

Estado de la Ciberseguridad y la Inteligencia Artificial en **Colombia**

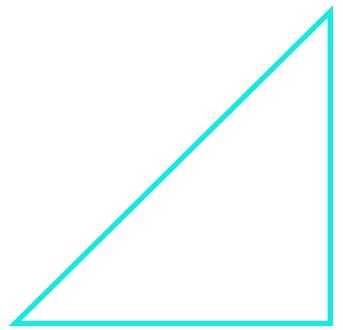




Estado de la Ciberseguridad y la Inteligencia Artificial en **Colombia**

Tanque de Análisis y Creatividad de las TIC - TicTac
Cámara Colombiana de Informática y Telecomunicaciones - CCIT

Germán López Ardila
Javier Lesmes
Valentina Díaz



Créditos

Equipo TicTac

Coordinador

Germán López Ardila

Co-autor

Javier Lesmes Patiño

Recopilación y apoyo investigativo:

Valentina Díaz Parra

Diseño y diagramación:

Paula Cruz Giraldo

Agradecimientos

Liliana Benítez

Pedro Romero

Sobre la CCIT

La Cámara Colombiana de Informática y Telecomunicaciones (CCIT) es una asociación gremial sin ánimo de lucro que reúne a las empresas más importantes de este sector en Colombia. Desde su fundación en 1993, ha desempeñado su papel como organización autorizada del sector tecnológico sin ánimo de lucro, reuniendo a actores del sector privado, la academia, la sociedad civil y el sector público, para promover el acceso a las tecnologías digitales en Colombia, romper la brecha digital y materializar la transformación digital.

Sobre el TicTac

El TicTac es el primer tanque de análisis y creatividad del sector TIC en Colombia, establecido por la CCIT con el fin de proponer iniciativas de política pública orientadas a la transformación digital del país, con base en la sostenibilidad y competitividad económica, la inclusión social y la eficiencia gubernamental.



Attribution-NonCommercial 4.0 International.

Copyright © CCIT 2025

Todos los derechos reservados.

La distribución y uso de este documento sin fines comerciales está permitida sin restricciones.

O p er en te n te c o n te n ci o n



1	Introducción \ 12
2	Panorama del ecosistema digital de Colombia
2.1	Infraestructura tecnológica \ 19
2.1.1	Conectividad digital \ 19
2.1.2	Dispositivos para la conectividad digital \ 24
2.1.3	Infraestructura de cómputo \ 12
2.2	Datos \ 29
2.3	Habilidades digitales \ 31
3	Políticas Digitales Transversales
3.1	Estrategia Nacional Digital \ 35
3.2	Colombia Potencia Digital \ 41
4	Ciberseguridad
4.1	Diagnóstico de país \ 47
4.2	Políticas Públicas y normatividad \ 60
4.3	Perspectivas de corto plazo \ 69
5	Inteligencia Artificial
5.1	Diagnóstico de país \ 72
5.2	Políticas Públicas y normatividad \ 87
5.3	Perspectivas de corto plazo \ 94
	Referencias \ 99

6699

En 2024, se reportaron 77.866 denuncias por delitos informáticos en Colombia, un aumento del 23% frente a 2023.

Resumen ejecutivo

La transformación digital en Colombia es un motor con el potencial de impulsar su desarrollo económico, social y ambiental. Sin embargo, para materializar estos objetivos es necesario entender el panorama actual de ciberseguridad e Inteligencia Artificial (IA), con el fin de garantizar que el ecosistema digital nacional sea seguro y confiable, a la vez que avanza en la adopción de tecnologías emergentes que consoliden las capacidades nacionales en todos los sectores. En ese sentido, el presente documento evalúa el estado de Colombia en estos dos frentes y establece unas recomendaciones preliminares, que esperamos sean útiles en los diálogos sobre el futuro digital del país.

En lo referente a la ciberseguridad, Colombia se enfrenta a un incremento de ciberamenazas, ciberataques y delitos informáticos, siguiendo una

tendencia mundial en el mismo sentido. Datos recientes proporcionados por SONICWALL ilustran esta realidad, con un aumento del 51% en los ataques de ransomware en Latinoamérica, cifra que subraya la vulnerabilidad de las organizaciones y los individuos en la región, incluida Colombia. De igual manera, el Centro Cibernético de la Policía Nacional de Colombia señala que, en **2024**, se realizaron **77.866** denuncias por delitos informáticos, un incremento del **23%** respecto a 2023.

Estas estadísticas refuerzan el hecho que la ciberseguridad se ha convertido en una prioridad ineludible para todos los actores de la sociedad colombiana, desde las entidades gubernamentales hasta el sector empresarial y los ciudadanos. Esto hace prioritario la construcción de políticas públicas y capacidades institucionales que permitan atender estas nuevas realidades del ecosistema digital.

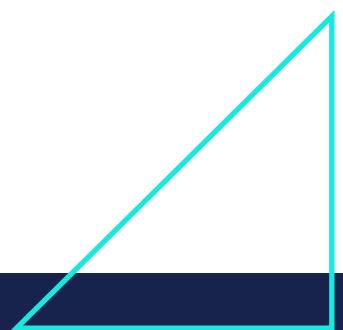
La creación de la *Agencia de Seguridad Digital* es crucial para mejorar la protección del ecosistema digital del país.

‘‘669’’



Así las cosas, aunque el Gobierno Nacional ha reconocido la importancia de la ciberseguridad y la seguridad y confianza digital, en documentos como el Plan Nacional de Desarrollo (PND) 2022-2026 y la Estrategia Nacional Digital (END) 2023-2026, **uno de nuestros hallazgos clave es la necesidad de acelerar y fortalecer la materialización de las acciones planteadas en estos documentos de política pública.** Al respecto, la Estrategia Nacional de Seguridad Digital, en la cual trabaja el Gobierno Nacional, es una oportunidad para contar con un instrumento adicional para fortalecer las capacidades del país en el corto plazo.

Asimismo, se espera que las acciones derivadas de esta estrategia no solo consoliden los objetivos de política ya definidos, sino que también se enfoquen en las áreas donde Colombia presenta mayores oportunidades de mejora y donde se puede robustecer la institucionalidad existente. En este contexto, la incertidumbre respecto al futuro del proyecto de ley para la creación de la Agencia de Seguridad Digital subraya la importancia de que la nueva estrategia avance de manera decidida en el **fortalecimiento de la institucionalidad de seguridad digital del país.**



En esa nota, identificamos la necesidad de **continuar consolidando las capacidades en ciberseguridad dentro del ecosistema digital nacional**. En este sentido, es necesario el **establecimiento de un marco institucional** que articule los diversos actores involucrados en la gobernanza de la seguridad digital en el país. Esto con el fin de **facilitar la implementación de políticas, la coordinación de respuestas ante incidentes y la promoción de una cultura de ciberseguridad a nivel nacional**. Además, consideramos vital la destinación de partidas presupuestarias específicas para que las entidades públicas puedan adquirir las soluciones de ciberseguridad necesarias para cumplir con el **Modelo de Gestión de Seguridad de la Información (MGSI)**, la normativa de protección de datos personales y, fundamentalmente, **garantizar los derechos digitales de los ciudadanos en el ecosistema digital**. Así pues, la inversión en tecnologías y herramientas de seguridad digital es un pilar esencial para **mitigar los crecientes riesgos cibernetíticos**.

Igualmente, Colombia debe continuar fortaleciéndose en el ámbito de cooperación internacional y adopción de estándares y mejores prácticas en el ámbito de ciberseguridad, para apoyar en el fortalecimiento de sus capacidades. Esta colaboración estratégica es clave en términos de acceso a recursos financieros y asistencia técnica especializada, elementos cruciales para el desarrollo e implementación de las acciones definidas en la nueva estrategia nacional de seguridad digital. Aprovechar estas oportunidades de cooperación internacional podría acelerar el progreso y permitir a Colombia **adoptar mejores prácticas y tecnologías en esta materia**.

Por otro lado, se destaca que la rápida digitalización tanto de las empresas como de las entidades públicas en Colombia está generando una creciente demanda de especialistas, productos y servicios de ciberseguridad, lo que a su vez mejora las perspectivas del mercado nacional en este sector. Sin embargo, se identifica una limitación importante: la escasez de capital humano calificado en esta área. Esta brecha de talento podría representar un obstáculo significativo y retrasar el desarrollo y consolidación del ámbito de la ciberseguridad en el país en los próximos años. Por lo tanto, la inversión en programas de formación y la promoción de carreras en ciberseguridad se consideran acciones prioritarias.

En cuanto al desarrollo y la adopción de IA en Colombia, el diagnóstico realizado por el reciente CONPES 4144 de 2025 señala que el país presenta bajas capacidades para la investigación, desarrollo, adopción y aprovechamiento ético y sostenible de sistemas de IA en asuntos estratégicos a nivel social, económico y ambiental. Esta limitación coloca a Colombia en una posición menos favorable en comparación con otros países de la región y a nivel global. No obstante, el CONPES 4144 también destaca un aspecto positivo: el abordaje conceptual de la política propuesta, que incluye factores habilitantes, la promoción de la adopción y la consideración de los riesgos responde a las necesidades identificadas para el país.

Por lo tanto, este documento sirve como una hoja de ruta para fortalecer la preparación del país para adoptar IA y acelerar su implementación en relación con los avances y el aprovechamiento de esta tecnología a nivel mundial.

Un hallazgo relevante es la importancia de promover la adopción de una política pública transversal de IA que permita a Colombia desarrollar sus capacidades sin la imposición de regulaciones que restrinjan injustificadamente la adopción y masificación de esta tecnología. En este sentido, consideramos fundamental la promoción de medidas que incentiven la inversión en IA y la articulación con actores privados, así como en los habilitadores digitales necesarios, tales como infraestructura de cómputo, datos y talento digital. Adicionalmente, sugerimos que las iniciativas legislativas en materia de IA se desarrollos de acuerdo con estándares y mejores prácticas internacionales, y tengan en cuenta los lineamientos y principios establecidos en el CONPES 4144 y la Hoja de Ruta del Ministerio de Ciencia, Tecnología e Innovación (MinCiencias).

“Sin duda alguna, es enorme el potencial de la IA como una tecnología de propósito general capaz de contribuir a la solución de los grandes desafíos que enfrenta Colombia a nivel económico, social y ambiental.”

Por lo tanto, las acciones derivadas de la nueva política nacional de IA deben enfocarse en apuestas que, a corto plazo, fortalezcan los habilitadores necesarios e impulsen la adopción de la IA en diversos sectores socioeconómicos y territorios del país. Adicionalmente, consideramos estratégico el aprovechamiento de iniciativas ya en marcha, como los **centros de IA que está desarrollando el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)**, para acelerar este proceso.

En el ámbito internacional, Colombia debe fortalecer su cooperación con distintos actores relevantes para el ecosistema global de IA, como la OCDE y UNESCO.

Estas colaboraciones serán claves para la implementación de la nueva política nacional de IA, así como para participar activamente en discusiones y proyectos estratégicos a nivel regional e internacional.

El objetivo es que **Colombia pueda aprovechar al máximo los beneficios de la IA** y posicionarse como un actor relevante en el contexto latinoamericano.

Finalmente, subrayamos la **prioridad de fortalecer la gobernanza de la IA** en Colombia, promoviendo una gobernanza basada en el conocimiento, la articulación y coordinación efectiva de las iniciativas desarrolladas por el Gobierno nacional, el sector privado y las demás partes interesadas. Asimismo, consideramos fundamental fomentar discusiones centralizadas al interior del Congreso de la República en torno a los proyectos de ley en curso sobre IA, así como promover el diálogo y la colaboración entre las entidades del Estado, la academia, el sector privado y las organizaciones de la sociedad civil en la construcción de cualquier iniciativa legislativa. El objetivo es consolidar una visión compartida sobre el desarrollo, la adopción y la regulación de la IA en Colombia, buscando un equilibrio que promueva la innovación, garantice la seguridad y fomente la confianza en el uso de esta tecnología.



En conclusión, Colombia se encuentra en un momento crucial en su proceso de transformación digital. Si bien existen avances y un reconocimiento de la importancia de la ciberseguridad y la IA, se requiere una acción decidida y coordinada para acelerar la implementación de las políticas existentes, fortalecer las capacidades nacionales, fomentar la colaboración entre los diferentes actores y aprovechar las oportunidades de cooperación internacional.



Solo a través de un esfuerzo conjunto y una visión estratégica clara, Colombia podrá maximizar los beneficios de la digitalización y mitigar los riesgos asociados, posicionándose de manera competitiva en la economía digital global.



Introducción





1.

Introducción

El avance acelerado de las tecnologías digitales y su adopción generalizada no solo están transformando la manera en que personas, empresas y entidades públicas interactúan, sino también están brindando nuevas oportunidades para superar varios desafíos que los países tienen a nivel económico, social y ambiental (Banco Mundial, 2023). En este sentido, cada vez es más necesario comprender los beneficios y desafíos que traen consigo estas tecnologías, especialmente las emergentes como la Inteligencia Artificial (IA), así como identificar los aspectos en los que se debe avanzar para que todos los agentes de la sociedad puedan aprovechar estas tecnologías en un entorno digital confiable y seguro.

Colombia ha realizado importantes esfuerzos y tiene avances significativos en su proceso de transformación digital. Sin embargo, aún tiene grandes desafíos por superar, que impactan directamente el desarrollo y adopción de la IA y la capacidad del país para gestionar las crecientes amenazas ciberneticas. Uno de los aspectos a destacar dentro de los avances de Colombia es la generación de un ambiente habilitador para el desarrollo del ecosistema digital, que se ha materializado a través de la formulación de políticas públicas para impulsar la transformación digital como, por ejemplo, la Estrategia Nacional Digital 2023-2026, y la expedición de regulación y leyes relacionadas con las Tecnologías de la Información y las Comunicaciones (TIC), la protección de datos personales y la ciberdelincuencia.

No obstante, el país tiene un gran desafío en cuanto a conectividad digital y el desarrollo de habilitadores digitales para las tecnologías emergentes, que involucra data centers, computación en la nube y capacidad de cómputo. De igual forma, el país enfrenta **retos importantes en cuanto a talento y habilidades digitales, e investigación, desarrollo e innovación**.

En términos generales, **Colombia está en un nivel intermedio con respecto a su proceso de transformación digital, así como en el desarrollo de un entorno seguro y aprovechamiento de la IA, por lo cual, necesita acelerar sus esfuerzos para tener un mayor avance, capturar los beneficios que representan las tecnologías digitales y así no quedar rezagado**. Aunque los puntajes y posiciones obtenidas por Colombia en las mediciones y estadísticas revisadas muestran que no es un país que esté iniciando en cuanto a transformación digital, ciberseguridad o IA, si queda en evidencia que está quedándose rezagado, incluso con respecto a otros países de América Latina. Por lo cual, dentro de las perspectivas de corto plazo, se destaca la importancia de que las políticas públicas, que actualmente está desarrollando el Gobierno Nacional con respecto a ciberseguridad e IA, se publiquen lo más pronto posible para también así iniciar prontamente su ejecución.

El desarrollo del presente documento tuvo en cuenta mediciones internacionales y estadísticas nacionales, así como documentos técnicos y de

política pública, que abordan los avances de Colombia en cuanto a transformación digital, materialización de capacidades de ciberseguridad, y desarrollo y adopción de IA. En cada caso, se consideró la información más actualizada que estaba disponible de manera pública a la fecha de elaboración del documento.

El documento está compuesto por esta introducción y cuatro secciones más. De estas cuatro secciones, la primera presenta el panorama del ecosistema digital de Colombia, haciendo énfasis en el estado de los habilitadores estratégicos de la transformación digital; la segunda contextualiza y destaca los objetivos y principales metas de la Estrategia Nacional Digital de Colombia 2023-2026, y la tercera y la cuarta presentan el diagnóstico y las perspectivas del país a corto plazo con respecto al desarrollo de capacidades en ciberseguridad y el desarrollo y adopción de IA, respectivamente. En ambos casos se hace énfasis en los aspectos relacionados más relevantes.



Panorama del ecosistema digital **de Colombia**



2.



Panorama del ecosistema digital de Colombia

El avance acelerado de las tecnologías digitales y su adopción generalizada no solo está transformando la manera en que personas, empresas y entidades públicas interactúan, sino que también está brindando nuevas oportunidades para superar varios desafíos que los países tienen a nivel económico, social y ambiental (Banco Mundial, 2023). En este sentido, los países han estado diseñando diferentes planes y estrategias para impulsar el acceso, uso y aprovechamiento de los datos y tecnologías digitales, de tal manera que puedan capitalizar los beneficios que representa la Cuarta Revolución Industrial.

Colombia ha realizado importantes esfuerzos y tiene avances significativos en su proceso de transformación digital, sin embargo, aún tiene grandes desafíos por superar. Esto ha quedado en evidencia en mediciones globales como el Global Digitalization Index (GDI) 2024¹ de Huawei y del International Data Corporation (IDC) y el World Digital Competitiveness Ranking (WDC) 2024² del Institute for Management Development (IMD), que miden los avances de los países en cuanto al desarrollo de los habilitadores de la transformación digital y el grado de adopción de las tecnologías digitales para la transformación de las prácticas gubernamentales, los modelos empresariales y la sociedad en general (*Ver Tabla 1 y Tabla 2*).

¹ El IDG 2024 mide el progreso de la digitalización de 77 países utilizando 42 indicadores bajo cuatro dimensiones: i) *Conectividad ubicua*: considera que el acceso a conexiones de red estables y continuas es una necesidad básica y un derecho de todos, es la base de una economía digital inclusiva (por ejemplo, 5G y fibra óptica); ii) *Fundación digital*: considera que es necesario una base digital que respalde el almacenamiento, el procesamiento y la computación de los datos (por ejemplo, centros de datos, potencia de cálculo, computación en nube); iii) *Energía verde*: considera la producción de fuentes de energía renovable como la solar y la eólica, teniendo en cuenta que estas fuentes son importantes para un desarrollo sostenible de la economía digital; y iv) *Política y ecosistema*: Hace referencia a que los gobiernos deben habilitar la transformación digital, ya que se encuentran en una posición única para proporcionar apoyo sistemático en términos de organizaciones, fondos, políticas y regulaciones. El IDG 2024 agrupa a los países en tres clústeres: Frontrunners, Adopters y Starters.

² El WDC 2024 analiza y clasifica el grado en que 67 países adoptan y exploran las tecnologías digitales que conducen a la transformación de las prácticas gubernamentales, los modelos empresariales y la sociedad en general. Para ello tiene en cuenta tres factores: i) *Conocimiento*: conocimiento necesario para descubrir, entender y construir nueva tecnología (talento, educación y entrenamiento, y concentración científica); ii) *Tecnología*: contexto general que habilita el desarrollo de tecnologías digitales (marco regulatorio, capital y marco tecnológico); y iii) *Preparación para el futuro*: nivel de preparación del país para aprovechar la transformación digital (aptitudes adaptativas, agilidad en los negocios, e integración IT). Estos tres factores con sus respectivos sub-factores consideran 59 criterios alrededor de estos asuntos.

Tabla 1. Resultados del Global Digitalization Index 2024

País	Posición	Puntaje				
		Total	Conectividad ubicua	Base digital	Energía verde	Política y ecosistema
Estados Unidos	1	78,8	66,4	91,2	24,0	96,9
Singapur	2	76,1	72,8	87,6	19,2	86,8
Suecia	3	74,5	65,6	75,6	69,6	84,0
Chile	30	49,5	50,4	39,6	31,2	64,6
Colombia	49	39,9	31,2	33,6	19,2	61,8

Fuente: Elaboración propia a partir de (Huawei y IDC, 2024)

Tabla 2. Resultados del World Digital Competitiveness Ranking 2024

País	Posición	Puntaje			
		Total	Conocimiento	Tecnología	Preparación para el futuro
Singapur	1	100,00	95,40	97,58	100,00
Suiza	2	93,15	95,90	88,16	88,38
Dinamarca	3	91,99	85,76	86,48	96,72
Chile	42	61,71	51,38	62,72	64,01
Colombia	58	48,19	46,84	38,79	51,93

Fuente: Elaboración propia a partir de (IMD, 2024).

De acuerdo con el GDI 2024 y el puntaje obtenido para la dimensión denominada **"Política y ecosistema"**, uno de los aspectos a destacar dentro de los avances de Colombia es la generación de un ambiente habilitador para el desarrollo del ecosistema digital, que se ha materializado a través de la formulación de políticas públicas para impulsar la transformación digital, y la expedición de regulación y leyes relacionadas con las Tecnologías de la Información y las Comunicaciones (TIC). De igual forma, en el marco de este índice, **Colombia se destaca por sus avances en la apropiación de las tecnologías digitales por parte de las entidades públicas**. Esto está en línea con lo identificado en el diagnóstico país realizado por el (Banco Mundial, 2023), en el cual se menciona que Colombia está

entre los países más avanzados en América Latina en términos de gobierno digital.

Sin embargo, **el país tiene un gran desafío en cuanto al servicio de acceso a Internet y la generación de las capacidades tecnológicas para el aprovechamiento de tecnologías emergentes como la Inteligencia Artificial (IA)**. Tanto en el GDI 2024 como en el WDC 2024, las dimensiones en las que Colombia tiene los desempeños más bajos con respecto a los otros países son aquellas relacionadas con conectividad digital y el desarrollo de una base tecnológica para las tecnologías emergentes, que involucra data centers, servicios de la nube y capacidad de cómputo.

Esto se debe a las brechas que tiene el país en cuanto a acceso al servicio de Internet fijo y móvil, principalmente, en los hogares rurales y de bajos ingresos, y a la necesidad de un mayor despliegue de tecnologías como fibra óptica, servicios satelitales y 5G. Por otra parte, aunque se destaca la inversión en telecomunicaciones, el país registra una baja inversión en relación con data centers, servicios de la nube y capacidad de cómputo, lo cual está acompañado de oportunidades de mejora con respecto a la creación y disponibilidad de datos de calidad que sirvan para el desarrollo y escalabilidad de plataformas y aplicaciones.

Colombia también enfrenta desafíos importantes en relación con el talento y las habilidades digitales. En el WDC 2024, después de “Tecnología”, la dimensión denominada “Conocimiento” es en la que el país obtiene un menor desempeño. Aunque se destaca el gasto que realiza el Gobierno Nacional en educación, Colombia no queda bien posicionado en cuanto a los resultados de las pruebas PISA en Matemáticas, la oferta y calidad de educación en ciencias de la computación, y las habilidades digitales de la población. Asimismo, de acuerdo con

el GDI 2024, la fuerza laboral del país relacionada con TIC y la proporción de los estudiantes graduados en áreas STEM (Science, Technology, Engineering and Mathematics) del total de graduados está por debajo de los niveles obtenidos por países líderes como Singapur y Suecia.

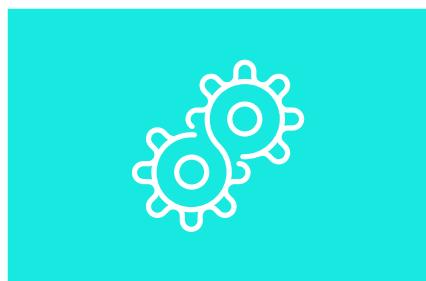
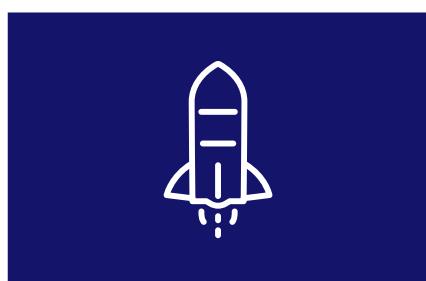
En el país aún existe una proporción importante de personas que no usa Internet y aquellos que ya son usuarios, lo utilizan principalmente para redes sociales. De acuerdo con el GDI 2024 y el WDC 2024, el número de usuarios de Internet en Colombia está por debajo del promedio de los países considerados en las mediciones. Adicionalmente, si bien el número de usuarios de Internet en el país ha incrementado en los últimos años, los usos en actividades como el comercio electrónico o el relacionamiento con entidades del Gobierno están por debajo de lo registrado en los países líderes en transformación digital. Asimismo, el país tiene oportunidades de mejora en la tenencia de dispositivos como teléfonos inteligentes, computadores o tabletas que permitan tener una mejor apropiación de Internet y de tecnologías digitales emergentes.



Las empresas en Colombia aún tienen un bajo uso y apropiación de las tecnologías digitales, especialmente de las emergentes. De acuerdo con el WDC 2024, de los 67 países o economías consideradas, Colombia está en el puesto 33 en el uso de big data y analítica por parte de empresas.

En este sentido, el GDI 2024 muestra que Colombia está por debajo del promedio de los países considerados, con respecto al gasto que realizan las empresas en procesos de transformación digital. Por otra parte, a partir de estas mediciones, si bien se identifica que el número de startups en el país es aún bajo, también se registra una percepción positiva con respecto a iniciar un negocio en el país.

Colombia es un país que ha estado avanzando en su proceso de transformación digital, pero necesita acelerarlo para no rezagarse y capturar los beneficios que representan las tecnologías digitales. Aunque los puntajes y posiciones obtenidas por Colombia en las mediciones revisadas muestran que no es un país que esté iniciando en este proceso, es necesario reforzar esfuerzo, con el fin de acercarse a los países en las primeras posiciones, que son los pioneros o están en la frontera tecnológica.



