2020 y 2022:

ENTIDAD EJECUTORA	2020 (MDP)	2021 (MDP)	2022 (MDP)	TOTAL INVERSIÓN
MinTIC (Ministerio de las TIC)	$450	$2.250	$1.850	$4.550 (54,5%)
DNP (Departamento Nacional de Planeación)	$0	$1.990	$1.010	$3.000 (36,0%)
DNI (Dirección Nacional de Inteligencia)	$0	$600	$0	$600 (7,2%)
Ministerio de Justicia y del Derecho	$24	$68	$72	$164 (2,0%)
SENA	$0	$14	$14	$28 (0,3%)
TOTAL GENERAL	**$474**	**$4.922**	**$2.946**	**$8.342 MDP**

5. Dictamen

> **ANÁLISIS CRÍTICO DE ARQUITECTURA E IMPLEMENTACIÓN**

> Como evaluación especializada de seguridad digital, el CONPES 3995 acierta tácticamente al introducir el concepto de confianza digital acoplado a la resiliencia operativa y no solo a la defensa militar. No obstante, desde la perspectiva de cibergestión práctica, el presupuesto asignado ($8,34 mil millones COP — aprox. USD 2,1 millones) resulta sumamente ajustado para la envergadura de las metas planteadas (creación de 2 nuevos CSIRTs sectoriales, desarrollo de plataformas de IoCs y modernización masiva de infraestructuras críticas). Por ello, el éxito real del modelo dependió de la capacidad de apalancamiento interinstitucional y la corresponsabilidad de inversión por parte del sector privado y las entidades territoriales.