El país ha tenido avances tanto en el desarrollo de los habilitadores de la transformación digital como en el impulso al uso y apropiación de los datos y las tecnologías digitales por parte de personas, entidades públicas, y empresas, pero se necesita actuar con una mayor contundencia para superar los desafíos existentes y hacer de las tecnologías digitales un pilar del desarrollo económico y bienestar social del país.

“

Teniendo en cuenta la importancia de habilitadores como el acceso a Internet y el desarrollo de infraestructura tecnológica, así como la disponibilidad de habilidades, para la adopción y aprovechamiento de las tecnologías digitales emergentes como la IA, **en las siguientes secciones se profundizará un poco más en cuanto a la evolución y estado actual de estos habilitadores en Colombia.**

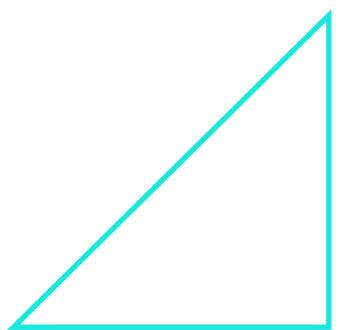
”

2.1



Infraestructura tecnológica

2.1.1 Conectividad digital

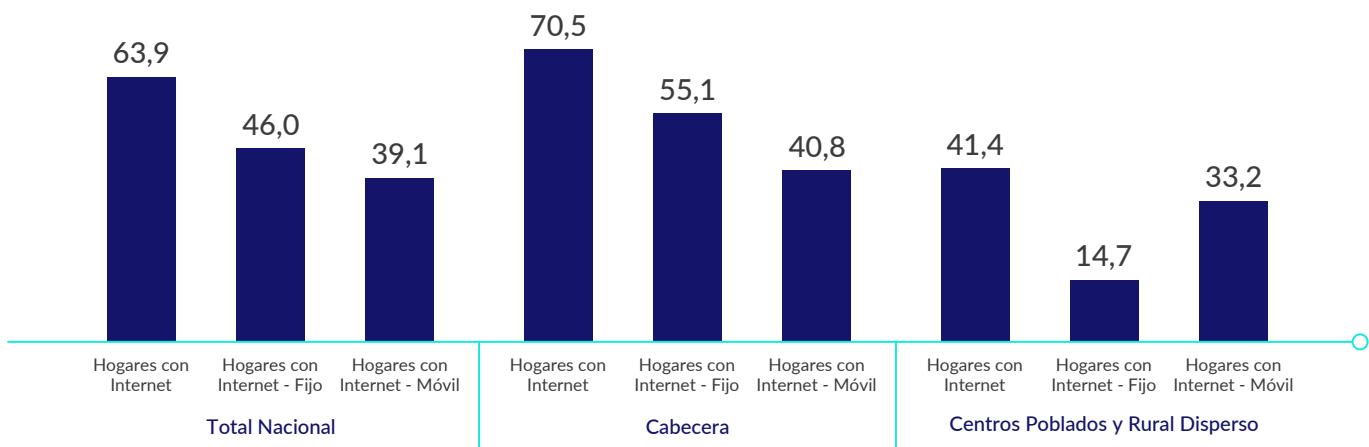


A pesar de los avances, **en Colombia persisten las brechas en el acceso al servicio de Internet, principalmente en las zonas rurales y apartadas del país.** De acuerdo con la Encuesta de Calidad de Vida (ECV) del Departamento Administrativo Nacional de Estadística (DANE) de 2023 (ECV-DANE 2023), si bien en 2023 el 63,9% de los hogares poseía el servicio de acceso a Internet para el total nacional, que representa un avance con respecto al porcentaje de hogares de 2022 (59,5%), aún persiste una diferencia importante en el acceso a este servicio entre los hogares de las cabeceras municipales y los centros poblados y rural disperso. Para el año 2023, esta diferencia era de aproximadamente 29 puntos porcentuales. La conexión a Internet fijo registró mayor proporción de hogares en las cabeceras

municipales 55,1%, mientras que la conexión a Internet móvil registró una mayor proporción de hogares en los centros poblados y rural disperso (33,2%) (*Ver Gráfico 1*).

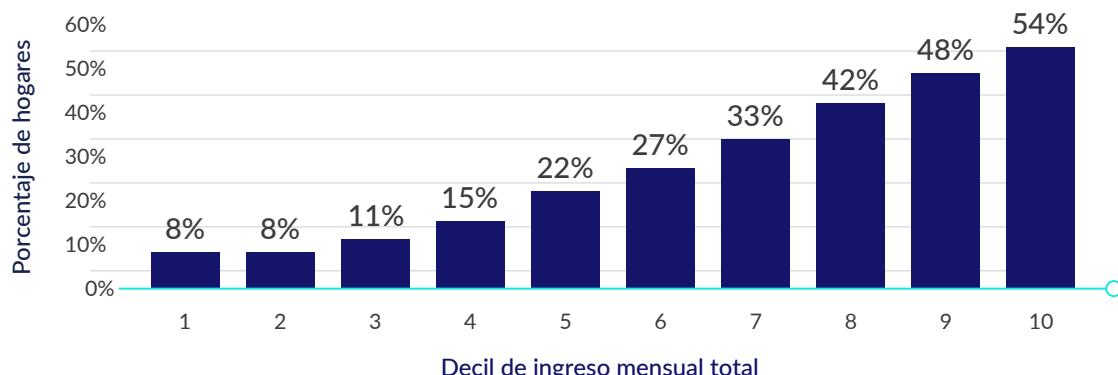
De igual forma, **los hogares de menores ingresos tienen dificultades para acceder a servicios de Internet en Colombia.** De acuerdo con (DNP, 2024), el 92% de los hogares más pobres (primer y segundo decil de ingresos) no tienen el servicio de acceso fijo a Internet, mientras que los hogares con los ingresos más altos, por ejemplo, en los hogares en el décimo decil de ingresos este porcentaje no alcanza el 50% (*Ver Gráfico 2*). Según (DANE, 2024), el costo de servicio es la principal razón por la cual los hogares no tienen acceso al servicio de Internet.

Gráfico 1. Proporción de hogares que poseen el servicio de acceso a Internet según tipo de conexión en cualquier lugar (2023)



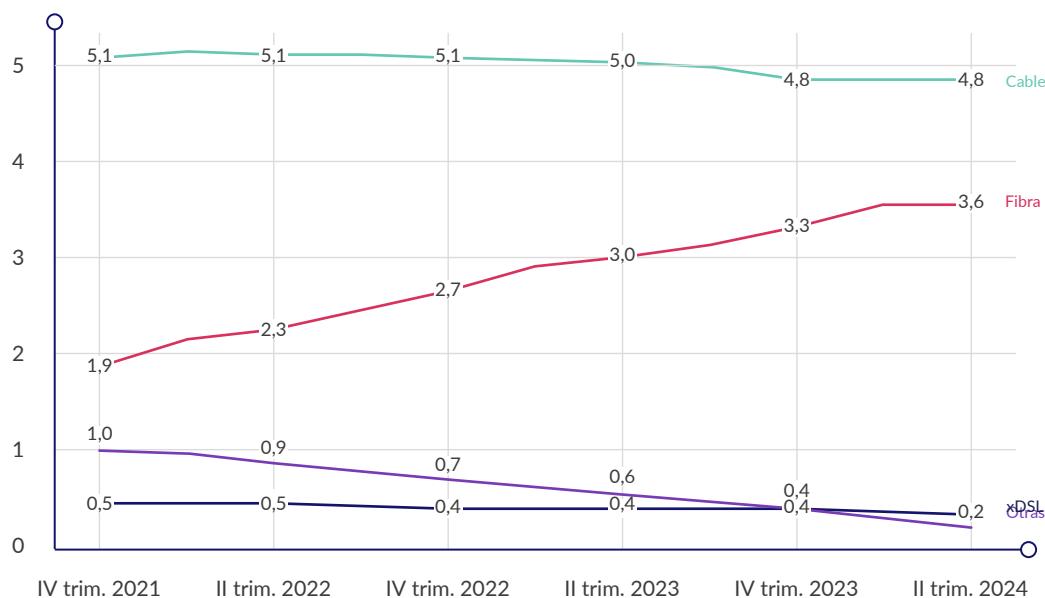
Fuente: Elaboración propia a partir de (DANE, 2024)

Gráfico 2. Porcentaje promedio de hogares que demandan Internet fijo (solo o empaquetado) desagregados por decil de ingreso (2023)



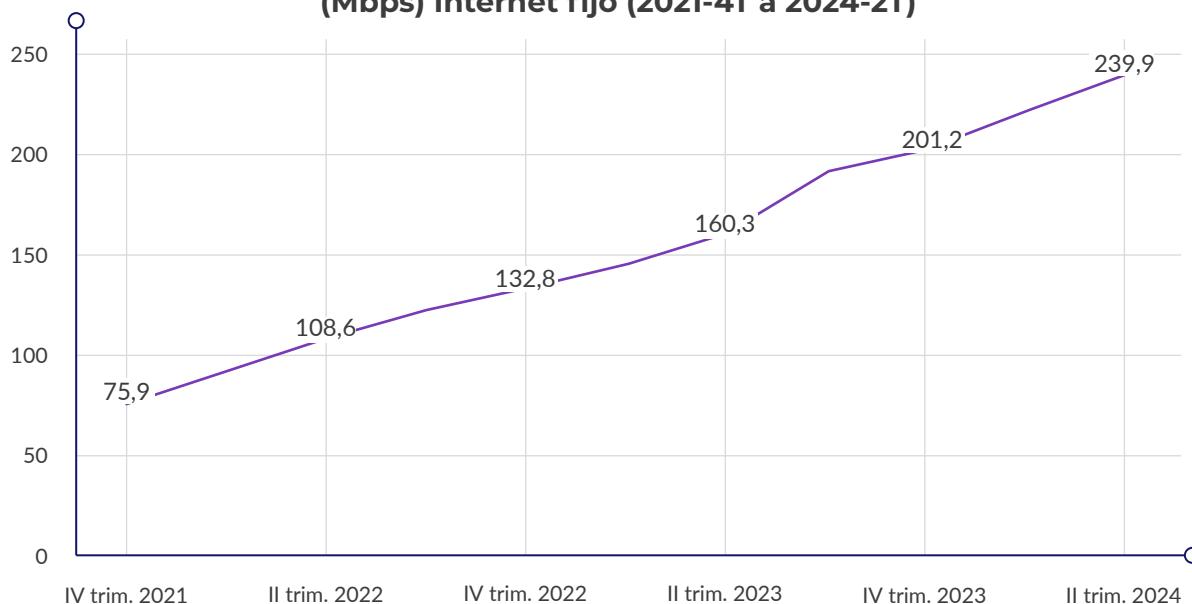
Fuente: Extraído de (DNP, 2024). Página 36.

Con respecto a la tecnología utilizada para la prestación del servicio de Internet, es relevante mencionar que **Colombia ha estado migrando, tanto en el servicio fijo como móvil, hacia tecnologías que permiten unas mayores velocidades de descarga y carga, pero aún existen oportunidades de mejora**. De acuerdo con el Boletín TIC del Ministerio de Tecnologías de la Información y las Comunicaciones para el segundo trimestre de 2024 (Boletín TIC MinTIC 2024-2T), en el caso de Internet fijo, el despliegue de fibra óptica se ha intensificado en el país y esta tecnología, con un total de 1,9 millones de accesos, pasó de representar el 22,4% del total de los accesos a Internet fijo en el cuarto trimestre de 2021 (2021-4T) al 40,0% en el segundo trimestre de 2024 (2024-2T) con un total de 3,6 millones de accesos ([Ver Gráfico 3](#)).

Gráfico 3. Accesos fijos a Internet por tipo de tecnología (millones) (2021-4T a 2024-2T)

Fuente: Extraído de (MinTIC, 2024). Página 15.

Este mayor despliegue de fibra óptica se ha visto reflejado en el crecimiento sostenido de la velocidad de descarga que han experimentado los suscriptores del servicio de Internet fijo en el país en los últimos años. De acuerdo con el Boletín TIC MinTIC 2024-2T, para el segundo trimestre de 2024 la velocidad de descarga promedio para el total nacional era de 239,9 Megabits por segundo (Mbps), que representa un crecimiento del 216% con respecto al cuarto trimestre de 2021 ([Ver Gráfico 4](#)). Este crecimiento se ha experimentado tanto hogares como empresas, para el segundo trimestre de 2024 la velocidad de descarga promedio era de 236,9 Mbps para hogares y de 273,1 Mbps para empresas. Sin embargo, es relevante mencionar que estas altas velocidades aún no se registran en los hogares de bajos ingresos, como los hogares del Estrato 1, ni tampoco aquellos ubicados en las zonas rurales o apartadas del país.

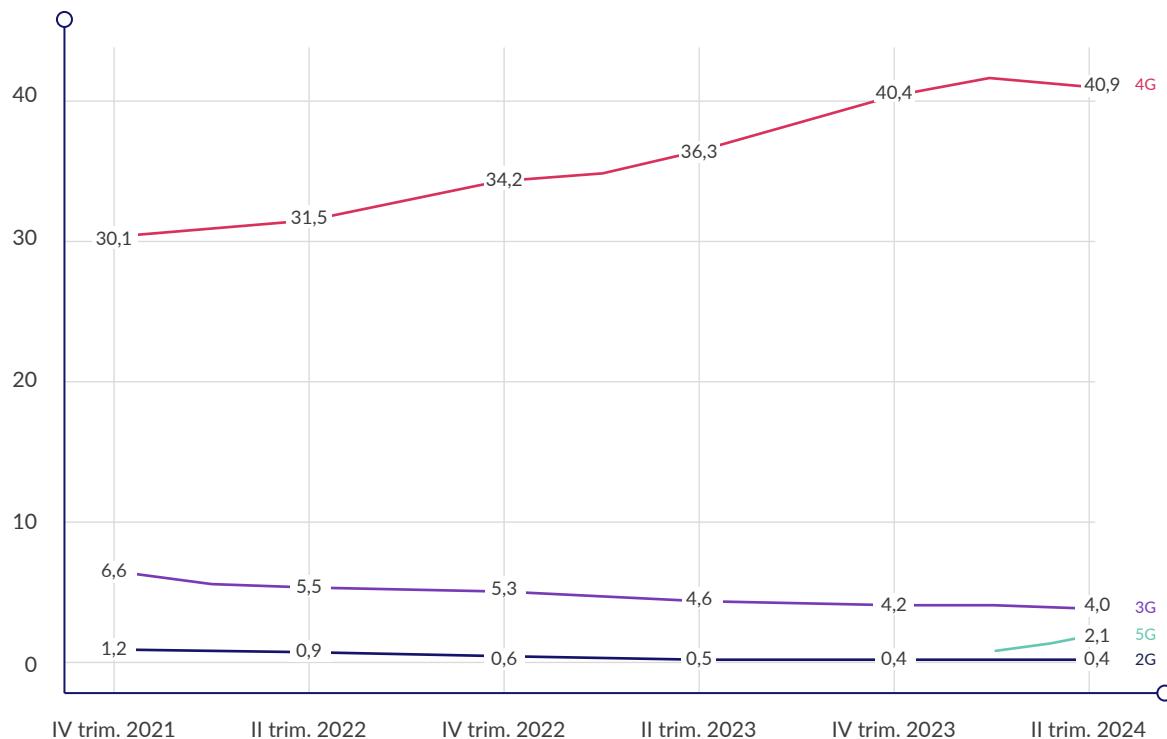
Gráfico 4. Velocidad de descarga promedio nacional (Mbps) Internet fijo (2021-4T a 2024-2T)

Fuente: Extraído de (MinTIC, 2024). Página 12.

Nota: El valor promedio de descarga incluye los segmentos Residencial, Corporativo y no estratificado.

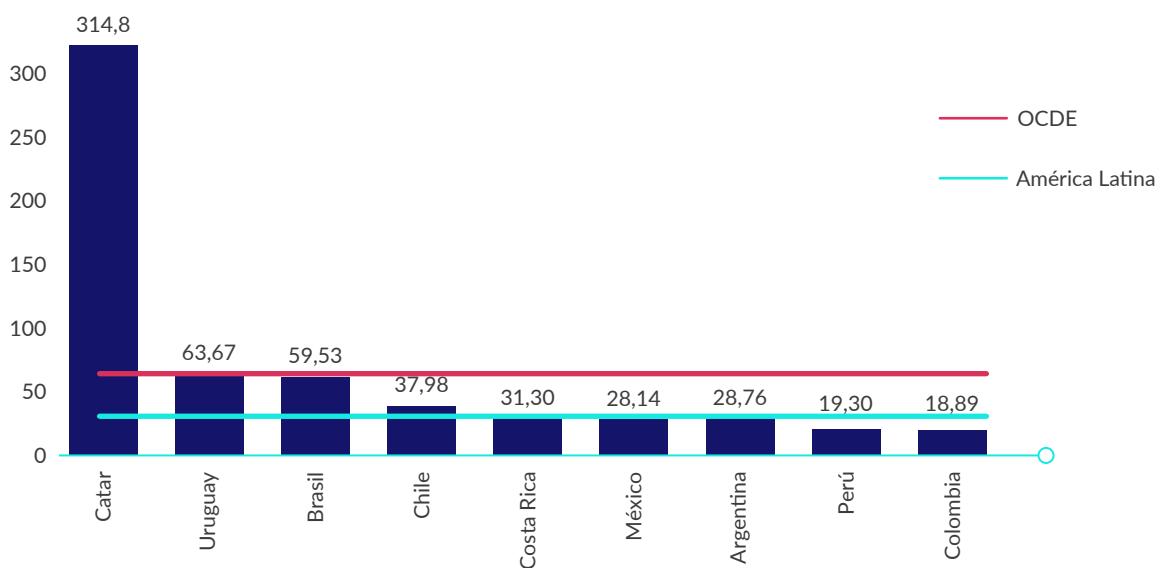
Con respecto a Internet móvil, la tecnología 4G se ha consolidado como la principal tecnología de acceso en el país. Aunque ya se tienen accesos con tecnología 5G, estos aún son muy pocos. Según el Boletín TIC MinTIC 2024-2T, para el segundo trimestre de 2024 la tecnología 4G, con 40,9 millones de accesos, representaba el 86,1% de los accesos de Internet móvil. Adicionalmente, para este trimestre el país registró los primeros accesos con tecnología 5G, que alcanzaron los 2,1 millones y representan el 4,4% del total de accesos a Internet móvil ([Ver Gráfico 5](#)).

Gráfico 5. Accesos a Internet móvil por tipo de tecnología (millones) (2021-4T a 2024-2T)



Fuente: Extraido de (MinTIC, 2024). Página 23.

Gráfico 6. Velocidad promedio de descarga (Mbps) Internet móvil. Colombia y países de referencia (abril de 2024)



Fuente: Extraído de (CPC, 2024) . Página 200.

A pesar de estos avances, **el despliegue tardío en el país de la tecnología 5G, con respecto a países líderes, ha llevado a que Colombia esté rezagada en cuanto a la velocidad de descarga de Internet móvil.** Como se observa en el **Gráfico 6**, el promedio de la velocidad de descarga de Internet móvil en el país está por debajo del promedio de América Latina y de los países miembros de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

De igual manera, es relevante señalar la expedición del **Plan Integral de Expansión de Conectividad Digital** expedido por el MinTIC en diciembre de 2024. Este gira en torno a cuatro objetivos principales:

1 El cierre de la brecha digital

A través de la conectividad en comunidades rurales y urbanas desconectadas

2 Transformación social

Utilizando la **conectividad como una herramienta para promover al acceso a educación y salud, así como aumentar la productividad en sectores vulnerables de la población**

3 Implementación de infraestructura avanzada

Con tecnologías como redes de fibra óptica, conectividad satelital y 5G para cubrir el **98%** de los hogares colombianos en 2033

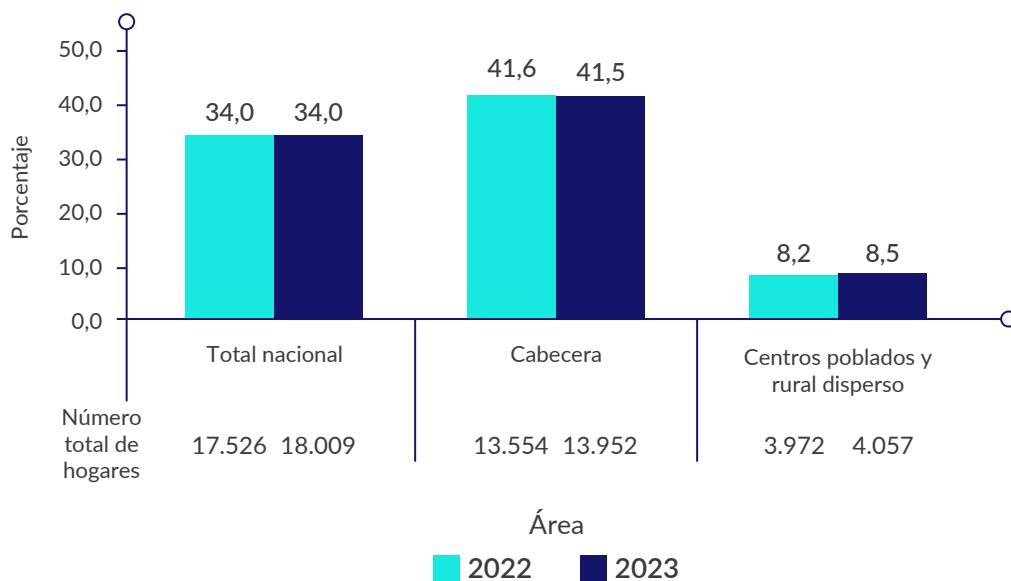
4 Fomentar la inclusión digital

A través del uso y apropiación de las TIC, cerrando la brecha urbana-rural. A través de estos planteamientos, el MinTIC busca cerrar definitivamente la brecha digital y atender las dificultades señaladas a lo largo de este numeral

2.1.2 Dispositivos para la conectividad digital

En Colombia un número bajo de hogares posee un computador o tableta, especialmente en las zonas rurales. De acuerdo con la ECV-DANE 2023, para el año 2023 solo el 34,0% de los hogares en el país poseía computador de escritorio, portátil o tableta. En las cabeceras municipales este porcentaje fue de 41,5%, mientras que en los centros poblados y rural disperso fue de 8,5%. Estos porcentajes fueron similares a los registrados en 2022 (*Ver Gráfico 7*). Cuando se indaga sobre las razones por las cuales los hogares no se poseen alguno de estos dispositivos, se encuentra que la razón principal fue su costo con 58,0 % para el total nacional, seguido por la falta de interés en adquirirlo con 27,0% y el desconocimiento en el uso con 13,9% (DANE, 2024).

Gráfico 7. Proporción de hogares que poseen computador de escritorio, portátil o tableta (2022 y 2023)

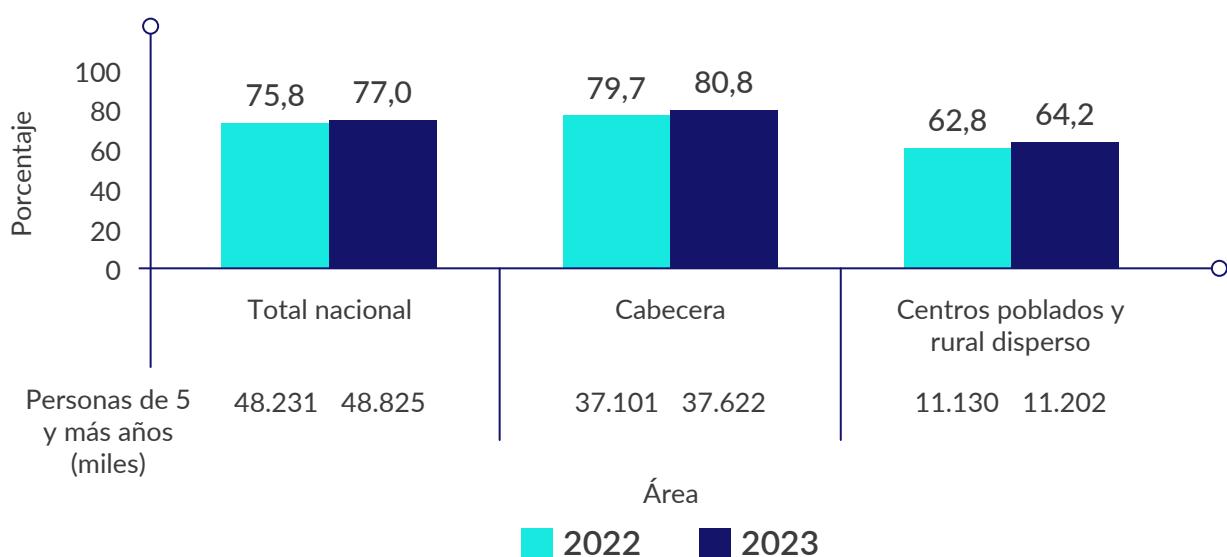


Fuente: Extraído de (DANE, 2024). Página 11.

Cada vez son más los colombianos que tienen un teléfono celular inteligente. Los resultados con respecto a tenencia de computador o tableta contrastan con la tenencia de teléfono celular. Según la ECV-DANE 2023, para el año 2023 el 77,0% de las personas de 5 y más años reportaron poseer teléfono celular, 80,8% en cabeceras y 64,2% en centros poblados y rural disperso. Estos porcentajes representan incrementos con respecto al año 2022, principalmente, en los centros poblados y rural disperso donde aún existe un porcentaje importante de personas sin uno de estos dispositivos (*Ver Gráfico 8*).

Respecto al tipo de celular, la ECV-DANE 2023 encontró que, del total nacional de las personas de 5 y más años que tenían teléfono celular, el 90,3% reportaron poseer teléfono celular inteligente (smartphone), este porcentaje fue de 80,8% en cabeceras y 64,2 % en centros poblados y rural disperso. No obstante, existen oportunidades de mejora con respecto a la asequibilidad de estos teléfonos. Según el Índice Latinoamericano de Inteligencia Artificial (ILIA) 2024 del Centro Nacional de Inteligencia Artificial de Chile (Cenia), el precio promedio de un smartphone en Colombia es más alto que el promedio de América Latina y el Caribe (ALC).

Gráfico 8. Proporción de personas de 5 y más años que poseen teléfono celular (2022 y 2023)



Fuente: Extraída de (DANE, 2024). Página 8.

2.1.3 Infraestructura de cómputo

El país cuenta con una baja capacidad cómputo que limita sus procesos de transformación digital. De acuerdo con el ILIA 2024, con un puntaje de 16,33 puntos de 100 posibles, Colombia registra un nivel menor a la media regional de ALC (21,76 puntos) en cuanto a capacidad de cómputo, para lo cual se consideran aspectos como servicios de nube, capacidad de infraestructuras de computación de alto rendimiento (HPC por sus siglas en inglés)³, centros de datos certificados, entre otros elementos. Estos resultados evidencian que ALC en general tiene limitaciones importantes en cuanto a las capacidades de las infraestructuras de cómputo.

³ De acuerdo con el ILIA 2024, esto hace referencia al acceso a máquinas capaces de procesar una gran cantidad de datos y de realizar cálculos intensivos para resolver problemas complejos en ciencia, ingeniería y negocios, es esencial para el desarrollo de la IA y el desarrollo tecnológico general, ya que sus aplicaciones son transversales a cualquier disciplina.



Como se muestra en el **Gráfico 9**, según el ILIA 2024, en cuanto a los servicios de Nube Colombia registra un puntaje de 35,00 puntos, que si bien es similar al de la región de ALC puede considerarse de bajo a moderado si se tiene en cuenta que son 100 los puntos posibles. De acuerdo con el GDI 2024, en el país la inversión en servicios de la nube es aún bajo y hay oportunidades de mejora en cuanto a la migración de las organizaciones a los servicios de Nube.

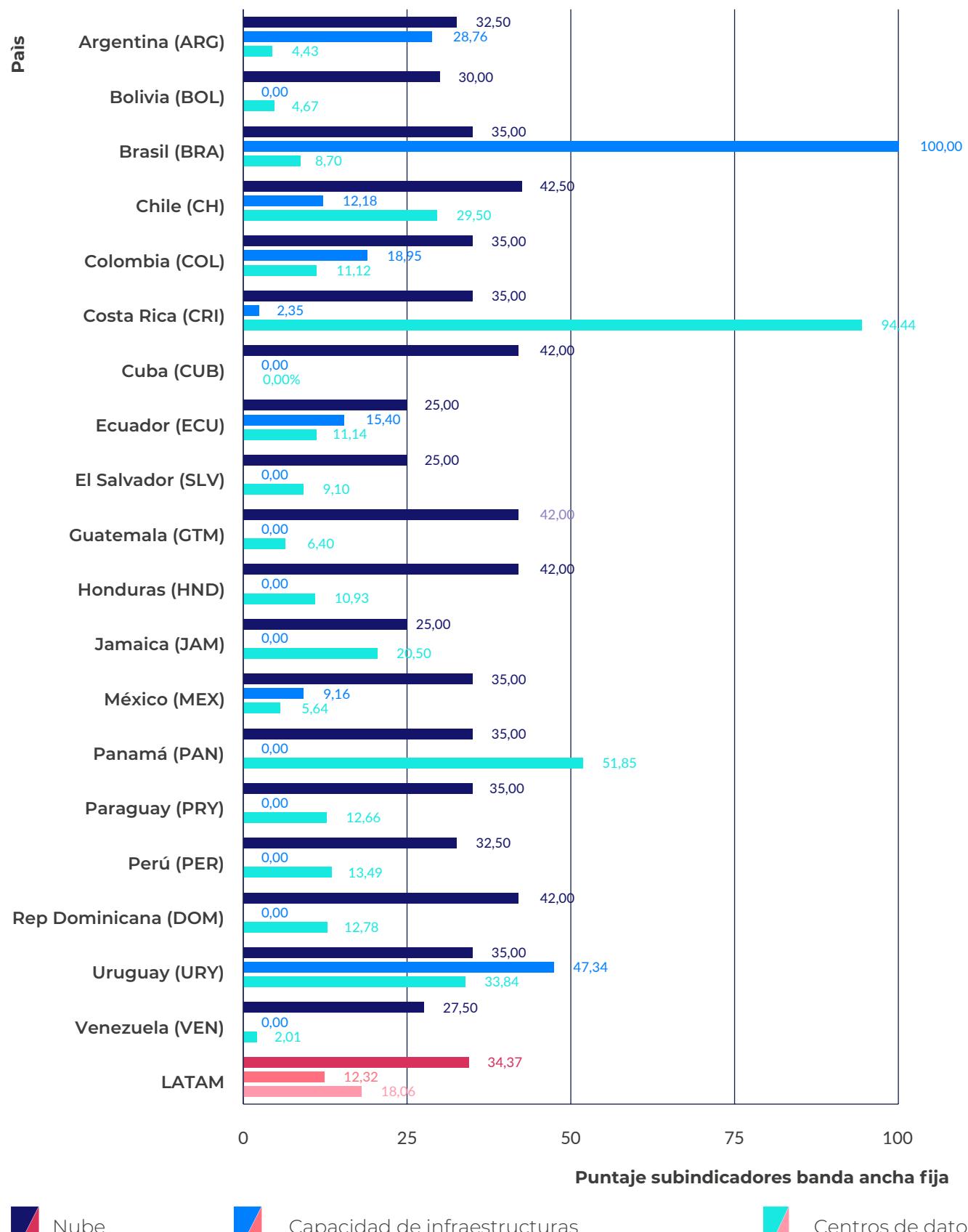
Con respecto a la capacidad de infraestructuras de computación de alto rendimiento, según ILIA 2024, Colombia supera levemente el promedio regional de ALC (12,32 puntos). Actualmente, el país tiene 11 infraestructuras que soportan un tipo de cómputo intensivo, el cual es medido en Teraflops (Tflops)⁴. Estas infraestructuras que están distribuidas en nueve organizaciones suman una capacidad total de 5076,496282 Tflops (**Ver Tabla 3**). Sin embargo, el país está detrás de países como Brasil, que tiene infraestructuras reconocidas a nivel mundial en términos de capacidad.

Asimismo, el país tiene un desafío en cuanto a desarrollar centros de datos certificados. De acuerdo con ILIA 2024, Colombia tiene un bajo puntaje (11,12 puntos) en comparación con el promedio regional de ALC (18,06 puntos). Mientras Costa Rica y Panamá, que lideran en la región este tipo de infraestructura tienen respectivamente una tasa de 3,2 y 1,7 centros de datos verificados por cada millón de habitantes, en Colombia esta tasa es de 0,3.



⁴ Un Teraflop (Tflop) es una unidad de medida que indica la potencia de cálculo de un ordenador o un GPU (Graphics Processing Unit) en función del número de operaciones de coma flotante (FLOPS) que puede realizar por segundo. Un TFLOP equivale a 1 billón de FLOPS.

Gráfico 9. Puntaje subindicadores de Nube/Capacidad de infraestructuras de HPC/ Centros de datos certificados del ILIA 2024



Fuente: Extraído de (Cenia, 2024). Página 63.

Tabla 3. Capacidad de infraestructuras de computación de alto rendimiento de Colombia

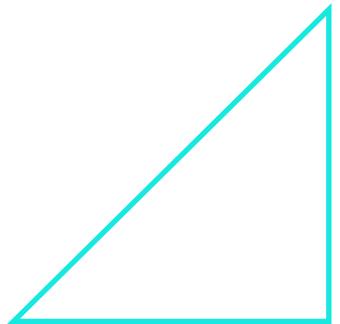
Institución	Fabricante	Theoretical Tflops
Fuerza Aérea Colombiana	HPE Cray	52
Policía Nacional de Colombia	HPE Cray	920
Seguridad Nacional de Colombia	HPE Cray	1569,6
Universidad de Ibagué	HPE Cray	1024
Telco Colombia	HPE Cray	1024
Universidad de Cartagena	HPE	36,6125
Universidad de los Andes Colombia	DELL	30,2984375
SC3UIS	HPE	133,3748444
	DELL Supermicro	92,6
BIOS	HPE	6,9
	Inspur	187,1105

Fuente: Elaboración propia a partir de (Cenia, 2024).



2.2

Datos



Colombia se destaca por tener un ecosistema avanzado de datos.

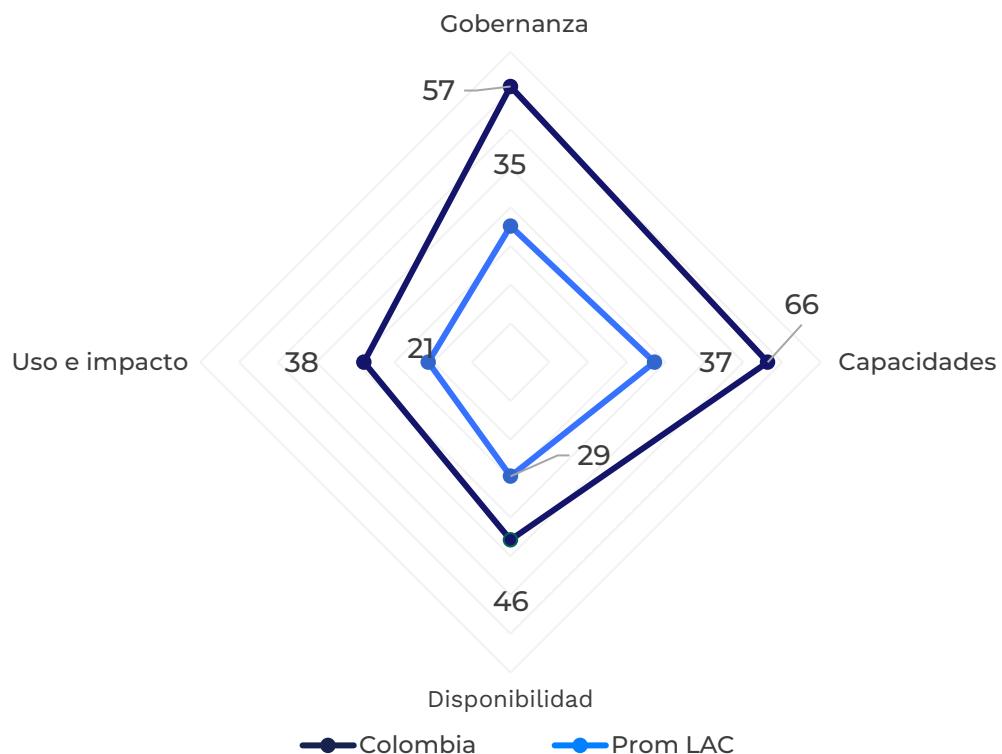
De acuerdo con el Global Data Barometer (GDB) de 2022, que proporciona una medición sobre los avances de los países con respecto al gobierno, uso y aprovechamiento de los datos para el bien público, Colombia, con un puntaje general de 54 puntos, obtuvo el tercer mejor resultado en la región de América Latina y el Caribe, y se ubicó en el puesto 17 con respecto a los 109 países considerados. Estos resultados ubican al país entre los de alto desempeño y lo posicionan como uno de los líderes de la región.

Al observar los resultados del país en cada uno de los pilares del índice (gobernanza, capacidad, disponibilidad de datos, y uso e impacto)⁵ ([Ver Gráfico 10](#)), se encuentra que Colombia obtuvo un desempeño superior al promedio de la región de ALC

en todos los pilares, principalmente, en los pilares de capacidades (66 puntos) y gobernanza (57 puntos), en los cuales supera el promedio regional en más de 20 puntos y se resaltan los avances del país en la manera de recopilar, descargar, procesar, usar y compartir los datos, así como en el marco normativo y de políticas públicas orientadas a garantizar el derecho a la información, el acceso a datos fiables, completos y transparentes, y la protección de los datos personales. En ese sentido, de acuerdo con (DNP, 2022), se destacan iniciativas como el marco de interoperabilidad de la Política de Gobierno Digital, la Ley 1581 de 2012 sobre protección de datos personales, y la Ley 1712 de 2014 sobre transparencia y derecho de acceso a información pública.

⁵ El índice se construye sobre cuatro pilares: i) *Gobernanza*: analiza las políticas existentes para permitir un ecosistema de datos públicos digno de confianza; ii) *Capacidad*: mapea las capacidades de los gobiernos, la sociedad civil y el sector privado para recopilar, gestionar, compartir y utilizar los datos.; iii) *Disponibilidad de los datos*: evalúa la disponibilidad, la apertura y las características de una amplia gama de conjuntos de datos públicos, tratando de comprender el estado de los datos nacionales y subnacionales; y iv) *Uso e impacto*: identifica hasta qué punto se utilizan los datos para proporcionar bienes sociales, hacer frente a grandes retos y afrontar riesgos.

Gráfico 10. Desempeño de Colombia versus el promedio de América Latina y el Caribe en los pilares del GDB (2022)



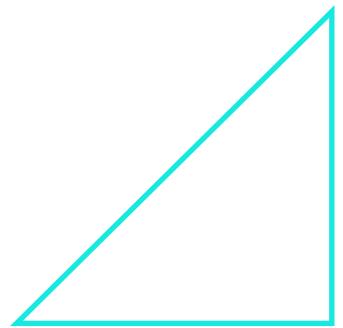
Fuente: Extraído de (DNP, 2022). Página 5.

Aunque en las otras dos dimensiones (Disponibilidad y Uso e impacto) el país también registró un puntaje superior al promedio de la región de ALC, la diferencia fue menor (17 puntos), evidenciando una oportunidad de mejora en estas dimensiones. Según (DNP, 2024), en Colombia aún existe una baja disponibilidad de datos de calidad, entre ellos, los datos geoespaciales, y las entidades públicas, especialmente las del orden subnacional, no están aprovechando los datos para la toma de decisiones. Según el Índice de Gobierno Digital de MinTIC de 2023, las entidades del orden nacional obtuvieron en promedio 68,0 de 100 puntos en el componente de **“Toma de decisiones basadas en datos”**, mientras que las entidades del orden subnacional obtuvieron en promedio 29,8 de 100 puntos.



2.3

Habilidades digitales



Aunque el número de usuarios de Internet sigue creciendo en el país, aún existe un porcentaje importante de personas que no lo son porque no saben usarlo. De acuerdo con la ECV-DANE 2023, para el total nacional, el 77,3% de las personas de 5 y más años utilizó Internet en el año 2023, lo cual representó un incremento de 4,5 puntos porcentuales con respecto al 2022. Para aquellas que usaron Internet la principal actividad fue redes sociales (82,8%), seguido de enviar y recibir correos (49,5%). Para las personas que indicaron no usar Internet, la principal razón para no hacerlo fue el no saber usarlo (40,1%), seguido por no considerarlo necesario (24,8%).



Tabla 4. Proporción de personas de 5 y más años que usaron computador* o Internet, según el tipo de habilidad 2023

Habilidades en el uso del computador	Total	Cabecera	Centros Poblados y Rural Disperso
Usar procesadores de texto (Word, Google Docs, etc.)	52,6	55,9	37,2
Usar las funciones de copiar y pegar para duplicar o mover información entre documentos	48,5	52,2	31,1
Enviar correos electrónicos con archivos adjuntos (documentos, fotos, videos, etc.)	54,2	58,3	35,1
Conectar o instalar dispositivos adicionales (ej. impresora, módem, cámara, etc.)	35,1	38,9	17,8
Usar fórmulas matemáticas básicas en una hoja de cálculo (Excel, Open office calc, etc.)	30,8	34,3	14,2
Crear presentaciones mediante un programa especializado para ello (Powerpoint, Prezi, otros)	31,3	34,8	15,3
Transferir archivos entre computadores y otros dispositivos (USB, celular, etc.)	36,8	39,8	22,8
Descargar o instalar programas computacionales (software)	25,2	28,1	11,8
Utilizar un lenguaje de programación especializado	9,3	10,7	3,1
Implementar medidas de seguridad efectivas para proteger dispositivos y cuentas de Internet (contraseñas fuertes, notificación de intento de conexión, etc.)	20,7	23,4	8,1
Limitar la difusión de datos o información personal en dispositivos, cuentas o aplicaciones de Internet (nombre, información de contacto, fotografías, etc.)	20,5	23,3	8,0
Comprobar que las noticias o información que consulta o recibe a través de Internet son ciertas o verdaderas	24,6	27,4	11,6

Fuente: Elaboración propia a partir de (DANE, 2024)

Nota 1: Una persona puede tener varias habilidades, por lo que las opciones de respuesta no son excluyentes.

Nota 2: La base de cálculo es el total de personas que usaron computador o Internet en cada una de las coberturas que se presentan.

*La definición de computador comprende el de escritorio, portátil o tableta.



En Colombia se debe continuar promoviendo el desarrollo de habilidades digitales, especialmente las intermedias y avanzadas⁶. Según la ECV-DANE 2023, los mayores avances en el país con respecto a las habilidades digitales están asociadas a las habilidades básicas. En el año 2023, para el total nacional, la habilidad con mayor porcentaje registrado en las personas de 5 y más años que usaron computador o Internet fue enviar correos electrónicos con archivos adjuntos con 54,2%. Le siguieron, en orden de importancia, la habilidad de usar procesadores de texto (52,6%) y usar las funciones de copiar y pegar para duplicar o mover información entre documentos, dispositivos o a través de Internet (48,5 %).

Aunque estas habilidades todavía tienen oportunidades de mejora, en el caso de las habilidades intermedias y avanzadas se registraron porcentajes menores, que resaltan la importancia de un mayor énfasis en el desarrollo de este tipo de habilidades. Por ejemplo, la habilidad intermedia de usar fórmulas matemáticas básicas en una hoja de cálculo tiene un porcentaje de 30,8% y la habilidad avanzada de utilizar un lenguaje de programación especializado el porcentaje es de 9,3% ([Ver Tabla 4](#)). De hecho, esta última habilidad, que es significativa para el desarrollo y adopción de tecnologías emergentes como la IA, es la que tiene el menor porcentaje de todas las habilidades consideradas.

⁶ Estas habilidades hacen referencia a actividades como: Copiar o mover un archivo o carpeta; Utilizar las herramientas de copiar y pegar para duplicar o mover información dentro de un documento; Envío de correos electrónicos con archivos adjuntos (por ejemplo, documentos, imágenes, videos); Transferir archivos entre un ordenador y otros dispositivos (Habilidades digitales básicas); Utilizar fórmulas aritméticas básicas en una hoja de cálculo; Conectar e instalar nuevos dispositivos (por ejemplo, un módem, una cámara o una impresora); Buscar, descargar, instalar y configurar programas informáticos; Crear presentaciones electrónicas con software de presentación (incluyendo imágenes, sonido, video o gráficos) (Habilidades digitales intermedias); Programación informática, desarrollo de software, ciencia de datos y gestión de redes (Habilidades digitales avanzadas). Construido teniendo en cuenta información de (UIT, 2020)



Políticas Digitales **Transversales**





3.0

Políticas digitales transversales

3.1 Estrategia Nacional Digital

En el mes de febrero de 2024, el Gobierno nacional de Colombia lanzó la Estrategia Nacional Digital (END) 2023-2026, que se define como “(...) el instrumento que contiene y coordina todas las iniciativas de política pública del Gobierno nacional relacionadas con conectividad y transformación digital para los próximos años, proporcionando la visión de Colombia con respecto al acceso, uso y apropiación de los datos y las tecnologías digitales.” (DNP, 2024, pág. 2)

Esta estrategia fue construida por la Presidencia de la República, el Departamento Nacional de Planeación (DNP) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y parte de lo dispuesto en el Plan Nacional de Desarrollo (PND) 2022-2026 “Colombia, Potencia Mundial de Vida”⁷. Este destaca la conectividad y la transformación digital como elementos clave, en los que se debe avanzar para lograr los objetivos de política pública del Gobierno Nacional en materia de transformación y cierre de la brecha digital.

⁷ El PND 2022 – 2026 propone acciones teniendo como punto de partida el territorio y las personas. En concreto, el PND 2022 – 2026 está conformado por cinco transformaciones: i) Ordenamiento del territorio alrededor del agua; ii) Seguridad humana y justicia social; iii) Derecho humano a la alimentación; iv) Transformación productiva, internacionalización y acción climática; v) Convergencia regional. Con estas transformaciones se busca orientar la economía hacia la promoción de un desarrollo económico, social y ambiental. En cada una de estas, se consideran a los datos y las tecnologías digitales como un aspecto importante, por lo cual, las acciones relacionadas con conectividad y transformación digital están distribuidas en todo el PND. La END 2023-2026 recoge y complementa estas acciones.



La **END 2023-2026** es la primera estrategia de este tipo en el país. Si bien el Gobierno de Colombia anteriormente había definido instrumentos de política pública para impulsar el acceso y apropiación de las tecnologías digitales en el país, estos correspondían principalmente a los planes sectoriales de MinTIC. A diferencia de esto, la **END 2023-2026** aborda no solo las iniciativas que está implementando el MinTIC, sino también aquellas que están desarrollando las otras entidades del Gobierno nacional para impulsar la transformación digital de sus sectores.

En este sentido, de acuerdo con lo indicado por (DNP, 2024), con esta estrategia se espera evidenciar de una mejor manera las **prioridades con respecto a los datos y las tecnologías digitales** en el país y tener un entendimiento holístico de la transformación digital, con un enfoque integral de todo el Gobierno que facilite la articulación y coordinación institucional, así como realizar seguimiento y tomar medidas con respecto a la implementación de las iniciativas de política pública propuestas. También se espera facilitar la conversación con los diferentes actores a nivel nacional e internacional para impulsar las **apuestas estratégicas del país alrededor de la transformación digital**.

Concretamente, la END 2023-2026 plantea como principal objetivo “*desencadenar el potencial de la transformación digital para superar los desafíos que enfrenta Colombia a nivel económico, social y ambiental, a través del fortalecimiento de sus elementos habilitadores y un impulso decidido al uso y apropiación de los datos y las tecnologías digitales por parte de las personas y los hogares, las entidades públicas, y el sector productivo, abordando los retos, riesgos y daños potenciales que traen consigo la aceleración de la digitalización.*” (DNP, 2024, pág. 3)

Para el cumplimiento de este gran objetivo la estrategia define ocho ejes (**Ver Figura 1**), para los cuales a su vez plantea un objetivo, que está acompañado de líneas estratégicas y acciones concretas. En la **Tabla 5** se resumen los ejes, objetivos y líneas estratégicas de la END 2023 – 2026 para Colombia, que se desarrollarán a través de 95 acciones a cargo de diferentes entidades del Gobierno nacional.

Figura 1. Ejes de la Estrategia Nacional Digital de Colombia 2023-2026

Fuente: Extraído de (DNP, 2024). Página 3.

Adicionalmente, según DNP (2024), con el propósito de implementar exitosamente la END, se definirá un esquema o modelo de gobernanza que facilite la articulación y coordinación interinstitucional, así como el seguimiento del desarrollo de estas iniciativas y apoye la toma de decisiones en materia de transformación digital en el país. Este esquema también definirá los mecanismos de articulación y participación de otros actores como los entes territoriales, el sector privado, la academia, la sociedad civil y los aliados internacionales.

Tabla 5. Ejes, objetivos y líneas estratégicas de la END 2023-2026

EJES	OBJETIVOS	LÍNEAS ESTRATÉGICAS
Conectividad digital para cambiar vidas	Conectar a los habitantes de Colombia, reconociendo el acceso y uso de las TIC como un derecho y no un privilegio, especialmente en las zonas que no cuentan con estos servicios o que requieren mejorar la cobertura y calidad de estos, para contribuir a la generación de oportunidades, riqueza, igualdad y productividad en el país.	<ul style="list-style-type: none"> Impulsar el despliegue de redes de comunicaciones como generador de oportunidades, riqueza, igualdad y productividad. Promover la asignación y uso eficiente del espectro radioeléctrico para maximizar el bienestar social. Fomentar la masificación de las TIC para contribuir al cierre de la brecha urbano-rural. Fortalecer los servicios de televisión y radiodifusión sonora para la inclusión social.
Acceso, uso y aprovechamiento de datos para impulsar la transformación social	Desarrollar en el país una infraestructura de datos sólida, segura y de calidad que permita aumentar la disponibilidad, uso e intercambio de datos, mejorar la toma de decisiones y consolidar una cultura de datos en el país.	<ul style="list-style-type: none"> Garantizar y aumentar la disponibilidad de datos básicos de calidad en el país. Impulsar la adopción de la interoperabilidad como bien público digital. Promover y aumentar la reutilización y transmisión segura de información.
Seguridad y confianza digital para la garantía de las libertades y el desarrollo integral de las personas	Generar las capacidades necesarias para fomentar la protección de las libertades, la dignidad y el desarrollo integral de todos los colombianos frente a las posibles amenazas y riesgos que puedan surgir en el entorno digital.	<ul style="list-style-type: none"> Fortalecer la planificación, coordinación y articulación del país en materia de seguridad digital. Fomentar la preparación y la resiliencia del país en el entorno digital. Proteger y fortalecer a las personas, las infraestructuras digitales, y las entidades del Estado para garantizar la prestación de sus servicios en el entorno digital. Desarrollar una legislación nacional para un ecosistema digital seguro y confiable.

EJES	OBJETIVOS	LÍNEAS ESTRATÉGICAS
Habilidades y talento digital como motor de oportunidades	<p>Fortalecer las habilidades y el talento digital de la población colombiana con el fin de promover la creación de oportunidades y el desarrollo de capacidades que potencien su desempeño en los ámbitos educativo, social y productivo.</p>	<p>Acelerar los procesos de alfabetización y apropiación digital para desarrollar la sociedad del conocimiento y la tecnología.</p> <p>Incrementar el talento digital como factor clave en la productividad laboral y la empleabilidad de las personas.</p> <p>Impulsar el acceso y uso de las tecnologías digitales en el sistema educativo.</p>
IA y otras tecnologías emergentes para la generación de valor económico y social	<p>Generar oportunidades de aprovechamiento, implementación y democratización de la IA y otras tecnologías digitales emergentes para crear valor económico y social, teniendo como referencia principios éticos, gestión de riesgos de estas tecnologías y la protección de los derechos humanos.</p>	<p>Diseñar y fortalecer iniciativas de política pública para el desarrollo de la IA y otras tecnologías digitales emergentes.</p>
Transformación digital pública para fortalecer el vínculo Estado - Ciudadanía	<p>Fortalecer el vínculo Estado - Ciudadanía, haciéndolo más eficiente, humano y oportuno, para dar respuesta a las necesidades de la población y la resolución de problemas sociales a través del uso de tecnologías digitales, el aprovechamiento de datos, y el desarrollo innovador de servicios centrados en el ciudadano.</p>	<p>Fortalecer el Gobierno Digital del país para tener una relación eficiente entre el Estado y el ciudadano.</p> <p>Impulsar la innovación pública para una mejor respuesta a las necesidades de los ciudadanos.</p> <p>Desarrollar una justicia digital eficiente e incluyente para el bienestar de las personas en los territorios.</p>
Economía digital para la transformación productiva	<p>Impulsar el uso y la adopción de las tecnologías digitales para una transformación productiva del país que cierre brechas tecnológicas, fortalezca los encadenamientos productivos, diversifique la oferta interna y exportable, y permita pasar de una economía extractivista hacia una economía del conocimiento, incluyente y sostenible.</p>	<p>Impulsar la utilización y aprovechamiento de las tecnologías digitales en los sectores productivos del país.</p> <p>Fortalecer la industria digital para habilitar la adopción de tecnologías en el sector productivo e impulsar el desarrollo de contenidos digitales.</p> <p>Impulsar el emprendimiento digital, la innovación y el desarrollo de procesos de transformación digital como instrumentos para la generación de empleo y el crecimiento económico del país.</p> <p>Abordar los desafíos alrededor de las nuevas formas de trabajo generadas por las tecnologías digitales.</p>
Sociedad digital para un desarrollo inclusivo, equitativo, y sostenible	<p>Promover una sociedad que ubique a las personas y su bienestar como el centro del desarrollo digital, mediante el uso inclusivo y equitativo de las tecnologías digitales, la protección de los derechos de las personas en el entorno digital, y el aprovechamiento de los datos para hacer frente a los desafíos sociales y ambientales.</p>	<p>Promover un uso inclusivo y equitativo de las tecnologías digitales para disminuir las desigualdades sociales.</p> <p>Abordar los desafíos y riesgos asociados a la desinformación y el contenido falso en línea.</p> <p>Impulsar el uso de tecnologías digitales y el aprovechamiento de datos para responder a los desafíos sociales y ambientales.</p> <p>Promover el desarrollo de las ciudades y los territorios inteligentes.</p> <p>Impulsar el sector espacial para el desarrollo social y económico.</p>

Fuente: Elaboración propia a partir de (DNP, 2024).

La END 2023-2026 también plantea una serie de indicadores y metas que el Gobierno nacional buscará alcanzar al año 2026 con su implementación. Estos indicadores y metas corresponden a lo definido en el PND 2022 – 2026 para los aspectos relacionados con datos y tecnologías digitales. En la **Tabla 6** se destacan ocho de los trece indicadores definidos, indicando la línea base y la meta que se quiere alcanzar.

Tabla 6. Indicadores y metas estratégicas END 2023-2026

Indicador	Línea Base	Meta
Accesos móviles y fijos a internet en el país	38.585.482 (2021)	71.383.142
Accesos móviles a Internet	30.133.039 (2021)	61.400.000
Entidades del orden nacional y territorial que den apertura, actualicen o usen los datos abiertos	651 (2022)	800
Personas sensibilizadas en el Uso Seguro y Responsable de las TIC	0	4.200.000
Formaciones finalizadas en habilidades digitales	0	797.000
Empresas y/o empresarios que adopten herramientas tecnológicas para la transformación digital	12.822 (2022)	32.822
Empresas de la Industria Digital beneficiadas para impulsar la transformación productiva del país.	1.569 (2022)	3.405
Personas mayores de cinco años que usan Internet	73,03 % (2021)	85 %

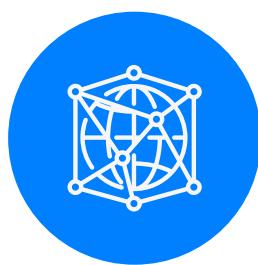
Fuente: Elaboración propia a partir de (DNP, 2024).

3.2 Colombia Potencia Digital

Con el fin de desarrollar una estrategia integral para desarrollar el ecosistema digital del país, el Gobierno Nacional comenzó a implementar "Colombia Potencia Digital", que busca **acelerar la transformación digital, cerrar brechas de conectividad y fortalecer los ecosistemas de innovación de todas las regiones del país.** Bajo el liderazgo del MinTIC, se busca posicionar a Colombia como un referente en materia de TIC y digitalización en el país, así como en la implementación y desarrollo de tecnologías de la cuarta revolución industrial, especialmente IA, en América Latina.

A través de esta estrategia se busca impactar a los distintos actores del ecosistema digital, con el fin de generar sinergias y articulación entre ciudadanía, empresarios, academia y sector público. Especialmente, se busca fortalecer las **comunidades de conectividad y las juntas de Internet** como una manera de cerrar la brecha de conectividad, así como el establecimiento de **Centros Potencia y Microcentros de IA** para fomentar la colaboración entre los distintos actores del ecosistema digital.

La estrategia se sustenta en tres pilares fundamentales:



Conectividad



Educación Digital



Ecosistemas de Innovación.

En cuanto a conectividad, el objetivo principal es **garantizar el acceso a Internet de alta velocidad en todo territorio nacional**, reduciendo la brecha digital y facilitando la adopción de tecnologías digitales en diversos sectores. Para ello, se ha destinado una inversión cercana a 5,4 billones de pesos, que incluye importantes proyectos como "Conectividad para Cambiar Vidas". Este programa fortalecerá las redes de transporte en 178 municipios y proporcionará conexión de banda ancha a 400 mil hogares de estratos 1 y 2. Además, a través de las líneas de fomento 1.0 y 2.0, se conectarán a 293.417 hogares de bajos recursos a Internet fijo, trabajando en colaboración con PRST y comunidades organizadas de conectividad.

Otros esfuerzos destacados en conectividad incluyen la iniciativa "Centros Digitales", que establecerá 14.057 puntos de conectividad gratuita en veredas, y "Zonas Comunitarias para la Paz", que brindará acceso a internet en 1.262 sedes educativas rurales de 162 municipios del Programa de Desarrollo con Enfoque Territorial (PDET). También se implementará el programa "Juntas de Internet - Comunidades de Conectividad", con el que 2.848 comunidades podrán acceder al servicio de internet, incluyendo soluciones satelitales para 1.640 de ellas. Finalmente, tras la Subasta 5G, se beneficiarán 1.191 sedes educativas en 233 municipios, que recibirán acceso comunitario a Internet mediante fibra óptica.

En cuanto a la educación digital, el enfoque está en la **formación de talento humano con habilidades digitales**, preparándolos para los desafíos de un mercado laboral cada vez más competitivo y tecnológico. Con una inversión de 720.000 millones de pesos, se busca capacitar a un millón de personas mediante programas como Generación TIC, Talento Tech, Senatec y Colombia Programa. Generación TIC se enfoca en ofrecer cursos adaptados a las necesidades regionales para niños, adolescentes, jóvenes y adultos. Talento Tech promueve la formación en áreas críticas como programación, inteligencia artificial y análisis de datos, mientras que Senatec se dirige a la formación técnica tanto en colegios públicos como privados, además de proporcionar cursos cortos a jóvenes y adultos. Por último, Colombia Programa está diseñado para formar a docentes con el objetivo de **fomentar el pensamiento computacional en instituciones educativas oficiales**, garantizando así la inclusión tecnológica en todos los niveles educativos.

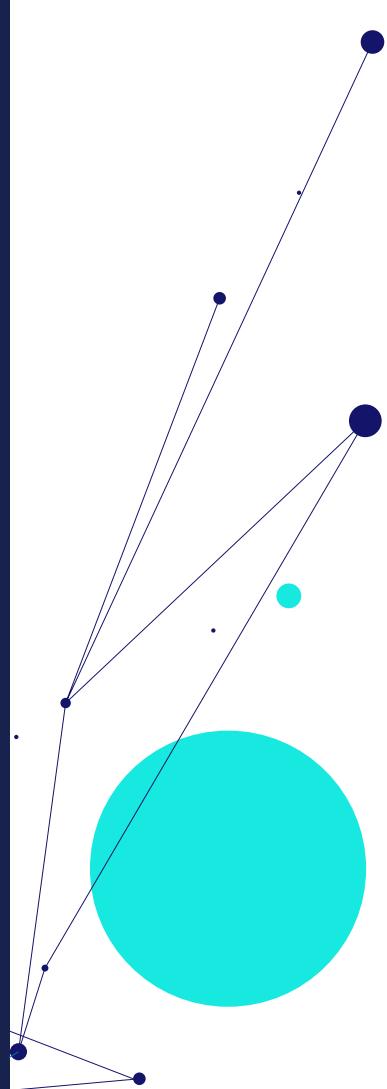
El pilar de ecosistemas de innovación busca **fomentar la creación de un entorno propicio para el emprendimiento digital, impulsando la colaboración entre los sectores público, privado y la academia**. A través del programa Colombia Potencia Digital, se han identificado áreas de desarrollo estratégico como TurismoTech, AgroTech y SaludTech. Estas áreas, seleccionadas con base en diagnósticos departamentales, serán trabajadas con estrategias específicas diseñadas para potenciar la innovación y el desarrollo socioeconómico del país. Este enfoque permitirá fortalecer el ecosistema de innovación de Colombia, atrayendo inversiones, generando empleo de calidad y consolidando al país como un líder en innovación digital en la región.

Adicionalmente, la estrategia "Colombia Potencia Digital" establece **objetivos y metas** a través de las cuales busca materializar estos pilares. Principalmente, esta busca impactar de manera significativa el desarrollo tecnológico y económico del país, mediante la promoción de la creación de nuevas empresas digitales y el apoyo a los ecosistemas digitales ya presentes en los distintos departamentos.

Esto permitirá diversificar la economía regional, así como aumentar la productividad de distintos sectores clave para el país como son: el agro, el turismo, las industrias creativas, los servicios financieros y los servicios en salud. Al respecto, la estrategia busca incrementar la productividad a través de la adopción de tecnologías digitales en los procesos productivos, permitiendo que las empresas, especialmente las de sectores tradicionales, optimicen sus operaciones y mejoren su competitividad tanto a nivel nacional como internacional.

Paralelamente, busca reducir la desigualdad digital, asegurando que todos los ciudadanos, sin importar su ubicación geográfica o nivel socioeconómico, tengan acceso a las tecnologías digitales, empezando por acceso a la conectividad y otros habilitadores digitales. Esto garantiza un desarrollo más equitativo y sostenible, donde todas las regiones puedan beneficiarse de los avances tecnológicos.

Por último, la estrategia busca generar empleo de calidad, con un énfasis especial en el sector TIC, que se proyecta como uno de los principales motores de crecimiento económico. Esto no solo contribuirá a la creación de oportunidades laborales bien remuneradas, sino que también fortalecerá el desarrollo de capacidades tecnológicas en el país, asegurando que Colombia esté preparada para enfrentar los desafíos del futuro digital.



Brecha digital y talento

Precisamente, la implementación de “**Colombia PotencIA Digital**” busca la superación de desafíos identificados en la transformación digital de Colombia. Uno de los principales retos es la persistencia de la brecha digital regional, que afecta especialmente a las zonas rurales en comparación con las urbanas. A pesar de los esfuerzos adelantados en el país, es necesario trabajar en garantizar una conectividad equitativa y un acceso adecuado a dispositivos tecnológicos en todo el territorio nacional.

Otro desafío radica en las necesidades de talento humano. La creciente demanda de profesionales con habilidades digitales supera ampliamente la oferta disponible en el país, lo que evidencia la necesidad de fortalecer los programas de formación. Además, es clave implementar estrategias que atraigan talento internacional para suplir esta carencia y enriquecer las capacidades locales.



En el ámbito empresarial, **la madurez digital de muchas MIPYME sigue siendo limitada**, lo que retrasa su capacidad para integrar tecnologías digitales en sus procesos productivos. Este aspecto se suma al desafío relacionado con la infraestructura tecnológica. Asimismo, se presentan dificultades para articular adecuadamente a los distintos actores del ecosistema. Adicionalmente, la inversión en redes de fibra óptica, centros de datos y otras tecnologías avanzadas es esencial para garantizar una conectividad estable y de alta velocidad que permita soportar la creciente demanda de servicios digitales.



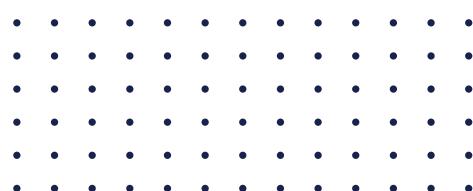
Igualmente, **el marco regulatorio del sector digital debe adaptarse a las nuevas dinámicas tecnológicas.** Es necesario contar con normativas claras y flexibles que no solo protejan a los usuarios, sino que también incentiven la innovación y la competencia dentro del sector, creando un entorno favorable para el desarrollo de la economía digital, especialmente en las regiones de Colombia.

Con este contexto en mente, se espera que Colombia Potencia Digital tenga un impacto en el país, particularmente en la transformación digital de los departamentos más rezagados. En términos económicos, **la digitalización de la economía debe convertirse en un motor clave para el crecimiento del PIB, estimulando la creación de nuevos empleos y fortaleciendo sectores clave.** Además, la adopción de tecnologías digitales en procesos productivos fortalecerá al empresariado al optimizar operaciones, reducir costos y mejorar la eficiencia.

La estrategia también pretende fomentar la innovación en el ecosistema empresarial, ofreciendo oportunidades para que las empresas desarrollen nuevos productos y servicios que respondan a las necesidades de un mercado cada vez más digitalizado. Esto se verá reflejado en un entorno de mayor competitividad y dinamismo económico.

En términos sociales, Colombia Potencia Digital apunta a una mayor inclusión social, a través del cierre de la brecha digital especialmente en las zonas rurales y apartadas. El acceso a Internet y a servicios digitales reducirá la desigualdad, permitiendo que más ciudadanos disfruten de una mejor calidad de vida y tengan acceso a oportunidades educativas, laborales y culturales que antes les eran inaccesibles.

Finalmente, es fundamental apostar por la transformación digital del país, ya que esto lo posicionará como un destino atractivo para la inversión extranjera directa, especialmente en el sector tecnológico y demás sectores estratégicos (agro, turismo, salud, industrias creativas y servicios financieros). Esto no solo fortalecerá la economía, sino que también impulsará la transferencia de conocimientos y tecnologías que beneficiarán a largo plazo a toda la sociedad colombiana.





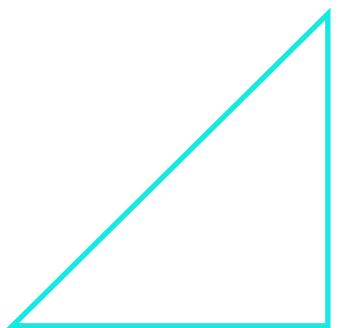
Ciberseguridad



4.0

Ciberseguridad

4.1 Diagnóstico de país



El rápido avance y adopción de las tecnologías digitales ha traído grandes beneficios para la sociedad, lo cual ha llevado a que estas sean una parte esencial de las dinámicas y el quehacer de personas, empresas y gobiernos. Un ejemplo de ello es que estas se han convertido en partes esenciales de la cadena de suministro de muchos servicios fundamentales, incluidos los servicios sociales (Banco Mundial, 2023). **No obstante, la digitalización también requiere avanzar en la garantía de ambientes digitales seguros y confiables, que permitan continuar consolidando el ecosistema digital en Colombia y en el resto del mundo.**

Por ejemplo, **Colombia, con cinco mil millones de intentos de ciberataques durante el primer semestre de 2023, fue el cuarto país más atacado de América Latina**, después de Brasil, México y

Venezuela (LINKTIC, 2024). Asimismo, de acuerdo con (Policía Nacional de Colombia, 2025), **en el año 2024 se reportaron 77.866 denuncias por delitos informáticos**, que representan un aumento del 23% con respecto al 2023 (63.249 denuncias). En ese sentido, se mantiene una tendencia creciente, asociada a una mayor digitalización del país. En 2024, los hurtos por medios informáticos fueron de nuevo el delito con mayor cantidad de denuncias (**37.409**) y registró un crecimiento del **20%** con respecto al 2023.

Por esto, la Policía Nacional señala que a medida que el uso y la dependencia de las tecnologías digitales se vuelven más generalizadas en la sociedad, las conductas delictivas relacionadas con el entorno digital han crecido de manera exponencial en sofisticación y en frecuencia (Policía Nacional de Colombia, 2025).

El panorama mundial de la ciberseguridad ha cambiado drásticamente en los últimos años, especialmente por los avances de tecnologías emergentes como la IA, el Blockchain y la computación cuántica, que han permitido que las amenazas y los ataques sean cada vez más sofisticados. Asimismo, el factor humano sigue siendo un elemento importante. La falta de habilidades con respecto a la ciberseguridad y el uso no responsable de las tecnologías digitales facilita que los cibercriminales exploten vulnerabilidades y con mayor frecuencia se materialicen conductas criminales.

Esta realidad ha llevado a que la ciberseguridad se convierta en un componente estructural del ecosistema digital global y que los países dediquen recursos e incrementen esfuerzos por tener un entorno digital seguro, confiable y resiliente. De esta manera, se busca generar confianza en la interacción con las tecnologías digitales, propender por la integridad y disponibilidad de los servicios fundamentales, y evitar afectaciones a la seguridad nacional.

Son varios los índices que miden a nivel mundial las capacidades o qué tan preparados están los países en términos de ciberseguridad. Uno de los más relevantes y actualizados es el Global Cybersecurity Index (GCI) de la UIT. Este índice particularmente evalúa el compromiso de los países con respecto a la ciberseguridad en torno al desarrollo de medidas agrupadas en cinco pilares: i) legal, ii) técnico, iii) organizacional, iv) desarrollo de capacidad, y v) cooperación⁸.

Colombia requiere un mayor compromiso en el desarrollo de capacidades relacionadas con ciberseguridad. De acuerdo con los resultados del GCI para las mediciones de 2020 y 2024, en los últimos años Colombia ha tenido un progreso en el desarrollo de las capacidades de ciberseguridad, pero este no ha sido integral. Si bien tiene avances con respecto a las medidas legales, de organización y de capacidades, también tiene retrocesos con respecto a las medidas de cooperación y medidas técnicas. Asimismo, los resultados dejan en evidencia que para ninguno de los pilares del GCI el país alcanza el máximo de los 20 puntos de referencia y, a pesar de los avances, aún tiene oportunidad de mejora en todas las medidas consideradas, principalmente, en cuanto a las medidas legales, de organización y a las medidas de cooperación (*Ver Tabla 7*).

⁸ Concretamente cada uno de los pilares mencionados miden lo siguiente: i) *Medidas legales*: Mide la implementación de leyes y regulaciones relacionadas con la ciberseguridad y el cibercrimen, entre otros; ii) *Medidas técnicas*: Mide la implementación de capacidades técnicas a través de agencias nacionales y en sectores específicos, esto incluye la existencia de equipos de respuesta a incidentes informáticos (CIRTs) y adopción de estándares de ciberseguridad; iii) *Medidas organizativas*: Mide el desarrollo de estrategias nacionales de ciberseguridad y la existencia de agencias de ciberseguridad que impulsan su implementación; iv) *Desarrollo de capacidades*: Mide el desarrollo de programas de concienciación y formación en ciberseguridad; v) *Medidas de cooperación*: Mide la participación en acuerdos internacionales y colaboración con otros países, agencias, y empresas en temas de ciberseguridad.

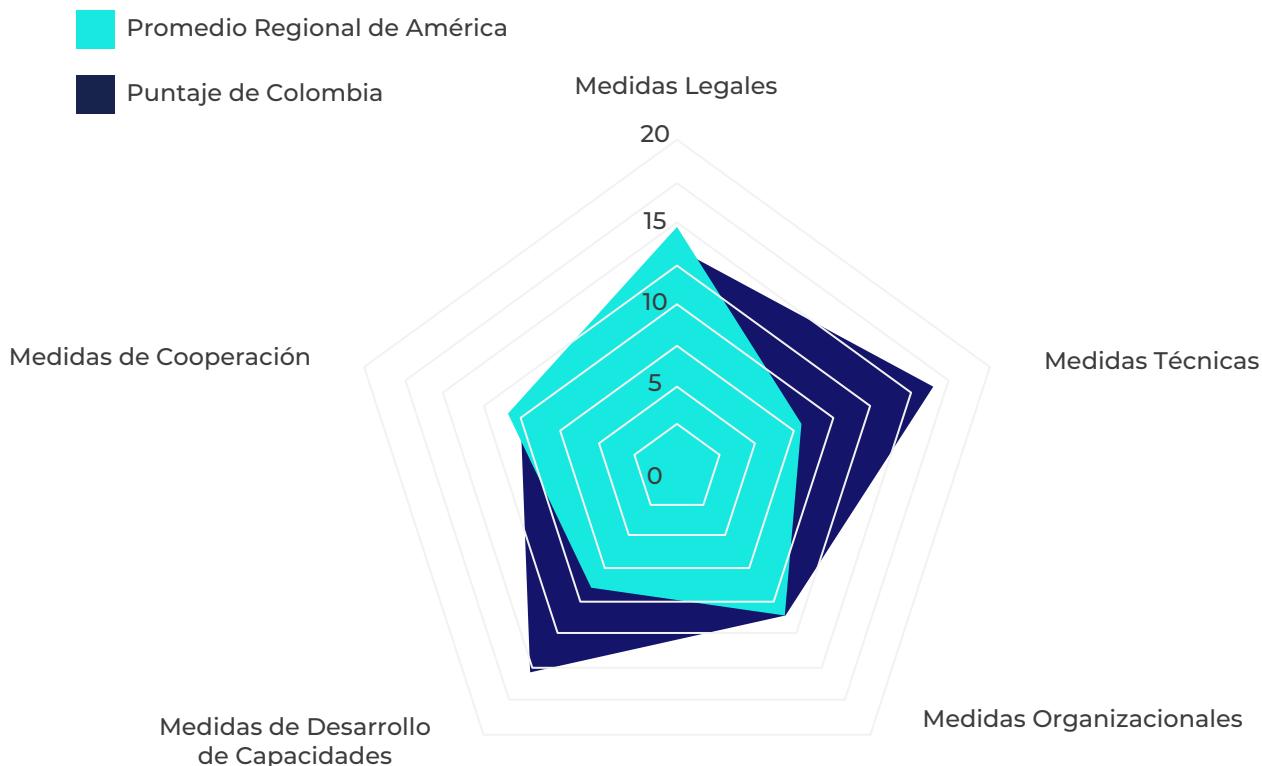
Tabla 7. Resultados de Colombia en el Global Cybersecurity Index 2020 y 2024

Pilares	2020	2024	Variación
Medidas legales	9,14	13,37	 4,23
Medidas técnicas	17,58	16,22	 -1,36
Medidas de organización	6,67	10,91	 4,24
Desarrollo de capacidad	14,42	15,14	 0,72
Medidas de cooperación	15,93	10,23	 -5,7
Total	63,74	65,87	 2,13

Fuente: Elaboración propia a partir de (UIT, 2020) y (UIT, 2024)

Cuando se analizan los resultados de Colombia en comparación con los obtenidos para toda la región de las Américas, se observa que son las medidas legales, de organización y de cooperación en las cuales el país tiene un desempeño similar o menor con respecto a los países de la región, confirmando que son las áreas en las cuales se requiere un mayor esfuerzo. Mientras que en las medidas técnicas y de desarrollo de capacidad son aquellas en las cuales se destaca al compararse con los países de la región y pueden considerarse fortalezas sobre las cuales seguir avanzando (*Ver Gráfico 11*). En la región de las Américas se destacan países como Estados Unidos y Brasil con un puntaje total de 99,86 y 96,38, respectivamente.

Gráfico 11. Resultados de Colombia y la región de las Américas en el Global Cybersecurity Index 2024



Fuente: Extraído de (UIT, 2024). Página 56.

De acuerdo con la UIT, Colombia es un país en proceso de consolidación de sus capacidades con respecto a la ciberseguridad. El GCI 2024 clasifica a los países en cinco niveles de acuerdo con su desempeño⁹ y ubica a Colombia en el nivel intermedio con respecto al desarrollo de sus capacidades de ciberseguridad (nivel 3). Esto indica que Colombia ha realizado avances relevantes en la implementación de medidas ciberseguridad a través de acciones impulsadas por el Gobierno que abarcan la evaluación, el establecimiento o la implementación de ciertas medidas en un número moderado de los pilares o indicadores considerados en la medición. Sin embargo, se requiere que la ciberseguridad siga siendo una prioridad y, con ello, se destinen mayores recursos y se incrementen los esfuerzos para diseñar e implementar las medidas requeridas.



⁹ Los cinco niveles son: 1) Role-modelling (puntaje de 95-100); 2) Advancing (puntaje de 85-95), 3) Establishing (puntaje de 55-85); 4) Evolving (puntaje de 20-55); y 5) Building (puntaje de 0-20).

A continuación, se profundiza con respecto al avance del país en estas medidas o capacidades de ciberseguridad.



Medidas Legales

Colombia cuenta con un marco de protección de datos robusto y ha desarrollado legislación para abordar la ciberdelincuencia. Con respecto a la protección de datos el país cuenta con dos leyes estatutarias y varios reglamentos, decretos y directivas sectoriales complementarias. Estas leyes estatutarias son: i) la Ley 1226 de 2008, por la cual se dictan las disposiciones generales del hábeas data financiero y se regula el manejo de la información contenida en bases de datos personales en este sector; ii) la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales¹⁰. Asimismo, el país cuenta con una entidad que actúa como autoridad de protección de datos que es la SIC, quien realiza la supervisión del cumplimiento de las disposiciones de protección de datos personales en el sector privado, e impulsa la concientización pública sobre la protección de datos personales en el país (Banco Mundial, 2023).

En relación con delitos informáticos, como lo destaca (Banco Mundial, 2023), Colombia cuenta con la Ley 1273 de 2009¹¹, que es considerada la principal legislación sustantiva sobre delitos ciberneticos en el país.

¹⁰ Ambas leyes se desarrollan con base en los derechos constitucionales establecidos en los artículos 15 y 20 de la Constitución Política de Colombia.

¹¹ Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las TIC, entre otras disposiciones.



Esta ley integra varios delitos ciberneticos en el Código Penal y se complementa con los siguientes actos jurídicos: Código Penal (Ley 599 de 2000), y leyes sobre pornografía infantil y explotación sexual (Ley 300 de 1996, Ley 679 de 2001 y Ley 1336 de 2009). Asimismo, la Ley 527 de 1999 reconoce la prueba digital como material probatorio dentro de los procesos de investigación judicial. Otras disposiciones procesales sobre ciberdelincuencia están contempladas en el Código General del Proceso (Ley 1564 de 2012), el Código de Procedimiento Penal (Ley 904 de 2004), y la Ley 270 de 1996 y en varias resoluciones de la Fiscalía que abordan temas relevantes como los procedimientos de cadena de custodia. También es importante destacar que, desde 2020, Colombia es parte signataria del Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como Convenio de Budapest (Ley 1928 de 2018).

Sin embargo, como queda en evidencia en el GCI 2024, Colombia aún tiene oportunidades de mejora con respecto a las medidas legales. De acuerdo con (Banco Mundial, 2023), el marco de protección de datos del país podría fortalecerse con algunos elementos básicos y una base jurídica adicional para el tratamiento legal de los datos. De igual forma, en el caso de la ciberseguridad, la END de Colombia 2023-2026 deja en evidencia la necesidad de crear una hoja de ruta que aborde e integre los esfuerzos interinstitucionales en materia legislativa, con el fin de evitar la obsolescencia normativa del país con respecto a los delitos informáticos y facilitar la cooperación internacional para combatir el cibercrimen.

Asimismo, **el país enfrenta retos para llevar a cabo la efectiva implementación de sus avances normativos.** Según (Banco Mundial, 2023), la Fiscalía General de la Nación, quien es la entidad encargada de la investigación y persecución de los casos de ciberdelincuencia en Colombia, y se fortaleció con la creación de la Dirección Especializada contra los Delitos Informáticos, de acuerdo con lo dispuesto en la Ley 2197 de 2022¹², presenta un déficit de personal calificado (abogados especializados en ciberdelincuencia y pruebas digitales), así como de recursos financieros y técnicos dado el aumento creciente de la ciberdelincuencia en el país. A esto se le suma, que los jueces y magistrados del sistema judicial, que son los responsables de juzgar los casos de ciberdelincuencia, tienen conocimientos limitados en esta materia y en evidencia digital. Además, a diferencia de la Fiscalía, el sistema judicial de Colombia no tiene una unidad especializada en ciberdelincuencia.

¹² Por medio de la cual se dictan normas tendientes al fortalecimiento de la seguridad ciudadana y se dictan otras disposiciones.



Medidas Técnicas

El Gobierno de Colombia ha avanzado en el desarrollo de capacidades técnicas para responder a emergencias ciberneticas y a incidentes de seguridad informática a nivel nacional. Como resultado del desarrollo de política pública en el país con respecto a ciberseguridad y seguridad digital, Colombia cuenta con un Grupo Interno de Trabajo de Respuesta a Emergencias Ciberneticas (ColCERT) y varios grupos sectoriales de respuesta a incidentes de seguridad informática (CSIRT). Estos grupos constituyen el esfuerzo nacional de respuesta a incidentes de ciberseguridad.

De acuerdo con lo dispuesto en el CONPES 3701, en 2013, se creó el ColCERT en el Ministerio de Defensa Nacional (MinDefensa), el cual fue transferido en 2022 al MinTIC y es el punto de contacto a nivel nacional e internacional con respecto a la respuesta a incidentes.

El **ColCERT** se apoya con los **CSIRT**, dentro de estos se destaca el **CSIRT Gobierno (CSIRT Gob)**, que es administrado por MinTIC y ubicado en las instalaciones de la Policía Nacional. Este dentro de sus funciones proporciona **apoyo técnico a las instituciones públicas** con su ciclo de **gestión de respuesta a incidentes**. También se destaca el **CSIRT Defensa**, que protege la **infraestructura de TIC de las fuerzas armadas** y del grupo de **empresas vinculadas al sector de la defensa**. También es relevante mencionar que en el **sector privado** las grandes empresas de los sectores de telecomunicaciones, financiero y energético de Colombia han desarrollado sus propias capacidades de gestión de respuesta a incidentes. De acuerdo con (Banco Mundial, 2023), existen en el país **20 CSIRT y centros de operaciones de seguridad debidamente registrados**.



De acuerdo con los resultados del GCI para el 2020 y 2024, **a pesar de los avances en este tipo de medidas, en 2024 los resultados del pilar “medidas técnicas” disminuyó levemente en comparación con 2020, mostrando que el país todavía tiene oportunidades de mejora en este aspecto.** De acuerdo con (Banco Mundial, 2023), el ColCERT aún se encuentra en proceso de consolidación, teniendo en cuenta que la transición a MinTIC no incluyó ni el personal y los equipos que tenía en MinDefensa. Por otra parte, aunque existe comunicación entre el ColCERT y los CSIRT, tanto públicos como del sector privado, se requiere una mayor coordinación entre ellos, así como desarrollar mecanismos más eficientes y expeditos para el intercambio de información.



Medidas de organización

Colombia tiene importantes avances con respecto a las políticas y estrategias de ciberseguridad y seguridad digital, así como en los mecanismos de gobernanza. Desde 2011 en el país se han diseñado e implementado políticas públicas, con el fin de desarrollar las capacidades necesarias para gestionar las amenazas informáticas y generar un entorno digital seguro y confiable. A la fecha el país ha desarrollado tres políticas nacionales: CONPES 3701 de 2011¹³, CONPES 3854 de 2016¹⁴, y CONPES 3995 de 2020¹⁵. De igual forma, se ha avanzado en facilitar la participación, articulación e interacción de las múltiples partes interesadas para fortalecer las capacidades en la gestión de riesgos de seguridad digital y lograr un abordaje integral que promueva el adecuado aprovechamiento del entorno digital. En 2022, se expidió el Decreto 338¹⁶, con el cual se crea el modelo y las instancias de gobernanza de seguridad digital en el país. Dentro de las instancias definidas están: i) Coordinación Nacional de Seguridad Digital; ii) Comité Nacional de Seguridad Digital; iii) Grupos de Trabajo de Seguridad Digital; iv) Mesas de Trabajo de Seguridad Digital; y v) Puestos de Mando Unificado de Seguridad Digital.

¹³ Lineamientos de política para ciberseguridad y ciberdefensa. Disponible en: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

¹⁴ Política Nacional de Seguridad Digital. Disponible en: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

¹⁵ Política Nacional de Confianza y Seguridad Digital. Disponible en: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf>

¹⁶ Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866>

Sin embargo, como se evidencia con los resultados del GCI 2024, **a pesar de los avances, es en relación con las medidas organizativas donde el país tiene mayores oportunidades de mejora. Algunas de ellas son:**

Primero

Colombia aún no tiene una política o estrategia nacional vigente de ciberseguridad o seguridad digital. El periodo de implementación de la última política nacional (CONPES 3995) terminó 2022 y, aunque el PND 2022-2026 y en la END de Colombia 2023-2026 definen que el Gobierno Nacional diseñará e implementará una estrategia para la protección de las personas y las infraestructuras digitales, así como para el fortalecimiento de las entidades del Estado y la garantía en la prestación de sus servicios en el entorno digital, a la fecha esta nueva estrategia aún sigue en proceso de elaboración.



Segundo

El Gobierno Nacional no cuenta con una agencia de ciberseguridad. Si bien el país tiene un modelo de gobernanza para la seguridad digital, este aún está en proceso de implementación y consolidación. Adicionalmente, como lo indica (DNP, 2024), el liderazgo del Gobierno Nacional en materia de seguridad digital está disperso. Aunque existen varias entidades que propenden por un entorno digital seguro para el país (por ejemplo, Presidencia de la República, MinTIC y MinDefensa), estas no cuentan con las capacidades y alcance suficientes para ejercer el liderazgo estratégico integral requerido en cuanto a seguridad digital.



Siguiendo las buenas prácticas a nivel internacional, tanto el PND 2022-2026, como la END 2023-2026, definieron acciones para fortalecer la planificación, coordinación y articulación del país en materia de seguridad digital, entre ellas la creación de una Agencia Nacional de Seguridad Digital y Asuntos Espaciales, que dependa directamente de la Presidencia de la República. Actualmente, existe además un proyecto de ley¹⁷ en el Congreso de la República para su creación; sin embargo, a la fecha solo ha surtido uno de los cuatro debates que se discutirán para que el proyecto de Ley sea una realidad en el país.



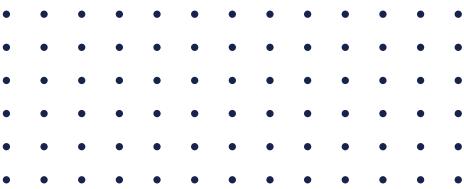
Desarrollo de capacidades

Colombia ha avanzado en la concientización y desarrollo de competencias de ciberseguridad. De acuerdo con el GCI 2024, una de las fortalezas del país es el desarrollo de capacidades de ciberseguridad, las cuales se han impulsado a través de las políticas nacionales que abordan de manera general la transformación digital como aquellas específicas en ciberseguridad o seguridad digital. Por ejemplo, en el CONPES 3995 se definió como uno de los objetivos principales el fortalecimiento de las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado. De igual forma, en la END de Colombia 2023-2026, se definieron acciones para fomentar la preparación de la ciudadanía y servidores públicos con respecto a la seguridad digital. En el marco de esta estrategia, el MinTIC está implementando el programa “*CiberPaz*”, que incluye sensibilizaciones y talleres en temas de ciberseguridad, entre otros. Para el 2024 se esperaba sensibilizar a 30.000 personas en todo el territorio nacional¹⁸.

Sin embargo, **el país aún tiene oportunidades de mejora en este aspecto dado el incremento de la ciberdelincuencia, así como el aumento de la demanda de servicios de ciberseguridad en el sector público y privado.** Por ejemplo, según la ECV-DANE 2023, para el total nacional, solo el 24,6% de las personas de 5 y más años que usaron computador o Internet indicó tener la habilidad de comprobar que las noticias o información que consulta o recibe a través de Internet son ciertas o verdaderas (*Ver Tabla 4*). Asimismo, de acuerdo con (Banco Mundial, 2023), los planes de estudio de las escuelas primarias y secundarias aún no incluyen cursos relacionados con la ciberseguridad y la oferta académica de educación en ciberseguridad a nivel terciario es aún insuficiente para suplir las demandas actuales del país. El déficit de talento en el país puede aumentar si se tiene en cuenta que el aumento de la demanda de servicios representa un incremento de la demanda de profesionales de seguridad calificados, que se complejiza dada las dificultades en la retención de talento y que las organizaciones buscan personas con competencias certificadas.

¹⁷ Proyecto de Ley 023 de 2023 Cámara

¹⁸ Para más información consultar: <https://ciberpaz.gov.co/portal/>



Medidas de Cooperación

En los últimos años el país ha retrocedido en cuanto a medidas de cooperación. De acuerdo con las mediciones del GCI, entre los años 2020 y 2024 Colombia disminuyó en 5,7 puntos con respecto al pilar de medidas de cooperación. En este pilar el país tiene la más baja calificación (10,23) de todos los pilares considerados, y está por debajo del promedio de la región de las Américas y, en ese sentido, tiene las mayores oportunidades de crecimiento. Aunque Colombia tiene varias alianzas (por ejemplo, CSIRT Américas de la OEA), la cooperación internacional en materia de seguridad digital aún es baja, especialmente para enfrentar amenazas transfronterizas y el cibercrimen.

No obstante, como lo menciona (Banco Mundial, 2023), los socios internacionales para el desarrollo (por ejemplo, el Banco Mundial, la OCDE, el Consejo de Unión Europea y la OEA, entre otros) están interesados y dispuestos a apoyar el fortalecimiento de la ciberseguridad en el país. Por ejemplo, actualmente, la Sección de Ciberseguridad de la OEA está apoyando al Gobierno nacional de Colombia en la elaboración de la estrategia nacional de seguridad digital para el periodo 2024-2026.



Ciberseguridad en Empresas y Entidades Públicas

Para las empresas de Colombia la ciberseguridad aún es una tarea pendiente. De acuerdo con la Encuesta de Tecnologías de la Información y las Comunicaciones en Empresas (ENTIC Empresas) de 2020 del DANE, el porcentaje de empresas que contaron con una política formal de administración de los riesgos de seguridad de las TIC fue bajo, principalmente para el sector industrial (29,8%) y el sector comercio (28,2%). En el caso de las actividades del sector servicios este porcentaje estuvo entre 29,3% y 70,5%. De igual forma, un porcentaje importante de empresas no cuentan con un software o sistema de ciberseguridad. Según la ENTIC Empresas 2020, solo el 20,1% del sector industria y 17,8% del sector comercio contaban con un software o sistema de ciberseguridad. Para las actividades del sector servicios este porcentaje estuvo entre 19,2% y 55,9%.

Adicionalmente, como se mencionó anteriormente, si bien las grandes empresas de los sectores de telecomunicaciones, financiero y energético de Colombia han desarrollado sus propias capacidades de gestión de respuesta a incidentes y tienen CSIRT y centros de operaciones de seguridad, es una realidad diferente con la MiPymes. En el caso de estas empresas la capacidad de respuesta a incidentes sigue siendo incipiente y el apoyo público a las MiPymes para mejorar sus capacidades de ciberseguridad es limitado (Banco Mundial, 2023).

Las entidades públicas de Colombia cuentan con directrices y lineamientos con respecto a la seguridad y privacidad de la información.

La Política de Gobierno Digital, que es el instrumento gubernamental que propende por la transformación digital pública en el país, incluye como uno de los habilitadores transversales de la transformación digital de las entidades públicas del país la seguridad y privacidad de la información para generar confianza en el uso del entorno digital.

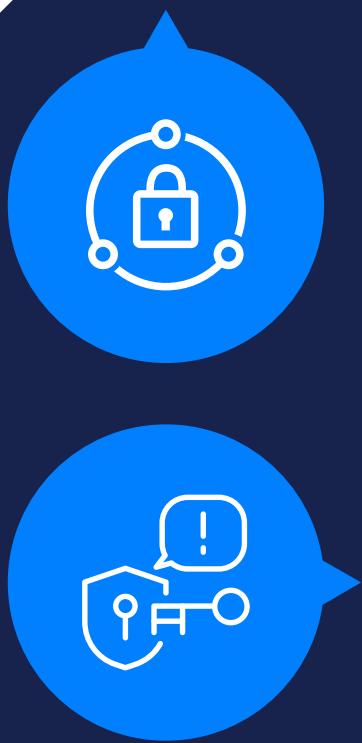
Con este habilitador se busca que las entidades públicas “(...) *desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos*” (Artículo 1, Decreto 767 de 2022). Dentro de los lineamientos que ha desarrollado MinTIC se encuentra el Modelo de Seguridad y Privacidad de la Información (MSPI)¹⁹, así como las orientaciones para desarrollar una política de seguridad y privacidad de la información.

¹⁹ Este modelo tiene el objetivo de formalizar al interior de las Entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital. El modelo consta de cinco (5) fases (diagnóstico, planificación, operación, evaluación de desempeño, y mejoramiento continuo), las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información.

No obstante, **las entidades públicas del país necesitan avanzar con mayor contundencia en términos de seguridad y privacidad de la información, especialmente las entidades del orden subnacional.** Según los resultados del Índice de Gobierno Digital de MinTIC para los años 2022 y 2023 para el componente de “Seguridad y Privacidad de la Información”, si bien las entidades públicas del orden nacional y del orden subnacional han avanzado, aún tienen un amplio margen de mejora en el desarrollo de las capacidades relacionadas, principalmente, las entidades públicas del orden subnacional.

Mientras que las entidades del orden nacional obtuvieron un promedio de 68,0 puntos en 2022 y de 72,8 puntos en 2023, de 100 puntos posibles, los puntajes de las entidades del orden subnacional fueron en promedio de 37,1 puntos en 2022 y 45,1 puntos en 2023.

Por otra parte, **Colombia ha avanzado en la identificación de los sectores estratégicos nacionales y las Infraestructuras Ciberneticas Críticas Nacionales (ICCN).** De acuerdo con (Banco Mundial, 2023), desde 2016 el Gobierno nacional, identificó los servicios esenciales nacionales y también realizó un inventario de las ICCN, el cual se ha venido actualizando en los años posteriores. Con el Decreto 338 de 2022, se establece que el MinTIC es responsable de hacer un inventario de las ICCN públicas y de los servicios esenciales y de actualizarlo cada dos años. En ese sentido, MinTIC junto con Presidencia de la República durante el 2024 han estado trabajando en la definición de la metodología para realizar el levantamiento de ICCN, así como en la respectiva actualización de estas infraestructuras. El Decreto 338 de 2022 también establece otros lineamientos para el fortalecimiento de la seguridad de las ICCN como, por ejemplo, la vinculación de los sectores críticos y prestadores de servicios esenciales al ColCERT, y obligaciones de seguridad de las autoridades titulares de infraestructura crítica, o que presten servicios esenciales, entre ellos un plan de seguridad digital, protección de las redes, las infraestructuras críticas ciberneticas, los servicios esenciales y los sistemas de información en el ciberespacio.



4.2 Políticas Públicas y Normatividad

Atendiendo a la creciente digitalización del país, **la ciberseguridad se ha convertido en una prioridad estratégica para Colombia en respuesta a la necesidad de contar con seguridad digital para fomentar confianza en todo el ecosistema digital, así como hacer frente a las amenazas digitales, como ataques cibernéticos, delitos informáticos y brechas de seguridad que afectan tanto al sector público como privado.** Asimismo, se ha comenzado a fortalecer las capacidades institucionales de ciberseguridad y ciberdefensa, con el fin de dotar a la administración pública de medios para atender incidentes de ciberseguridad. Este enfoque ha llevado al desarrollo de políticas públicas y marcos normativos que buscan proteger la infraestructura crítica del país, salvaguardar los datos personales, garantizar la seguridad en el entorno digital y proteger los derechos de la ciudadanía.

Documentos CONPES

Colombia ha definido estrategias clave y políticas públicas nacionales en ciberdefensa, ciberseguridad, y seguridad y confianza Digital a través de los documentos CONPES, que establecen las directrices y prioridades a nivel nacional. Estos han permitido establecer funciones e instituciones encargadas de la implementación de distintos procesos relevantes en el ecosistema de ciberseguridad nacional. Asimismo, han jugado un rol relevante en el proceso de adopción de mejores prácticas internacionales en las organizaciones del país. Con esto en mente, procedemos a mencionar los documentos CONPES relevantes en esta materia.

➤ El **CONPES 3701 de 2011** establece la Política Nacional para Ciberseguridad y Ciberdefensa en Colombia, con el objetivo de **fortalecer la protección de los activos estratégicos del país frente a las crecientes amenazas en el ciberespacio.** Este documento reconoce el impacto que los incidentes cibernéticos tienen en la seguridad nacional, la economía y la sociedad, y plantea estrategias para garantizar la seguridad de la información, mitigar el impacto de los incidentes y generar confianza digital.

Como parte de su enfoque, el CONPES 3701 propone la consolidación de una estructura organizativa que permita gestionar la seguridad cibernética de manera efectiva a través de la articulación de distintos actores. Para ello, **propone la creación de una Comisión Intersectorial, encargada de definir la visión estratégica en la gestión de la información y de establecer directrices sobre infraestructura tecnológica, seguridad digital y ciberdefensa.**

En el marco institucional que crea este documento CONPES, se destacan entidades clave como: el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), hoy en día adscrito al MinTIC, que actúa como coordinador nacional en asuntos de ciberseguridad; el Comando Conjunto Cibernético de las Fuerzas Militares (CCCOI), cuya misión es prevenir y contrarrestar amenazas cibernéticas contra la seguridad nacional; y el Centro Cibernético Policial (CCP), enfocado en la seguridad digital y la lucha contra los delitos informáticos en el país.

Otro aspecto fundamental del documento es el impulso a un **marco normativo sólido, que permita establecer regulaciones claras para la protección del ciberespacio**. En el cual se promueve la adopción de estándares internacionales en la gestión de la seguridad de la información, asegurando que el país cuente con leyes y normativas actualizadas en esta materia.

La protección de infraestructuras críticas, como telecomunicaciones, servicios financieros y el sector energético son pilares esenciales dentro de esta política. Para ello, el CONPES plantea la necesidad de identificar estos activos y aplicar medidas avanzadas de ciberseguridad que prevengan ataques o interrupciones en su funcionamiento. Adicionalmente, recomienda la realización de análisis de riesgos cibernéticos y la implementación de sistemas de gestión de seguridad basados en normas reconocidas a nivel global, como la ISO 27001.

El fortalecimiento del talento humano en ciberseguridad también es una prioridad. El CONPES 3701 busca fomentar la capacitación y especialización del personal técnico y de los funcionarios gubernamentales, al tiempo que se impulsa la investigación en este campo. En paralelo, destaca la importancia de la cooperación internacional, promoviendo acuerdos con otros países y organismos especializados para el intercambio de información y mejores prácticas en la lucha contra amenazas digitales.

Por último, el documento subraya el rol de la ciudadanía en la construcción de un entorno digital seguro. Para ello, contempla estrategias de concientización y educación que fomenten una cultura de seguridad digital y un uso responsable de la tecnología por parte de los ciudadanos.

➤ **El CONPES 3854 de 2016** establece la Política Nacional de Seguridad Digital, con el propósito de **fortalecer la protección de la información en el país y garantizar un entorno digital confiable y resiliente para ciudadanos, empresas e instituciones**. Este documento reconoce el impacto creciente de las amenazas cibernéticas y la importancia de consolidar estrategias articuladas para enfrentar estas en distintos sectores.

Uno de los principales lineamientos de esta política es **la creación de un marco de gestión de riesgos digitales**, que da lineamientos a entidades públicas y privadas para identificar, evaluar y mitigar las amenazas cibernéticas.

Se establece la necesidad de que cada sector económico adopte modelos de seguridad específicos y desarrolle capacidades para la prevención y respuesta ante incidentes digitales.

En el ámbito normativo y regulatorio, el CONPES 3854 **promueve la actualización de leyes y estándares relacionados con la seguridad digital**. Se enfatiza la necesidad de fortalecer la protección de datos personales, mejorar las normativas sobre delitos informáticos y garantizar la privacidad en línea. Además, se plantea la adopción de estándares internacionales en ciberseguridad, alineando las políticas nacionales con marcos como el Convenio de Budapest sobre ciberdelincuencia y las directrices de la OCDE.

El CONPES también resalta la importancia de la ciberseguridad en el sector productivo, promoviendo **la creación de estrategias para fortalecer la seguridad digital en sectores clave como el financiero, el energético y el de telecomunicaciones**. Se insta a las empresas a adoptar mejores prácticas en protección de la información, integrando la seguridad digital en sus planes de negocio.

Otro componente clave de esta política es el **desarrollo de capacidades humanas y técnicas en seguridad digital**. Este fomenta la creación de programas de formación y certificación en ciberseguridad, dirigidos a servidores públicos, profesionales de tecnologías de la información, así como usuarios y ciudadanos en general. Además, impulsa la inversión en investigación y desarrollo de soluciones innovadoras en seguridad digital.

En términos de cooperación internacional, el CONPES 3854 refuerza el compromiso de Colombia con organismos multilaterales y con iniciativas de colaboración en ciberseguridad. Este busca **fortalecer la cooperación con países aliados, participar en redes de intercambio de información sobre amenazas digitales y mejorar la capacidad de respuesta ante incidentes de gran escala**.

Finalmente, este documento destaca la importancia de **promover una cultura de seguridad digital en la ciudadanía**. Para ello, propone campañas de concientización sobre riesgos en internet, educación en buenas prácticas digitales y programas de acompañamiento a empresas y entidades públicas en la adopción de medidas de seguridad.

➤ El **CONPES 3995 de 2020** establece la Política Nacional de Confianza y Seguridad Digital, con el propósito de fortalecer la resiliencia del país frente a los riesgos digitales y consolidar un entorno confiable para la transformación digital del país.

Uno de los ejes clave del CONPES 3995 es la **gestión del riesgo digital en sectores estratégicos como salud, educación, finanzas y gobierno**. Además, establece mecanismos para fortalecer la seguridad en los servicios digitales y garantizar la continuidad de operaciones ante posibles ataques cibernéticos. También promueve la adopción de tecnologías emergentes como inteligencia artificial y blockchain, con el fin de mejorar la seguridad de los sistemas digitales.

Desde el punto de vista normativo, el documento propone modernizar el marco legal en materia de ciberseguridad, incluyendo la actualización de la legislación sobre delitos informáticos y protección de datos personales. Además, **enfatiza la necesidad de armonizar las regulaciones nacionales con estándares internacionales, en especial con los lineamientos de la OCDE y la Unión Internacional de Telecomunicaciones (UIT)**.

El fortalecimiento de la ciberseguridad en la administración pública es otro de los pilares de esta política. El CONPES plantea la implementación de una **Estrategia Nacional de Seguridad Digital**, que garantice que todas las entidades estatales adopten medidas de seguridad en la prestación de sus servicios digitales. Esto incluye el uso obligatorio de esquemas de autenticación robusta, protección de datos personales y monitoreo constante de incidentes cibernéticos.

En el ámbito empresarial, el CONPES 3995 impulsa la adopción de buenas prácticas en seguridad digital dentro del sector privado, incentivando a las empresas a invertir en infraestructura segura y desarrollar planes de respuesta ante incidentes cibernéticos. Igualmente, **fomenta la certificación en normas de seguridad como ISO 27001 e ISO 27701, especialmente en empresas que manejan grandes volúmenes de información sensible**.



El documento también subraya la importancia de la **educación y concientización en seguridad digital**, proponiendo estrategias para fortalecer la formación en ciberseguridad desde la educación básica hasta la especialización profesional. Asimismo, establece programas de sensibilización dirigidos a ciudadanos y pequeñas empresas, con el objetivo de reducir los riesgos asociados a fraudes electrónicos y suplantación digital.

Otro aspecto fundamental del CONPES 3995 es la promoción de la cooperación internacional en ciberseguridad. Este busca reforzar la colaboración con organismos multilaterales, participar en redes de inteligencia sobre amenazas digitales y mejorar la capacidad de respuesta ante ataques cibernéticos globales. **En este sentido, Colombia reafirma su compromiso con acuerdos internacionales en la materia, incluyendo la lucha contra el cibercrimen y la protección de infraestructuras críticas.** Asimismo, es relevante tener en cuenta estándares y mejores prácticas internacionales para garantizar niveles adecuados de seguridad en las redes. En ese sentido, destacamos el rol de la Mobile Cibersecurity Knowledge Base (MCKB) de GSMA, como un insumo valioso para identificar, mapear y mitigar riesgos cibernéticos.

Finalmente, el CONPES hace énfasis en la necesidad de **generar confianza digital en la ciudadanía, garantizando que el ecosistema digital sea seguro, accesible y respetuoso de los derechos de las personas.**

Para ello, se proponen mecanismos de auditoría y control sobre el uso de tecnologías digitales, asegurando que las instituciones públicas y privadas cumplan con altos estándares de seguridad y transparencia.



Normatividad

➤ **La Constitución Política de Colombia**, consagra el derecho de habeas data y, por tanto, la protección de datos personales, como un derecho fundamental consagrado en su artículo 15. Este establece que todas las personas tienen derecho a conocer, actualizar y rectificar la información que sobre ellas se haya recogido en bancos de datos o archivos de entidades públicas y privadas. Este viene a complementar el derecho a la intimidad y la vida privada consagrado en el mismo artículo de la Constitución Política.

➤ Para desarrollar este derecho, se promulgó la **Ley 1581 de 2012**, conocida como la Ley de Protección de Datos Personales, que establece un marco normativo integral para el tratamiento de la información personal. Su objetivo es **garantizar el respeto por los derechos de privacidad, intimidad y habeas data de los ciudadanos, regulando la forma en que las entidades públicas y privadas pueden recolectar, almacenar, usar y compartir datos personales**.

La ley se fundamenta en **principios rectores que orientan el tratamiento de la información**, como la finalidad, la libertad, la transparencia, la veracidad, el acceso restringido, la seguridad y la confidencialidad. Estos principios establecen que los datos sólo pueden ser recolectados para propósitos específicos informados al titular, deben ser veraces y actualizados, no pueden ser accesibles por cualquier persona, deben contar con medidas de seguridad adecuadas y las personas involucradas en su manejo deben garantizar la reserva de la información.

Además, la ley también reconoce los derechos fundamentales para los titulares de los datos personales. Entre estos derechos se encuentran el acceso a la información almacenada en bases de datos, la posibilidad de actualizar o corregir información incorrecta, la facultad de revocar la autorización y solicitar la eliminación de datos cuando no exista un deber legal o contractual que justifique su conservación, y el derecho a ser informado sobre el uso que se le ha dado a su información.



➤ Para desarrollar las disposiciones contenidas en la Ley 1581 de 2012, el **Decreto 1377 de 2013** reglamenta su implementación y establece directrices operativas para garantizar su implementación efectiva. Entre sus disposiciones, define responsabilidades específicas para quienes tratan datos personales, regula la transferencia y transmisión de información a terceros, especialmente cuando esta es compartida con entidades extranjeras. Igualmente, desarrolló los principios de la Ley 1581 de 2012, especialmente el de responsabilidad demostrada. También establece la obligatoriedad de contar con políticas de tratamiento de información publicadas y accesibles para los titulares de los datos. Asimismo, refuerza la obligación de reportar incidentes de seguridad ante la SIC, en caso de vulneraciones o filtraciones de datos.

➤ En ese contexto, como entidad encargada de hacer cumplir la Ley 1581 de 2012, la SIC desarrolló en 2020 la **Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales**. Su propósito es orientar a las organizaciones en la prevención, detección y respuesta ante situaciones que puedan comprometer la privacidad de la información. Esta guía establece que se considera un incidente de seguridad cualquier acceso no autorizado, pérdida, alteración o divulgación indebida de datos personales. Además, establece la obligación de reportar estos incidentes a la SIC dentro de un plazo razonable y notificar a los titulares afectados, especificando el tipo de información comprometida y las medidas correctivas adoptadas.

Al respecto, para minimizar los riesgos asociados a la seguridad de la información, la SIC recomienda la implementación de protocolos de respuesta a incidentes, los cuales deben incluir la identificación y evaluación de riesgos, la descripción de las responsabilidades del personal, los tiempos de atención y ejecución, el reporte de progreso, planes de recuperación en caso de pérdida de información y la capacitación de empleados y usuarios en buenas prácticas de ciberseguridad.

➤ Por otro lado, la Ley 1266 de 2008, conocida como la Ley de Hábeas Data Financiero, establece el marco normativo para el tratamiento de la información crediticia, financiera, comercial y de servicios en el país. Esta norma otorga a los ciudadanos el derecho a conocer, actualizar y rectificar la información que se encuentra en bases de datos de entidades financieras y centrales de riesgo. Asimismo, impone obligaciones a los operadores de información en términos de seguridad, exigiendo la implementación de medidas que prevengan el acceso, uso o alteración no autorizada de los datos. En este sentido, los incidentes de seguridad en el tratamiento de información financiera deben ser gestionados bajo estrictos protocolos de control, notificación y respuesta.

Por su parte, la SFC, como entidad encargada de la vigilancia y control del sector financiero, ha desarrollado normativas específicas sobre reportes de seguridad de la información. A través de la **Circular Única 033 de 2020**, la entidad establece lineamientos para que bancos, aseguradoras y demás entidades vigiladas implementen políticas de seguridad cibernética. Estas deben incluir procedimientos de monitoreo, detección y respuesta ante incidentes que puedan comprometer la integridad, disponibilidad o confidencialidad de la información, garantizando así la estabilidad del sistema financiero y la protección de los datos de los usuarios.

En materia de la ciberseguridad y lucha contra los delitos informáticos, la **Ley 1273 de 2009**, también llamada Ley de Delitos Informáticos, representó un avance significativo en la legislación colombiana. Esta norma modificó el Código Penal para incluir una nueva categoría de delitos relacionados con la protección de la información y los datos en entornos digitales, estableciendo sanciones a quienes cometan delitos cibernéticos. Entre las conductas tipificadas se encuentran el acceso indebido a sistemas informáticos, la violación de datos personales, la interceptación de comunicaciones, el daño informático, la utilización de software malicioso y el fraude mediante medios electrónicos. Además, estableció penas más severas para quienes cometan este tipo de delitos, reconociendo la creciente amenaza que representan en un mundo cada vez más digitalizado.

Para fortalecer la seguridad de la información en el sector público, el MinTIC diseñó el **Modelo de Gestión de Seguridad de la Información (MGSI)**.



Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de los datos en el sector público, promoviendo una gestión eficaz de los riesgos asociados a la ciberseguridad. Este modelo sigue estándares internacionales como la norma ISO 27001, que establece buenas prácticas para la gestión de la seguridad de la información.

El MGSI se basa en un enfoque de gestión de riesgos, lo que implica que las entidades públicas deben identificar, analizar y mitigar amenazas que puedan comprometer la seguridad de la información. Para ello, se establecen políticas, procedimientos y controles que aseguren el cumplimiento de normativas y estándares en seguridad digital. Entre sus pilares fundamentales se encuentran la gestión de incidentes de seguridad, la protección de infraestructuras críticas y la capacitación de los funcionarios en ciberseguridad.

El MGSI se encuentra desarrollado normativamente en el **Decreto Único Reglamentario 1078 de 2015**, que regula la Política de Gobierno Digital, establece principios, directrices y procedimientos para mejorar la seguridad en el ámbito digital y la protección de los recursos y datos en las entidades del Estado. En términos de ciberseguridad, el decreto establece medidas que deben implementar las entidades para proteger la infraestructura digital y la información sensible, asignando responsabilidades específicas a áreas como la administración de la infraestructura tecnológica y la protección de datos.

Asimismo, regula el manejo de riesgos asociados a ciberataques, buscando que las entidades del Estado establezcan protocolos para identificar, gestionar y mitigar posibles incidentes relacionados con la ciberseguridad, como el acceso no autorizado a la información, el malware, entre otros. De igual manera, los lineamientos y estándares para la estrategia de seguridad digital, así como el MGSI como habilitador de la política de Gobierno Digital, se encuentran consagrados en la **Resolución 500 de 2021**.

Particularmente, el Decreto 338 de 2022, que modifica el Decreto 1078 de 2015, tiene como propósito fortalecer la seguridad digital en Colombia, estableciendo directrices para la coordinación y articulación interinstitucional en la prevención, detección y respuesta ante incidentes de seguridad digital. Este decreto refuerza el papel del Estado en la protección del ciberespacio nacional y la adopción de medidas de ciberseguridad en las entidades públicas y privadas que gestionan infraestructuras críticas.

Uno de los principales aspectos del Decreto 338 de 2022 es la consolidación de un **modelo de gobernanza en seguridad digital, promoviendo la cooperación entre el MinTIC, el ColCERT, el Centro Cibernético Policial y otras entidades estatales**. Además, establece la necesidad de adoptar estándares internacionales en gestión de riesgos y ciberseguridad, con el fin de mejorar la capacidad de respuesta ante amenazas ciberneticas.

El decreto también resalta la importancia de la educación y sensibilización en seguridad digital, promoviendo la capacitación de servidores públicos y el fortalecimiento de la cultura de seguridad de la información en la ciudadanía. De esta manera, busca garantizar que tanto el sector público como el privado cuenten con herramientas adecuadas para prevenir y mitigar ataques ciberneticos.

► De otro lado, se encuentra en desarrollo la **Estrategia Nacional de Seguridad Digital**, que tiene un enfoque integral que abarca desde la gobernanza hasta la cooperación internacional, adaptándose a las crecientes necesidades del país en un contexto global cada vez más digitalizado, que fue desarrollada por el Gobierno Nacional con apoyo de la OEA. Busca consolidar un entorno digital seguro mediante cinco ejes clave: fortalecimiento de la gobernanza en seguridad digital, protección de infraestructuras críticas, capacitación en ciberseguridad, cooperación internacional y fomento de la innovación tecnológica en seguridad digital. Esta estrategia es esencial para fortalecer la resiliencia digital del país, asegurando que Colombia pueda enfrentar los desafíos de la transformación digital de manera segura y sostenible.

► Por último, se encuentran en trámite en el Congreso de la República dos iniciativas legislativas que buscan establecer una Agencia Nacional de Seguridad Digital que sirva como articuladora del ecosistema de ciberseguridad del país, que son: el **Proyecto de Ley No. 010 de 2023 Senado** "Por la cual se crea la Agencia Nacional de Seguridad Digital y se fijan algunas competencias específicas", y el **Proyecto de Ley No. 023 de 2023 Cámara** "Por la cual se crea la Agencia Nacional de Seguridad Digital y asuntos espaciales y se fijan algunas competencias específicas".

Ambos proyectos de ley buscan fortalecer la gobernanza y la seguridad digital en Colombia, asegurando un marco legal que impulse la protección frente a amenazas ciberneticas en el país. Particularmente, buscan que la Agencia Nacional de Seguridad Digital que se crearía cuente con los recursos financieros y humanos necesarios para atender las necesidades de ciberseguridad del sector público y así atender incidentes y construir capacidades en la administración pública y todo el ecosistema digital de Colombia.

4.3 Perspectivas de corto plazo



Las amenazas, ataques y delitos informáticos seguirán creciendo de manera exponencial y con ello el aumento de los riesgos en el entorno digital para entidades públicas, las empresas y las personas a nivel global. Por ejemplo, de acuerdo con (SONICWALL, 2024), a junio de 2024 el ransomware mostró una tendencia al alza con un aumento del **15%** en Norte América y un **51%** en Latinoamérica. En el caso del malware, el volumen total global de malware aumentó un 30 % en la primera mitad de 2024, registrando un incremento masivo del **92%** solo en mayo. Por lo cual, la ciberseguridad cada vez más será una prioridad para todos los agentes de la sociedad colombiana.



Aunque la ciberseguridad y la seguridad digital son una prioridad para el Gobierno nacional, de acuerdo con lo establecido en el PND 2022-2026 y en la END 2023-2026, es importante que las apuestas planteadas en estos documentos de política pública se materialicen con mayor rapidez y contundencia para fortalecer las capacidades del país en el corto plazo. La nueva Estrategia Nacional de Seguridad Digital tiene un papel importante en esta tarea. Se espera que las acciones de esta estrategia no solo materialicen los grandes objetivos de política ya definidos, sino también que estén enfocadas en los aspectos donde el país tiene mayores oportunidades de mejora y fortalezca la institucionalidad existente. Esto teniendo en cuenta la incertidumbre que existe respecto al futuro del proyecto de ley que está proponiendo la creación de la Agencia de Seguridad Digital y Asuntos Espaciales. Esta estrategia está en desarrollo y se prevé que se publique a principios de 2025.





Asimismo, es necesario fortalecer la construcción de capacidades de ciberseguridad en el ecosistema digital nacional. En ese sentido, el establecimiento de Agencia Nacional de Seguridad Digital jugaría un rol crucial como coordinador de los distintos actores de gobernanza de seguridad digital. De igual manera, es vital establecer partidas presupuestarias para que las entidades públicas puedan adquirir las soluciones de ciberseguridad que requieran para cumplir con el MGSI, la normatividad de protección de datos y para garantizar los derechos de los ciudadanos.



Existe interés y una buena disposición por parte de la banca multilateral y de los organismos internacionales para apoyar a Colombia en el fortalecimiento de la ciberseguridad. Esto es estratégico para lo que implicará, en cuanto a recursos monetarios y asistencia técnica, el desarrollo de las acciones que se planteen en la nueva estrategia nacional de seguridad digital.



La rápida digitalización de las empresas y entidades públicas está impulsando la demanda de especialistas, productos y servicios de ciberseguridad, mejorando las perspectivas del mercado nacional de ciberseguridad. Sin embargo, las limitaciones en cuanto a la oferta de capital humano calificado pueden retrasar el desarrollo del ámbito de la ciberseguridad en el país durante los próximos años.





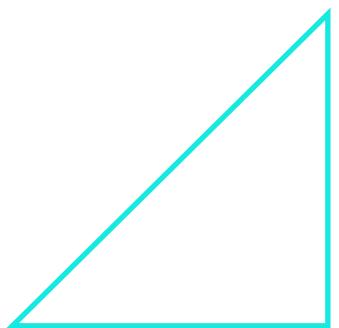
Inteligencia Artificial



5.0

Inteligencia Artificial

5.1 Diagnóstico de país



Durante la última década el ritmo de adopción y uso de la IA ha aumentado exponencialmente, especialmente en los dos últimos años con el lanzamiento de desarrollos de IA generativa. La proliferación de datos y las innovaciones en el procesamiento en la nube y la capacidad de cómputo han dado lugar a la rápida aceleración en el desarrollo y la adopción de la IA a nivel mundial.

Esta rápida adopción de la IA también ha estado impulsada por su amplia gama de beneficios, que incluye desde la automatización de procesos, hasta la ayuda en la toma de decisiones y resolución de problemas complejos, y resulta en mejoras en términos de eficiencia y productividad. **Sin embargo, la velocidad a la que evoluciona esta tecnología implica atender desafíos éticos y sociales** asociados a la apropiación de esta tecnología.

Estos elementos ponen de manifiesto el creciente interés de gobiernos, empresas, academia y sociedad civil en entender y medir el desarrollo y adopción de la IA. Actualmente, existen varios índices que permiten medir cómo están los países en términos de los factores habilitantes de esta tecnología (acceso a Internet, infraestructura tecnológica, datos y talento) y qué se está realizando para desarrollarla y aprovecharla de una manera ética y sostenible, donde el impulso a la investigación y desarrollo, así como la definición de esquemas de gobernanza y el abordaje regulatorio se vuelven esenciales. Puntualmente, para el presente análisis se consideran tres índices:

i)Global AI Index 2024 de Tortoise²⁰**ii)**Government AI Readiness Index 2023 de Oxford Insights²¹**iii)**Índice Latinoamericano de IA (ILIA) 2024 de Cenia²²**Tabla 8. Resultados del Global AI Index 2024**

País	Posición	Puntaje			
		Total	Implementación	Innovación	Inversión
Estados Unidos	1	100	98,67	100,00	91,50
China	2	54	54,00	61,50	57,00
Singapur	3	52	45,00	23,00	43,00
Brasil	30	12	33,67	4,00	21,50
Chile	38	11	31,67	1,00	23,50
Colombia	51	8	26,00	0,50	20,50

Fuente: Elaboración propia a partir de (Tortoise, 2024)**Nota:** Los puntajes de los pilares del índice son cálculos propios (promedio simple) teniendo en cuenta los puntajes de los sub-pilares proporcionados por (Tortoise, 2024)

²⁰ El Global AI Index 2024 aborda el panorama internacional de la IA con respecto a las áreas de talento, infraestructura, entorno operativo, investigación, desarrollo, emprendimientos comerciales y estrategia gubernamental. Los indicadores están agrupados en torno a tres pilares principales y siete subpilares: i) **Implementación**: Los indicadores dentro de este pilar reflejan la puesta en funcionamiento de la IA por parte de las empresas, el gobierno y las comunidades. Este pilar contiene los subpilares de talento, infraestructura y entorno operativo. ii) **Innovación**: Los indicadores dentro de este pilar reflejan avances tecnológicos y avances en metodología que son indicativos de una mayor capacidad para la IA en el futuro. Este pilar contiene los subpilares de investigación y desarrollo. iii) **Inversión**: Los indicadores dentro de este pilar reflejan compromisos financieros y de procedimiento con la IA. Este pilar contiene los subpilares de emprendimientos comerciales y estrategia gubernamental.

²¹ El Government AI Readiness Index 2023 ofrece un panorama del avance de los gobiernos con respecto a la IA a través de tres pilares: Gobierno: considera una visión estratégica de cómo desarrolla y goberna la IA, respaldada por una regulación adecuada y atención a los riesgos éticos (gobernanza y ética). ii) Sector tecnológico: Considera un buen suministro de herramientas de IA por parte del sector tecnológico del país, que debe ser lo suficientemente maduro como para abastecer al gobierno. El sector debe tener una gran capacidad de innovación, respaldada por un entorno empresarial que apoye el espíritu emprendedor y un buen flujo de gasto en I+D. También son cruciales unos buenos niveles de capital humano, es decir, las cualificaciones y la educación de las personas que trabajan en este sector. iii) Datos e infraestructura: Las herramientas de IA necesitan muchos datos de alta calidad (disponibilidad de datos) que, para evitar sesgos y errores, también deben ser representativos de los ciudadanos de un país determinado (representatividad de los datos). Por último, el potencial sin la infraestructura necesaria para alimentar las herramientas de IA y ponerlas a disposición de los ciudadanos.

²² El Índice Latinoamericano de IA 2024 ofrece una visión integral y estructurada sobre el progreso de la IA en América Latina y el Caribe. El ILIA organiza los elementos y variables que inciden en el desarrollo de los ecosistemas de IA en torno a tres dimensiones: i) **Factores habilitantes**: Mide el desarrollo de los elementos que son necesarios para que se desarrollen sistemas de IA. ii) **Investigación, desarrollo y adopción**: Mide el desarrollo del ecosistema de investigación, desarrollo e innovación relacionado a la IA. También considera el nivel de adopción de sistemas tecnológicos en el sector privado. iii) **Gobernanza**: Mide el nivel de desarrollo del entorno institucional con respecto a la IA.

Tabla 9. Resultados del Government AI Readiness Index 2023

País	Posición	Puntaje			
		Total	Gobernanza	Sector Tecnológico	Datos e Infraestructura
Estados Unidos	1	84,80	86,04	81,02	87,32
Singapur	2	81,97	90,40	66,19	89,32
Reino Unido	3	78,57	82,50	68,80	84,42
Brasil	32	63,70	72,44	45,08	73,57
Chile	41	61,95	74,56	40,91	70,38
Colombia	53	57,85	74,98	35,28	63,30

Fuente: Elaboración propia a partir de (Oxford Insights, 2023)

Tabla 10. Resultados del Índice Latinoamericano de IA (ILIA) 2024

País	Posición	Puntaje			
		Total	Factores Habilitantes	Investigación, Adopción y Desarrollo	Gobernanza
Chile	1	73,07	64,60	75,21	83,62
Brasil	2	69,30	52,48	79,17	82,38
Uruguay	3	64,98	60,70	66,68	69,43
Argentina	4	55,77	47,44	56,04	68,73
Colombia	5	52,64	44,46	54,87	62,62
México	6	51,40	48,16	66,20	35,87

Fuente: Elaboración propia a partir de (Cenia, 2024)

A partir de los resultados de estos índices se puede observar que, a pesar de los avances que ha tenido Colombia, en todos los aspectos considerados existe una oportunidad de mejora, incluso en aquellos en los que el país tiene un mejor desempeño ([Ver Tabla 8, Tabla 9 y Tabla 10](#)). El país no solo se está quedando rezagado con respecto a los países líderes y mejor posicionados como Estados Unidos y Singapur, sino también en comparación con los países de la región de América Latina. Según el ILIA 2024, Colombia está en el quinto puesto y hace parte de los países adoptantes de la IA. Chile, Brasil y Uruguay son los países pioneros de la región.

Colombia es un país adoptante de la IA.

Esta categorización que realiza el ILIA 2024 de “adoptante” para Colombia puede considerarse una buena forma de resumir el proceso del país en cuanto a desarrollo, adopción y aprovechamiento de la IA y, en ese sentido, los resultados obtenidos en los diferentes índices. Los puntajes y posiciones intermedias muestran que Colombia: i) cuenta con políticas públicas y está desarrollando estrategias para fomentar el acceso y adopción de esta tecnología; ii) ha comenzado a integrar la IA en diversos sectores de la economía y la sociedad, pero aún no tiene una posición de liderazgo; iii) aunque tiene avances en temas de investigación todavía no está a la escala de los países pioneros.

Así mismo, el análisis comparativo muestra que Colombia tiene fortalezas con respecto a la gobernanza de la IA y la disponibilidad de datos.

No obstante, tiene retos importantes que superar en cuanto a infraestructura tecnológica y otros factores habilitantes como el talento requerido para aprovechar esta tecnología. De igual forma, registra un bajo desempeño con respecto a investigación, innovación y desarrollo. Estas conclusiones se confirman en el Artificial Intelligence Landscape Assessment (AILA) realizado por el Programa de las Naciones Unidas para el Desarrollo (PNUD) en 2024²³, cuyos resultados muestran que Colombia se encuentra en un nivel diferenciador de preparación para desarrollar, adoptar, implementar y utilizar la IA, lo cual significa que ya existen fortalezas y elementos fundamentales de preparación para IA, aún así, también hay oportunidades significativas de mejora para que el país pueda materializar los beneficios potenciales de la IA. **El puntaje de Colombia en esta evaluación fue de 3,4 sobre 5.**



²³ El AILA está enfocado en las necesidades y capacidades del Gobierno como usuario de IA y como habilitador del ecosistema de IA, teniendo en cuenta la importancia del uso ético de IA en el país.

A continuación, se profundiza con respecto al avance del país en estos aspectos fundamentales para la IA.



Gobernanza de la IA²⁴

Colombia registra buenos resultados en el ámbito de la Gobernanza de la IA.

Gobernanza de la IA. En los tres índices analizados la dimensión o las subdimensiones en las cuales el país obtiene los mejores resultados están relacionadas con gobernanza. Colombia fue uno de los primeros países de América Latina en contar con una estrategia nacional para la IA, denominada “*Política Nacional de Transformación Digital e Inteligencia Artificial*” (CONPES 3975 de 2019). Aunque esta política finalizó en 2022, durante el 2025 el DNP publicó el CONPES 4144, “*Política Nacional de Inteligencia Artificial*”, que renueva la visión y objetivos de política pública de IA para el país, con las respectivas acciones y entidades para implementarlos. Esta nueva política tiene en cuenta la “*Hoja de Ruta para el Desarrollo y Aplicación de la Inteligencia Artificial*”, lanzada por el MinCiencias en febrero de 2024, y también los avances realizados por el MinTIC respecto a la IA con su estrategia “*Colombia PotencIA Digital*”.

²⁴ Aunque dependiendo del índice el abordaje de gobernanza puede variar, generalmente este hace referencia a si el país cuenta con una visión estratégica con respecto a la IA y las políticas públicas e institucionalidad para implementarla, la existencia de regulación apropiada y la atención a los riesgos éticos, y la participación en instancias internacionales y la incidencia que se tiene en estos espacios.

De igual forma, en 2019 Colombia acogió las Recomendaciones de la OCDE sobre Inteligencia Artificial de 2019, y en 2021 se adhirió a las Recomendaciones de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) sobre ética en la IA. En este contexto, en 2021 el Gobierno nacional publicó el *Marco Ético para la Inteligencia Artificial*, el cual aborda diversas temáticas vinculadas con la adopción de principios éticos. Con respecto a regulación es importante mencionar que, si bien Colombia aún no tiene una regulación específica, sí cuenta con marcos regulatorios relacionados con los principales habilitadores de la IA como son la protección de datos, la ciberseguridad, la experimentación regulatoria, entre otros. Adicionalmente, actualmente se están tramitando varios proyectos de ley en el Congreso de la República, con los cuales se quiere abordar la regulación de la IA en el país.

Con respecto a la participación en los espacios internacionales, es relevante mencionar que Colombia ha estado participando en las sesiones del Grupo de Trabajo de Gobernanza de IA de la OCDE y ha realizado aportes a los documentos de consulta como, por ejemplo, la actualización de las Recomendaciones sobre IA, que se publicó en 2024. De igual forma, ha participado en las dos cumbres ministeriales organizadas por la UNESCO y el Banco de Desarrollo de América Latina y el Caribe (CAF) sobre la ética de la IA en América Latina y el Caribe (Santiago de Chile 2023 y Montevideo 2024), contribuyendo en la definición de la agenda de trabajo para la región alrededor de las áreas prioritarias de la IA. Asimismo, en 2024 el Gobierno Nacional realizó en Cartagena una cumbre ministerial de Latinoamérica y el Caribe para promover la gobernanza de la IA en la región. El país también ha realizado aportes en los documentos y consultas de la Organización de Naciones Unidas (ONU) y la UIT, entre otros.

Estos avances son confirmados por los resultados del AI and Democratic Values Index (AIDV) 2023, que realiza una evaluación comparativa de los países sobre cómo gobernar la IA y por qué es necesaria. De acuerdo con el AIDV 2023, Colombia está en la cuarta posición y hace parte del grupo de países que están en el primer nivel (alto) de los cinco niveles considerados. Colombia está cumpliendo totalmente la mayoría de los aspectos considerados (ocho de doce), dentro de los cuales se destacan que el país ha suscrito las recomendaciones de la OCDE y de la UNESCO, así como la Declaración Universal de los Derechos Humanos. También se destaca que el país cuenta con un proceso de participación pública significativa en el desarrollo de una política nacional de IA y existe material sobre las políticas y prácticas de IA del país a disposición del público.



A pesar de estos avances, **Colombia aún necesita fortalecer la gobernanza alrededor de la IA.** De acuerdo con (DNP, 2024), el país carece de un marco formal e institucional de gobernanza para el desarrollo, adopción y aprovechamiento de sistemas de IA. Aunque el Gobierno Nacional ha creado instancias de gobernanza, como la Mesa Interinstitucional de IA liderada por la Presidencia de la República y el DNP, estas instancias no cuentan con un instrumento formal que determine su alcance, su posición institucional, ni su integración estratégica con otros modelos de gobernanza subnacionales y supranacionales para asuntos digitales, éticos o productivos (por ejemplo, el Comité Nacional de Infraestructura de Datos o el Comité Nacional de Seguridad Digital).

Asimismo, **a pesar de que Colombia ha demostrado un compromiso con el uso ético y transparente de la IA, aún enfrenta desafíos para asegurar su implementación efectiva** (PNUD, 2024). En este sentido, el (DNP, 2024) afirma que, **los mecanismos existentes a nivel nacional para verificar y hacer cumplir los marcos éticos de IA y su catálogo de principios son insuficientes.** Lo anterior, teniendo en cuenta que los marcos éticos y recomendaciones para el uso de IA acogidos por Colombia no contemplan la generación de capacidades institucionales y técnicas para construir mecanismos concretos que permitan la verificación, medición o seguimiento al cumplimiento de los principios éticos en la implementación de soluciones o desarrollos de la IA.

De igual forma, **el país requiere un mejor y mayor abordaje de los riesgos y efectos no deseados de la IA, de tal forma que el desarrollo y adopción de la IA no resulte en un aumento de la desigualdad, la exclusión social y afectación ambiental.** Por ejemplo, de acuerdo con (PNUD, 2024), Colombia no ha implementado suficientes medidas para promover y proteger la igualdad de género en las diferentes etapas del ciclo (diseño, desarrollo y uso) de las herramientas y sistemas de IA.

Colombia también debe fortalecer su participación y vinculación en los escenarios y organismos internacionales que están abordando y liderando las discusiones alrededor de la IA, especialmente con respecto a la definición de estándares para la IA como, por ejemplo, la participación en los procesos de definición de normas ISO. De acuerdo con los resultados del ILIA 2024, Colombia actualmente no está participando en estas instancias.



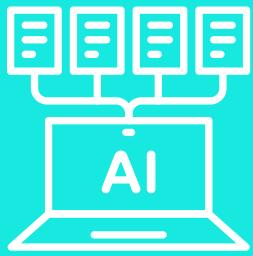
Factores habilitantes para la IA²⁵

Actualmente, el principal desafío de Colombia con respecto a la IA está en desarrollar y fortalecer los habilitadores de esta tecnología. Esto queda en evidencia en las dimensiones/pilares o subdimensiones/subpilares de los tres índices analizados que contemplan el estado del país en cuanto a estos factores. Por ejemplo, en el caso del Global AI Index 2024 en el pilar denominado “*Implementación*”, Colombia obtiene un puntaje de 26,00 puntos de 100 posibles, que lo ubican en posiciones por debajo no solo de los países líderes sino también de países de la región de ALC como Brasil y Chile. Estos resultados se confirman con el ILIA 2024, el cual destaca que la dimensión denominada “*Factores habilitantes*” es en la que Colombia obtiene el menor puntaje (44,46 puntos de 100 posibles), este puntaje lo ubica en la séptima posición de los 19 países considerados y muestran las oportunidades de mejora del país en cuanto infraestructura tecnológica, datos y capital humano para la IA.

A pesar de los avances, **en Colombia persisten las brechas en el acceso al servicio de Internet, principalmente en las zonas apartadas del país.** De acuerdo con (DANE, 2024), el 36,1% de los hogares colombianos no tienen acceso a Internet fijo o móvil, y en los centros poblados y zonas rurales dispersas este porcentaje asciende a 58,6%. El costo de servicio es la principal razón por la cual no se tiene acceso. El 49,7% de los hogares que no tenían el servicio de acceso a Internet indicaron que la razón por la cual no lo tienen es porque lo consideran muy costoso. El costo del servicio es aún más relevante si se tiene en cuenta la tenencia de dispositivos como el computador (de escritorio o portátil) o tableta. Según (DANE, 2024), el 66,0% de los hogares no tienen uno de estos dispositivos y para el 58,0% de estos hogares la principal razón por la que no lo tienen es porque lo consideran demasiado costoso.

Asimismo, **Colombia tiene un rezago en cuanto a la velocidad de descarga de Internet, principalmente en Internet móvil.** Según el ILIA 2024, en Colombia la velocidad de descarga en Internet móvil es en promedio 12 Mbps más lenta que la media regional y el avance en la cobertura de la tecnología 5G es aún bajo. En el caso del Internet fijo, de acuerdo con el ILIA 2024, si bien en el país el promedio de la velocidad de descarga es superior al promedio regional, está por debajo de los países líderes como Chile (265,12 Mbps).

²⁵ Aunque los indicadores los destacan y agrupan de diferente manera, cuando se hace referencia a los factores habilitantes se hace mención a principalmente a cuatro aspectos: i) acceso, asequibilidad y calidad del servicio de Internet (fijo y móvil); ii) infraestructura tecnológica para el almacenamiento y procesamiento de datos (por ejemplo, data centers, supercomputadores y nube); iii) disponibilidad de datos de calidad; y iv) talento o capital humano para desarrollar y adoptar la IA. Todos estos aspectos son esenciales para que se pueda desarrollar y adoptar la IA.



En el país existe una baja capacidad cómputo para soportar el desarrollo de sistemas y aplicaciones de IA.

Según el ILIA 2024, Colombia con un puntaje de 16,33 puntos de 100 posibles registra un nivel menor a la media regional de ALC (21,76 puntos). Aunque el país en cuanto a los servicios de Nube registra un puntaje similar al de la región y supera levemente el promedio, en materia de Capacidad de infraestructuras de computación de alto rendimiento tiene el desafío de desarrollar centros de datos certificados, IXP y servidores de Internet seguros, los cuales presentan bajos puntajes en comparación con el promedio regional de ALC. Por ejemplo, para el caso de centros de datos certificados, mientras el promedio regional de ALC es de 18,06 puntos, el puntaje de **Colombia es de 11,12 puntos**.

Colombia se destaca por tener un ecosistema avanzado de datos, pero aún tiene retos importantes en cuanto a la calidad de los datos, así como en el aprovechamiento de estos en las entidades públicas.

Resultados similares se obtienen en el Government AI Readiness Index 2023. En el pilar denominado “Disponibilidad de datos”, Colombia está seis puntos por encima del promedio de la región de ALC (56,52). Estos resultados indican que el país cuenta con disponibilidad de datos, capacidades para su administración y un marco de gobernanza robusto. Sin embargo, según (DNP, 2024), en Colombia se evidencia una baja disponibilidad de datos de calidad y con representatividad para el desarrollo de sistemas de IA. Asimismo, esta entidad señala que el país presenta falencias en la interoperabilidad de datos que dificultan el uso de datos para el desarrollo y aprovechamiento de sistemas de IA. A pesar de que el país tiene una plataforma de interoperabilidad (X-Road), las entidades públicas no se han visto beneficiadas por el servicio dispuesto. Dificultad a la que se le suma que las entidades públicas, especialmente las del orden subnacional, tienen bajas capacidades para usar y aprovechar datos para la toma de decisiones.

De acuerdo con el ILIA 2024, en la subdimensión de datos, **Colombia** con un puntaje de **51,74** puntos está por encima del promedio regional de ALC en casi 16 puntos.

El país está mejorando en cuanto a alfabetización y talento humano relacionado con la IA. De acuerdo con el ILIA 2014, Colombia se encuentra en un desarrollo intermedio en estos aspectos. Tiene avances importantes, pero aún con un margen de mejora. Estos resultados se confirman con los resultados de los otros índices. En el subpilar “*Talento*” del Global AI Index 2024, Colombia se ubica en el puesto 53 de las 83 economías analizadas.

En el caso Government AI Readiness Index 2023, para el subpilar de “*Capital humano*”, **Colombia tiene un puntaje de 46,27 puntos**, que está por encima del promedio regional de ALC en casi 10 puntos y no está tan rezagada frente a los países líderes como Estados Unidos (69,20) y Singapur (68,20).

Colombia tiene un rezago importante en las habilidades de sus ciudadanos con respecto al inglés. Según los resultados del ILIA 2024, con respecto a la alfabetización de IA, que aborda aspectos como la educación temprana en ciencia y la educación temprana en IA, el país registra puntajes por encima o cerca al promedio regional de ALC; no obstante, con respecto a la habilidad de inglés, el país presenta un rezago importante con respecto a los otros países de la región. En este caso, el país está casi 11 puntos por debajo del promedio regional de ALC que es de 48,96.

promedio regional. Aunque cuenta con programas de magíster en IA con acreditación y programas de magíster en IA en universidades del Ranking QS, carece de programas de doctorado en IA con estas características. Adicionalmente, similar al resto de la región, Colombia enfrenta el desafío de retener el talento especializado en IA. Se evidencia una tendencia a la fuga de cerebros. De acuerdo con el ILIA 2024, España y Estados Unidos siguen destacándose como los principales destinos de los autores que publican en Colombia.

En cuanto a la formación profesional en IA, Colombia requiere de más talento avanzado. Según el ILIA 2024, la penetración relativa de competencias asociadas a la IA en la fuerza de trabajo y el nivel de Licenciados en STEM en el país está por encima del promedio regional de ALC. Por ejemplo, en el caso de los licenciados en STEM, Colombia está 12,22 puntos por encima del promedio regional de ALC (43,49). No obstante, en materia de Talento humano avanzado, el país se encuentra por debajo del



Investigación, desarrollo e innovación (I+D+i) para la IA²⁶

Otro de los mayores desafíos de Colombia para la adopción de la IA está relacionado con la investigación, el desarrollo y la innovación. De acuerdo con los índices revisados, una de las dimensiones/pilares y subdimensiones/subpilares en las cuales el país no tiene un buen desempeño son aquellas que abordan estos aspectos, especialmente en cuanto a desarrollo e innovación. Si bien se han presentado avances, Colombia se caracteriza por tener bajos niveles de inversión pública y privada en investigación y desarrollo entorno a la IA, escasos emprendimientos y desarrollos de esta tecnología a nivel nacional, así como pocos incentivos para fomentar la innovación y varias oportunidades de mejora en la generación de conocimiento científico con respecto a la IA.

Colombia ha mejorado en cuanto a producción científica, pero no tanto en el impacto de esta. Según el ILIA 2024, Colombia se destaca en el área de Investigación, con subindicadores como publicaciones en IA que superan por 20 puntos la media regional de ALC (52,34 puntos), así como con un ecosistema de investigadores especializados en IA bastante robusto, destacando aspectos como la proporción de investigadoras autoras en IA (68,23 puntos) que supera en 10 puntos al promedio regional. No obstante, el número de publicaciones IA aún está por debajo de los países líderes como Chile y Brasil, y la productividad de los investigadores²⁷ y el impacto de esta producción científica²⁸ están por debajo del promedio regional.

²⁶ Los diferentes índices abordan los avances del ecosistema de investigación, desarrollo e innovación (I+D+i) a nivel público, privado y académico, haciendo énfasis en la capacidad de los países para generar nuevo conocimiento entorno a la IA, así como en los progresos en desarrollos e innovaciones relacionados con esta tecnología, que incluye, entre otros aspectos, el volumen de inversiones, patentes, el número de empresas de IA y startups, y el entorno emprendedor del país.

²⁷ Contabiliza el promedio anual de publicaciones por autor/a en los últimos cinco años -con el fin de evaluar la intensidad de publicación en el campo de la IA en ese período.

²⁸ Se refiere al promedio anual de citas de trabajos de investigación en el total de publicaciones y conferencias en este campo en los últimos cinco años.

En Colombia persiste una baja inversión pública y privada en investigación y desarrollo en torno a la IA.

Aunque, de acuerdo con el ILIA 2024, el país supera por 18 puntos la media de ALC (38,97 puntos) el valor de la inversión privada para la IA, este aún está por debajo de países como Chile y Uruguay en más de 50 puntos. Adicionalmente, el gasto en investigación y desarrollo en proporción al PIB del país (0,29%) es bajo no solo con respecto a los países líderes en la región de ALC como Brasil (1,17%), sino también en comparación a la media regional (0,33%). Resultados similares arroja el Government AI Readiness Index 2023 para el subpilar “Innovación”, el cual está incluido en el pilar de “Sector tecnológico” y considera las variables en análisis, en donde Colombia con una puntuación de 38,27 está por debajo del promedio de la medición (42,03) y también de los países mejor posicionados en este índice: Estados Unidos (89,10) y Singapur (75,61).

El país no cuenta con la madurez y la capacidad necesaria para innovar en bienes y servicios basados en IA.

Esto queda en evidencia en los resultados del Global AI Index 2024 en el pilar de “Innovación”, en donde Colombia no solo está por debajo de países líderes como Estados Unidos y China, sino también de algunos países de la región. Para el subpilar “Desarrollo”, que se enfoca en la creación de nuevos modelos de IA y la aplicación de la tecnología de IA en patentes de otros campos, el país obtuvo un puntaje de 1 de 100 posibles. Por ejemplo, con respecto a las patentes, de acuerdo con (DNP, 2024) teniendo en cuenta los datos de Organización Mundial de Propiedad Intelectual (WIPO), para los períodos 2019 y 2023 Colombia solo tuvo una solicitud de patentes en IA y se situó por debajo del promedio regional, mientras que Brasil registró (305), México (86) y Argentina (8).

En este sentido, los resultados del Government AI Readiness Index 2023 para el subpilar “Madurez”, el cual está incluido en el pilar de “Sector tecnológico” y considera variables relacionadas con la presencia de empresas unicornios y producción de bienes y servicios TIC, muestran que Colombia con una puntuación de 21,29 está por debajo de los países mejor posicionados en este índice como Estados Unidos (84,77) y también de países en ALC como Brasil (34,01) y Chile (34,72). Resultados similares arroja el ILIA 2024, a partir del cual se encuentra que, si bien Colombia cuenta con empresas unicornio (2,70 puntos) está casi ocho puntos por debajo del promedio y en materia de desarrollo de aplicaciones muestra un puntaje de 66,96, ocho puntos bajo la media. Aunque Colombia ha realizado esfuerzos para generar un mejor entorno para el emprendimiento y con esto mejorar el desarrollo y creación de emprendimientos relacionados con IA, de acuerdo con (KPMG, 2024), a corte de 2023 el país solo contaba con 31 startups de IA en el mercado, ubicándose por debajo de países como Chile con (56) y Brasil con (198). Adicionalmente, según (PNUD, 2024), en Colombia el desarrollo de startups y scaleups tecnológicas presenta una gran desigualdad territorial, concentrándose principalmente en Bogotá, Medellín y Cali.





Adopción de la IA en empresas y entidades públicas²⁹

Aunque se destaca en ALC, Colombia tiene oportunidades de mejora en cuanto a la adopción de la IA en las empresas y entidades públicas. Según el ILIA 2024, Colombia hace parte del grupo de países con alta adopción de esta tecnología con 71,20 puntos, junto con México que lidera este subdimension (con 94,56 puntos), Brasil (90,27), Argentina (73,36) y Chile (72,66). Sin embargo, la región de ALC aún se encuentra en el proceso de adopción de esta tecnología y, a pesar de estos avances, en el país aún existen oportunidades de mejora y enfrenta desafíos para tener una adopción más rápida y generalizada tanto en el sector privado como en el público.

En Colombia el uso y aprovechamiento de tecnologías digitales emergentes como la IA en las empresas del país aún es bajo. De acuerdo con la encuesta Pulso Empresarial del DANE, para el reporte de octubre - noviembre de 2022, si bien las empresas de los diferentes sectores económicos están utilizando diferentes tecnologías de IA como, por ejemplo, tecnologías que automatizan flujos de trabajo o asisten en la toma decisiones, estos porcentajes son muy pequeños. Según esta encuesta, el porcentaje de empresas que reportó no haber utilizado ninguna de las tecnologías de IA consideradas fue del 91%, destacándose el sector comercio con 94,5%, el cual estuvo seguido por el sector construcción (93,7%), industria manufacturera (91,3%) y sector servicios (86,8%) (DANE, 2022).

²⁹ Hace referencia principalmente al uso y aprovechamiento de la IA en los procesos, operaciones, desarrollo de productos o prestación de servicios de las entidades públicas y las empresas.



Las principales barreras para la adopción de la IA en las empresas del país son aquellas relacionadas con altos costos, falta de capital humano, o la no utilidad de su uso.

De acuerdo con la encuesta Pulso Empresarial del DANE, para el reporte de octubre - noviembre de 2022, las tres razones por las cuales las empresas no utilizan alguna de las tecnologías de IA que tuvieron una mayor proporción de respuestas son: i) las tecnologías de IA no son útiles para la empresa (42,5%), ii) los costos son demasiado altos (33%), y iii) la empresa no cuenta con la experiencia relevante para su uso (30,7%). En este sentido, por ejemplo, el 49,5% de las empresas del sector comercio encuestadas consideran que las tecnologías de IA no son útiles para su empresa (DANE, 2022).

A pesar de los avances, en el país existe una baja adopción de sistemas de IA en las entidades públicas. Aunque en términos de Gobierno Digital el país está bien posicionado a nivel internacional (por ejemplo, según el ILIA 2024 en el subíndicador Gobierno Digital, Colombia está por encima del promedio de ALC en 13 puntos (69,65)) y esto es una base importante para impulsar procesos de transformación en las entidades públicas basados en IA, cuando se profundiza en el uso de esta tecnología se encuentra que la adopción de la IA aún es baja, principalmente en las entidades subnacionales y aquellas entidades que no son del poder ejecutivo.

Según las respuestas dadas por las entidades públicas en 2023 al Formulario Único de Reporte de Avances de la Gestión (FURAG), de las 234 entidades públicas del orden nacional consideradas solo el 32,9% afirmó haber utilizado IA como tecnología emergente en procesos de innovación digital. En el caso de las entidades del orden subnacional este porcentaje fue tan solo del 2,3% de las 5.786 entidades públicas consideradas. Asimismo, de acuerdo con (Gutiérrez, J.D., Muñoz-Cadena, S., & Castellanos-Sánchez, M., 2023), que recopilaron y caracterizaron información respecto del uso y adopción de Sistemas Automatizados de Decisión (SDA) en el sector público colombiano, para el país se encontraron 113 casos de uso de este tipo de sistemas.

De acuerdo con sus resultados, las entidades públicas identificadas corresponden en su mayoría al poder ejecutivo (93%); el poder judicial y las entidades de control, corresponden a 4% y 3%, respectivamente.

Al igual que en el sector privado, **Colombia debe fortalecer el capital humano del sector público con respecto a las tecnologías digitales para aprovechar al máximo el potencial de la IA**. Como lo indica (PNUD, 2024), aunque en general se identifica un conocimiento general sobre el potencial de la IA en el gobierno, se requieren programas de capacitación en IA y la atracción de talento especializado en IA. Por lo cual, también es necesario que Colombia invierta en la formación y el desarrollo de capacidades en IA de los servidores públicos.

Por otra parte, de acuerdo con (DNP, 2024), **en Colombia los instrumentos de compra pública siguen siendo poco usados y, en especial, el esquema de contratación pública de tecnología asociado a la IA aún no ha sido muy explorado y tiene oportunidades de mejora para promover la concurrencia de ofertas**.

Por ejemplo, aunque el país cuenta con la herramienta “*Tienda Virtual del Estado Colombiano*”, que es la herramienta en línea del Sistema de Compra Pública para adquisición de bienes y servicios a través de mecanismos de acuerdos marco o agregación de la demanda, para el año 2022 solo el 38% de la contratación se había materializado mediante estos acuerdos con la compra de servicios de conectividad, servicios de nube pública y privada, compra y alquiler de computadores y periféricos, Software Empresarial y Software.



5.2 Políticas Públicas y normatividad

En Colombia, las políticas públicas relacionadas con IA y el manejo de grandes volúmenes de datos (Big Data) serán clave para promover la adopción y desarrollo de esta tecnología, así como su uso ético y responsable. En ese sentido, las iniciativas del Gobierno deben estar orientadas a garantizar la protección de los derechos ciudadanos, fomentar la innovación tecnológica y fortalecer la competitividad del país en el contexto de la transformación digital. Asimismo, a la adopción transversal de esta tecnología en la administración pública y los distintos sectores económicos.

Con esto en mente, aunque no hay una ley que regule propiamente la IA en Colombia, si existen varios documentos de política pública relevantes, así como normatividad tangencial que resulta relevante para analizar el estado de esta tecnología en el sistema jurídico colombiano.

Documentos CONPES

➤ El documento **CONPES 3920 de 2018**, que establece la Política Nacional de Big Data, tiene como objetivo potenciar el uso de grandes volúmenes de datos para la toma de decisiones informadas y la mejora de la competitividad en el sector público y privado. Esta política busca optimizar áreas clave como la salud, la educación, la agricultura y la seguridad, y contribuir al desarrollo económico sostenible, a través del uso de analítica de datos.

Para ello, propone la creación de un marco normativo que permita el uso ético y responsable de los datos masivos, asegurando la protección de los derechos de los ciudadanos y promoviendo la transparencia en el manejo de la información. Además, plantea la inversión en infraestructuras de datos avanzadas, como plataformas para analítica predictiva y la toma de decisiones en tiempo real. De igual manera, promueve la creación de centros de datos y redes de alta velocidad que permitan la gestión eficiente de Big Data a nivel nacional.

En el ámbito educativo, el CONPES 3920 también propone programas de formación continua en ciencia de datos y análisis de Big Data para generar una fuerza laboral especializada.

➤ El **CONPES 3975 de 2019** define la Estrategia Nacional de Transformación Digital e Inteligencia Artificial, que busca impulsar la modernización digital del país. Esta estrategia busca posicionar a Colombia como líder en la revolución digital, fomentando la innovación tecnológica y el fortalecimiento de la infraestructura digital, mientras aprovecha la inteligencia artificial para mejorar la calidad de vida de los ciudadanos y aumentar la competitividad del país. La digitalización de los servicios públicos y privados es uno de los pilares centrales de esta política, particularmente en sectores estratégicos como la salud, la educación, el transporte y la administración pública. La integración de soluciones basadas en IA en estos sectores pretende optimizar los procesos, mejorar la toma de decisiones y ofrecer una experiencia más eficiente y accesible a los ciudadanos.

Desde una perspectiva normativa, el CONPES 3975 promueve la creación de un marco de política pública actualizado para facilitar la adopción de tecnologías emergentes, garantizando la protección de los datos personales y el respeto a los derechos fundamentales. Además, subraya la importancia de la transparencia y la equidad en el uso de los algoritmos, así como la necesidad de garantizar la auditoría y el control de los sistemas automatizados. Este enfoque normativo busca que la IA sea implementada de manera ética y responsable, sin comprometer los principios de privacidad y derechos humanos. Además, se hace especial énfasis en la formación y capacitación en nuevas tecnologías, incluyendo la inteligencia artificial, en todos los niveles educativos, desde la educación básica hasta la formación técnica y profesional. Valga la pena mencionar, que, a pesar de estos lineamientos, en la actualidad no se ha expedido una ley que se encargue del tema de IA.

➤ El CONPES 4144 de 2025 actualiza los documentos anteriores y define la nueva Política Nacional de Inteligencia Artificial. Este se articula en torno a seis ejes estratégicos: 1) Ética y gobernanza, para fortalecer estos mecanismos y garantizar el uso y desarrollo responsable de IA, 2) Datos e infraestructura, promoviendo el fortalecimiento de la infraestructura tecnológica y la disponibilidad de datos necesarios para el desarrollo de IA, 3) Investigación, desarrollo e innovación (I+D+i) en sistema de IA para promover la productividad y beneficios concretos en el país, 4) el desarrollo de capacidades y talento digital, 5) la mitigación de riesgo relacionados con sistemas de IA, y 6) el uso y adopción de sistemas de IA en entidades pública, sector privado y los territorios.

Con esto en mente, el CONPES 4144 busca generar capacidades para promover la investigación, desarrollo, adopción y aprovechamiento ético y sostenible de sistemas de IA, y así impulsar la transformación digital, económica y social de Colombia a 2030. Asimismo, establece un presupuesto de 479.273 millones de pesos del Presupuesto General de la Nación, para llevar a cabo los seis ejes estratégicos ya mencionados. Además, esta política contará con el liderazgo del DNP, MinTIC, MinCiencias, MEN, DAPRE y MinTrabajo.

Documentos de política pública

➤ El Marco Ético para la Inteligencia Artificial en Colombia busca garantizar que la Inteligencia Artificial se utilice de manera responsable, respetando los derechos humanos, la privacidad y la dignidad de las personas. Entre los principios clave se destacan la justicia y la no discriminación, la protección de datos personales, la transparencia en los algoritmos, la sostenibilidad, la responsabilidad y control humano y el beneficio social y bien común. Además, se enfatiza que los sistemas de IA deben ser explicables y auditables, lo que significa que los ciudadanos deben poder comprender cómo se toman las decisiones automatizadas, garantizando que los resultados sean justos, transparentes y no sesgados.

➤ **La Hoja de Ruta para el Desarrollo y Aplicación de Inteligencia Artificial** de MinCiencias es un documento estratégico que orienta el desarrollo de la IA en Colombia, y tiene como propósito fomentar el uso de estas tecnologías en sectores como la salud, la educación, la agricultura y el transporte posicionando al país como un líder regional en innovación tecnológica.

Este plan establece objetivos relacionados con la capacitación y desarrollo de talento humano especializado en IA, el fomento de la investigación y desarrollo tecnológico, la creación de ecosistemas de innovación, el impulso a la cooperación entre los sectores público y privado para el desarrollo de soluciones tecnológicas avanzadas y el establecimiento de incentivos y apoyos para empresas que adopten o desarrollen soluciones basadas en IA, con el fin de facilitar la transición digital de la industria colombiana y fomentar la creación de startups tecnológicas que contribuyan al ecosistema innovador del país. En su implementación, también se contempla el fortalecimiento de la infraestructura digital necesaria para facilitar el uso de la IA, así como la creación de marcos regulatorios que favorezcan la innovación responsable y ética.

➤ La Estrategia Colombia PotencIA Digital establece la construcción de centros y microcentros virtuales de IA, con el objetivo de construir capacidades regionales en esta tecnología y de esa manera fortalecer los ecosistemas locales de innovación digital, así como promover el cierre de la brecha digital. Adicionalmente, en el marco de esta, se desarrolla la iniciativa “Territorios IA”, que busca fortalecer las capacidades digitales de la administración pública, a través de la adopción de solución de IA en autoridades territoriales.

Normativa

6699

Como mencionamos, aunque no hay una ley o una normativa concreta que regule los sistemas de IA en el país, sí hay algunos documentos normativos relevantes, aunque tangenciales, para entender el desarrollo de IA en nuestro sistema jurídico, a saber:

➤ La SIC emitió la **Circular Externa 002 de 2024**, la cual establece directrices para regular las prácticas comerciales y el uso de tecnologías digitales que puedan afectar los derechos de los consumidores. En este contexto, hace especial énfasis en la protección de datos personales y la transparencia en el uso de algoritmos, garantizando que las decisiones automatizadas sean equitativas y no discriminen a los consumidores. La circular establece principios sobre la responsabilidad de las empresas que emplean IA en sus productos y servicios, y exige que los consumidores sean debidamente informados sobre el uso de estas tecnologías en la toma de decisiones.

➤ De otro lado, la **Circular Externa 003 de 2024** de la SIC establece directrices clave para regular el uso de plataformas digitales y el comercio electrónico en Colombia, enfocándose en la protección de los derechos de los consumidores. Resalta la necesidad de que las empresas proporcionen información clara y veraz sobre productos y servicios, garantizando transparencia en las condiciones de compra, precios y políticas de devolución.

Además, la circular establece obligaciones específicas para las plataformas de terceros (como marketplaces), que deben asegurarse de que los vendedores cumplan con las normativas de protección al consumidor, evitando prácticas comerciales desleales. Se enfatiza la importancia de la seguridad digital, la protección de datos personales y el uso ético de tecnologías emergentes como la inteligencia artificial en la personalización de ofertas y publicidad, con el objetivo de promover un entorno de confianza en el comercio digital y prevenir el fraude electrónico.

➤ El **Decreto 1732 de 2021** establece un marco normativo para el impulso de modelos de negocio innovadores en Colombia, facilitando la creación de sandboxes regulatorios. Estos espacios permiten a las empresas probar nuevas tecnologías, como la IA, en un entorno controlado, sin las restricciones de los marcos regulatorios tradicionales. El objetivo es flexibilizar las regulaciones para empresas emergentes, promoviendo la innovación responsable en sectores como Fintech y otras soluciones tecnológicas disruptivas. Así las cosas, esta normatividad habilitaría el desarrollo de sandbox de IA en el país.

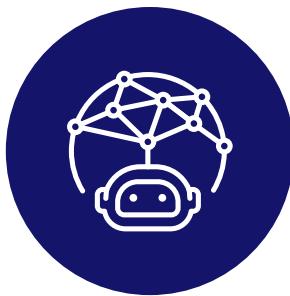
➤ El **Decreto 767 de 2022** regula las políticas de ciberseguridad y protección de datos en Colombia, estableciendo las directrices para garantizar la seguridad en la infraestructura digital del país. Este decreto es particularmente relevante en el contexto del uso de tecnologías avanzadas como IA, ya que establece medidas para proteger los sistemas críticos y los datos personales.

A su vez, incluye disposiciones sobre la gestión de incidentes cibernéticos y promueve la cooperación internacional en ciberseguridad.

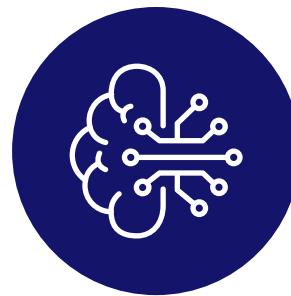
➤ El **Decreto 1263 de 2022** establece directrices adicionales para la regulación de la inteligencia artificial en Colombia, enfocándose en la seguridad y la ética de los sistemas automatizados. Este decreto busca crear un marco normativo que fomente la innovación tecnológica sin comprometer principios como la transparencia, la no discriminación y la rendición de cuentas. Además, establece la necesidad de una supervisión constante de las tecnologías de IA implementadas en el país.



Por último, el Congreso de la República ha avanzado en el trámite de varios proyectos de ley relacionados con IA. Estos buscan abordar una gran variedad de temas, desde el uso e implementación ético de IA, hasta su relación con el trabajo, derechos de autor o responsabilidad penal. Algunos de los más relevantes son:



Proyecto de Ley No. 059 de 2023 Senado
"Por medio de la cual se establecen los lineamientos de política pública para el desarrollo, uso e implementación de inteligencia artificial y se dictan otras disposiciones"



Proyecto de Ley No. 091 de 2023 Senado
"Mediante la cual se establece el deber de información para el uso responsable de la inteligencia artificial en Colombia y se dictan otras disposiciones"



Proyecto de Ley No. 130 de 2023 Senado
"Por medio de la cual se crea la armonización de la inteligencia artificial con el derecho al trabajo de las personas"



Proyecto de Ley No. 255 de 2024 Senado
"Por la cual se establecen lineamientos de uso de inteligencia artificial para mejorar la eficiencia en disminución de siniestros viales y sus costos, automatizando los procesos de análisis y control de riesgos de siniestralidad vial en tiempo real con IA"



Proyecto de Ley No. 005 de 2024 Cámara
"Ley de inteligencia artificial ética y
sostenible para el bienestar social"



Proyecto de Ley No. 113 de 2024 Cámara
"Por medio de la cual se modifica el
Estatuto Tributario Nacional, creando
incentivos tributarios para que las
empresas capaciten a sus empleados en
inteligencia artificial (IA) y se dictan otras
disposiciones"



Proyecto de Ley No. 154 de 2024 Cámara
"Por la cual se define y regula la inteligencia
artificial, se ajusta a estándares de
derechos humanos, se establecen límites
frente a su desarrollo, uso e
implementación se modifica parcialmente
la ley 1581 de 2012 y se dictan
otras disposiciones"



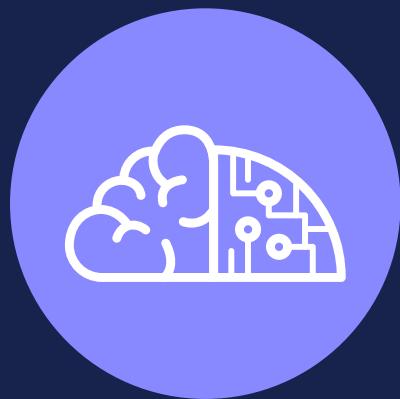
Proyecto de Ley No. 293 de 2024 Senado
"Por medio del cual se establecen
lineamientos para el entrenamiento de
modelos o sistemas de inteligencia
artificial (IA) y se define la gestión colectiva
obligatoria de algunas formas de uso de
obras protegidas por derechos de autor y
se dictan otras disposiciones"

“

Por último, MinCiencias y MinTIC han mencionado que se encuentran trabajando conjuntamente en un Proyecto de Ley "Por medio de la cual se regula la Inteligencia Artificial en Colombia para garantizar su desarrollo ético y sostenible", que sería radicado en el Congreso de la República en el primer semestre de 2025.

”

5.3 Perspectivas de corto plazo



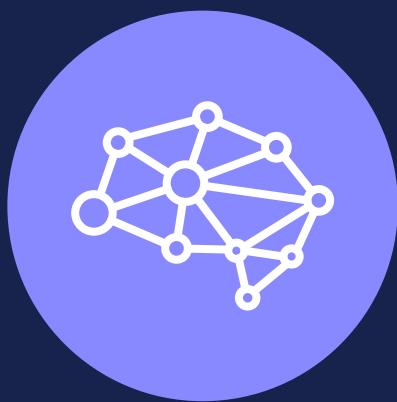
Como lo plantea el CONPES 4144 de 2025, “Colombia presenta bajas capacidades para la investigación, desarrollo, adopción y aprovechamiento ético y sostenible de sistemas de IA en asuntos estratégicos a nivel social, económico y ambiental.” (DNP, 2024). Sin embargo, el abordaje conceptual (factores habilitantes, adopción, riesgos y efectos no deseados) y la propuesta de objetivos y acciones de esta política responden a estas necesidades del país. Por lo cual, con su publicación, el Gobierno Nacional confirma su compromiso para fortalecer las capacidades del país con respecto a la IA y evitar unos mayores rezagos con respecto a los avances y aprovechamiento de esta tecnología, que se están experimentando a nivel mundial. Esta política cumplirá con uno de los principales objetivos de la END de Colombia 2023-2026.



Es relevante promover la adopción de una política pública transversal de IA, que permita al país desarrollar sus capacidades, sin que medien regulaciones que restrinjan injustificadamente la adopción de esta tecnología en el país. En ese sentido, se hace relevante la promoción de medidas que incentiven la inversión en IA, así como en los habilitadores digitales necesarios. Adicionalmente, las iniciativas legislativas deberían acotarse a los lineamientos que incluye el CONPES 4144, así como la Hoja de Ruta del MinCiencias.



La IA es una tecnología de propósito general que puede ayudar al país a enfrentar sus grandes desafíos a nivel económico, social y ambiental. Por lo cual, se espera que las acciones de la nueva política se enfoquen en apuestas que en el corto plazo fortalezcan los habilitadores e impulsen la adopción de la IA en varios sectores socioeconómicos y en los diferentes territorios del país. El aprovechamiento de iniciativas que ya están en marcha como los centros de IA que está desarrollando el MinTIC serán estratégicos en este propósito.



Colombia tiene acceso a redes globales, así como apoyo de la banca multilateral (por ejemplo, la CAF) y de organizaciones internacionales como la OCDE y la UNESCO, que serán claves para la implementación de la nueva política nacional de IA, así como para discutir, aportar y participar en asuntos y proyectos estratégicos para que los beneficios de la IA se pueden aprovechar en el país y en la región de ALC, teniendo en cuenta los riesgos y efectos no deseados.



El fortalecimiento de la gobernanza de la IA, y una gobernanza desde el conocimiento, deberá ser una prioridad en el país. Además de una mayor articulación y coordinación en el desarrollo de iniciativas por parte del Gobierno Nacional, que se espera avance con la expedición de la política de IA, también deberá avanzarse en las discusiones al interior del Congreso de la República alrededor de los diferentes proyectos de ley en curso, así como en las conversaciones de las entidades del Estado con la academia, el sector privado, y las organizaciones de la sociedad civil para que el país avance en una consolidación de la visión con respecto a la IA, su desarrollo, adopción y regulación. En este último caso, debe avanzarse en políticas públicas que equilibren innovación y seguridad, promoviendo la confianza en el uso de la IA.

Siglas y Abreviaturas

4G – Tecnología móvil de cuarta generación

5G – Tecnología móvil de quinta generación

AILA – Artificial Intelligence Landscape Assessment

AIDV – AI and Democratic Values Index

ALC – América Latina y el Caribe

BID – Banco Interamericano de Desarrollo

CAF – Corporación Andina de Fomento

Cenia – Centro Nacional de Inteligencia Artificial de Chile

CoICERT – Grupo Interno de Trabajo de Respuesta a Emergencias Ciberneticas de Colombia

CONPES – Consejo Nacional de Política Económica y Social

CPC – Consejo Privado de Competitividad

CSIRT – Equipo de Respuestas a Incidentes de Seguridad Informática

CSIRT Gob – Equipo Gubernamental de Respuestas a Incidentes de Seguridad Informática

DAPRE – Departamento Administrativo de Presidencia de la República

DANE – Departamento Administrativo Nacional de Estadística

DNP – Departamento Nacional de Planeación

ECV – Encuesta de Calidad de Vida

END – Estrategia Nacional Digital

ENTIC – Encuesta de Tecnologías de la Información y las Comunicaciones

FURAG – Formulario Único de Reporte de Avances de la Gestión

GCI – Global Cybersecurity Index

GDI – Global Digitalization Index

GDB – Global Data Barometer

HPC – High Performance Computing

IA – Inteligencia Artificial

ICCN – Infraestructuras Ciberneticas Críticas Nacionales

I+D+i – Investigación, desarrollo e innovación

IDC – International Data Corporation

ILIA – Índice Latinoamericano de Inteligencia Artificial

IMD – Institute for Management Development

ISO – International Organization for Standardization

IXP – Internet Exchange Point

Mbps – Megabits por segundo

MGSI – Modelo de Gestión y Seguridad de la Información

MinDefensa – Ministerio de Defensa Nacional

MinCiencias – Ministerio de Ciencia, Tecnología e Innovación

MinTIC – Ministerio de Tecnologías de la Información y las Comunicaciones

MIPYME – Micro, Pequeña y Mediana Empresa

OCDE – Organización para la Cooperación y el Desarrollo Económicos

OEA – Organización de Estados Americanos

ONU – Organización de las Naciones Unidas

PISA – Programme for International Student Assessment

PND – Plan Nacional de Desarrollo

PNUD – Programa de las Naciones Unidas para el Desarrollo

PRST – Proveedores de Redes y Servicios de Telecomunicaciones

SDA – Sistemas Automatizados de Decisión

SFC – Superintendencia Financiera de Colombia

SIC – Superintendencia de Industria y Comercio

STEM – Science, Technology, Engineering and Mathematics

TIC – Tecnologías de la Información y las Comunicaciones

UIT – Unión Internacional de Telecomunicaciones

UNESCO – Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

WDC – World Digital Competitiveness Ranking

WIPO – World Intellectual Property Organization

Referencias

Banco Mundial. (2023). *Economía Digital para América Latina y el Caribe - Diagnóstico de país: Colombia.*

Extraído de: <https://openknowledge.worldbank.org/handle/10986/39906>

Cenia. (2024). *Índice Latinoamericano de Inteligencia Artificial 2024.* Santiago de Chile.

CPC. (2024). *Informe Nacional de Competitividad 2024 - 2025.* Bogotá, D.C.

DAPRE (2021) Marco de Ético para la Inteligencia Artificial en Colombia

DANE. (2022). *Encuesta Pulso Empresarial. Resultados para la ronda 31 (Octubre - Noviembre de 2022).*

DANE. (2024). *Boletín Técnico Indicadores básicos de tenencia y uso de Tecnologías de la Información y las Comunicaciones - TIC en hogares y personas de 5 y más años de edad 2023.* Bogotá. Extraído de: <https://www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/tecnologias-de-la-informacion-y-las-comunicaciones-tic/indicadores-basicos-de-tic-en-hogares>

DNP. (2022). *Informe sobre resultados Colombia Global Data Barometer 2022.* Bogotá, D.C

DNP. (2024). *Definición de una canasta básica TIC para la inclusión digital de los hogares en Colombia.* Bogotá, D.C.

DNP. (2024). *Documento para comentarios Política Nacional de Inteligencia Artificial.* Bogotá, D.C.

DNP. (2024). *Estrategia Nacional Digital de Colombia 2023-2026.*

DNP. (2024). *Resumen Ejecutivo Estrategia Nacional Digital de Colombia 2023-2026.* Bogotá, D.C.

Gutiérrez, J.D., Muñoz-Cadena, S., & Castellanos-Sánchez, M. (2023). *Sistemas de decisión automatizada en el sector público colombiano (Versión V1).* Universidad del Rosario.

Huawei e IDC. (2024). *Global Digitalization Index 2024.* Extraído de: <https://www.huawei.com/en/gdi>

IMD. (2024). *IMD World Digital Competitiveness Ranking 2024.* Extraído de: <https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/>

KPMG. (2024). *Colombia Tech Report 2023-2024.*

LINKTIC. (2024, 02 13). *LINKTIC BLOG.* Extraído de: <https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia/#ataquesciberseguridad>

Referencias

KPMG. (2024). Colombia Tech Report 2023-2024.

MinTIC (2024) Colombia Potencia Digital

MinTIC (2024) Plan Integral de Expansión de Conectividad Digital.

MinTIC. (2024). Boletín Trimestral de las TIC - Segundo Trimestre de 2024. Bogotá, D.C.

Oxford Insights. (2023). Government AI Readiness Index 2023.

PNUD. (2024). AILA: Evaluación del Panorama de la Inteligencia Artificial en Colombia.

Policía Nacional de Colombia. (2025). Balance de Anual 2024: Centro Cibernético Policial.

SONICWALL. (2024, 07 23). www.sonicwall.com. Extraído de:

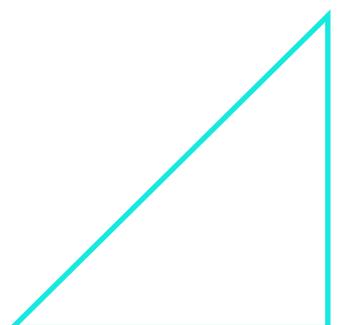
<https://www.sonicwall.com/es-mx/news/sonicwall-report-details-exponential-increase-in-overall-cyberattacks-reveals-potential-revenue-risk-for-businesses>

Tortoise. (2024, 12 13). The Global AI Index 2024. Extraído de:

<https://www.tortoisemedia.com/intelligence/global-ai/#rankings>

UIT. (2020). Global Cybersecurity Index.

UIT. (2024). Global Cybersecurity Index 2024 5th Edition.



Listas de Gráficos

Gráfico 1. Proporción de hogares que poseen el servicio de acceso a Internet según tipo de conexión en cualquier lugar (2023) \ 20

Gráfico 2. Porcentaje promedio de hogares que demandan Internet fijo (solo o empaquetado) desagregados por decil de ingreso (2023) \ 20

Gráfico 3. Accesos fijos a Internet por tipo de tecnología (millones) (2021-4T a 2024-2T) \ 21

Gráfico 4. Velocidad de descarga promedio nacional (Mbps) Internet fijo (2021-4T a 2024-2T) \ 21

Gráfico 5. Accesos a Internet móvil por tipo de tecnología (millones) (2021-4T a 2024-2T) \ 22

Gráfico 6. Velocidad promedio de descarga (Mbps) Internet móvil. Colombia y países de referencia (abril de 2024) \ 22

Gráfico 7. Proporción de hogares que poseen computador de escritorio, portátil o tableta (2022 y 2023) \ 24

Gráfico 8. Proporción de personas de 5 y más años de edad que poseen teléfono celular (2022 y 2023) \ 25

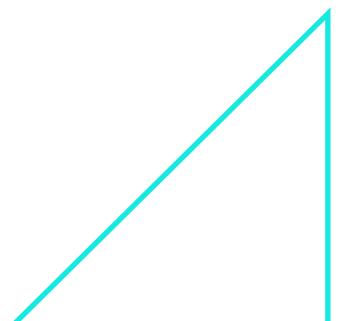
Gráfico 9. Puntaje subindicadores de Nube/Capacidad de infraestructuras de HPC/ Centros de datos certificados del ILIA 2024 \ 27

Gráfico 10. Desempeño de Colombia versus el promedio de América Latina y el Caribe en los pilares del GDB (2022) \ 30

Gráfico 11. Resultados de Colombia y la región de las Américas en el Global Cybersecurity Index 2024 \ 50

Listas de Figuras

Figura 1. Ejes de la Estrategia Nacional Digital de Colombia 2023-2026 \ 37



Lista de Tablas

Tabla 1. Resultados del Global Digitalization Index 2024 \ **16**

Tabla 2. Resultados del World Digital Competitiveness Ranking 2024 \ **16**

Tabla 3. Capacidad de infraestructuras de computación de alto rendimiento de Colombia \ **28**

Tabla 4. Proporción de personas de 5 y más años de edad que usaron computador o Internet, según el tipo de habilidad 2023 \ **32**

Tabla 5. Ejes, objetivos y líneas estratégicas de la END 2023-2026 \ **38**

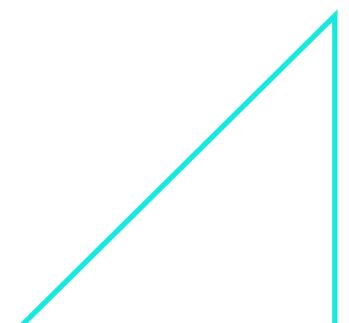
Tabla 6. Indicadores y metas estratégicas END 2023-2026 \ **40**

Tabla 7. Resultados de Colombia en el Global Cybersecurity Index 2020 y 2024 \ **49**

Tabla 8. Resultados del Global AI Index 2024 \ **73**

Tabla 9. Resultados del Government AI Readiness Index 2023 \ **74**

Tabla 10. Resultados del Índice Latinoamericano de IA (ILIA) 2024 \ **74**





CCIT tictac

