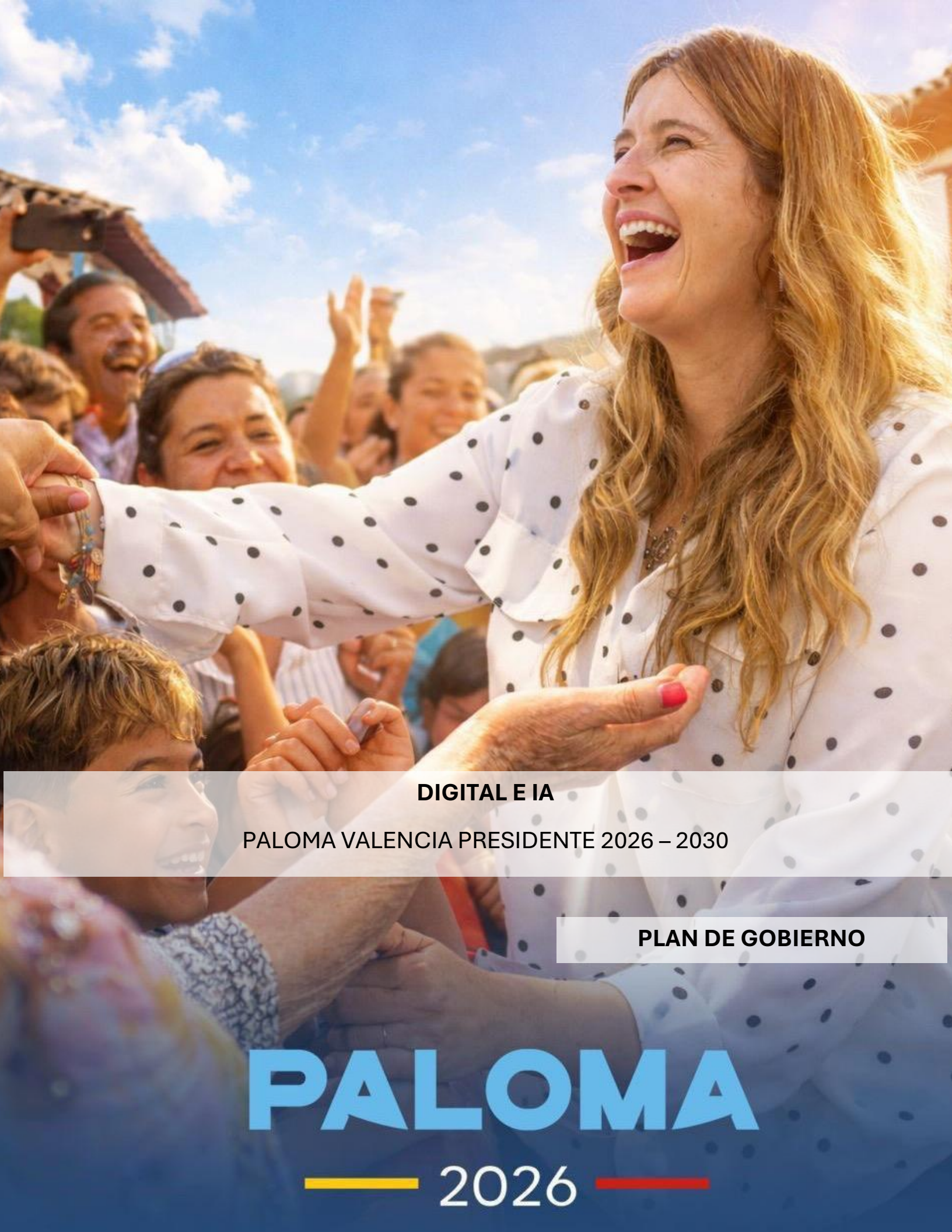

DIGITAL E IA

PALOMA VALENCIA PRESIDENTE 2026 – 2030

PLAN DE GOBIERNO

PALOMA

2026

PLAN DE TECNOLOGÍA
PALOMA VALENCIA
2026 – 2030

1. DIAGNÓSTICO

A continuación, se proporciona una visión estratégica y basada en datos sobre el estado de la economía digital en Colombia, identificando tanto los logros actuales como los desafíos críticos que deberán abordarse en el periodo 2026-2030. Igualmente, presentamos nuestra aproximación para lograr que la transformación digital y el uso intensivo de la tecnología no sea solo un discurso o divertimento, sino una política de inclusión, desarrollo y competitividad.

1.1. La brecha digital

La brecha digital en Colombia revela una tendencia de progreso constante, consolidando una reducción acumulada del 12,72% en el Índice de Brecha Digital (BID) entre los años 2018 y 2024. Para el cierre de 2024, el país alcanzó un puntaje nacional de 0,384, lo que representa una mejora de 0,006 puntos respecto al año anterior en una escala donde los valores cercanos a cero indican un mayor avance en el cierre de la brecha. Este comportamiento positivo se sustenta principalmente en las dimensiones de acceso material y habilidades digitales, las cuales explican en conjunto el 65,7% del fenómeno a nivel nacional.

En términos de infraestructura, destaca el incremento del 29,6% en la velocidad promedio de internet fijo residencial, llegando a los 227 Mbps, y una cobertura de redes móviles 4G o superiores que ya alcanza al 91,3% de la población.

A pesar de estos avances técnicos, el panorama nacional sigue fragmentado por profundas disparidades regionales y desafíos en la apropiación efectiva de las tecnologías. Bogotá se mantiene como el ente territorial con menor brecha digital (0,239), mientras que departamentos periféricos como Vichada (0,698) y Vaupés (0,624) presentan los niveles de rezago más críticos.

Por otro lado, la dimensión de aprovechamiento emerge como el área más desafiante, pues solo siete departamentos lograron reducir su brecha en este ámbito durante el último año. Esto sugiere que, si bien la infraestructura está llegando a más territorios, el uso diversificado y productivo de las herramientas digitales no se garantiza automáticamente con el acceso físico.

En conclusión, aunque el país progresa, el cierre definitivo de la brecha requiere esfuerzos focalizados en los departamentos históricamente rezagados y un fortalecimiento continuo de las habilidades digitales avanzadas.

1.2. La Transformación Digital y la Arquitectura Empresarial (2024-2025)

El estado de la transformación digital en Colombia enfrenta un escenario de contrastes marcado por un reciente retroceso en escalafones internacionales. Según el Índice de Gobierno Digital 2024-2025 de la OCDE, el país quedó fuera del top 10 mundial, evidenciando dificultades para mantener el ritmo de innovación frente a otras economías que han acelerado su transición hacia un Estado centrado en datos. Aunque a nivel interno se reportan incrementos en los indicadores de gestión de las entidades, persiste una brecha de implementación entre el cumplimiento normativo (el "papel") y la

transformación real de los servicios ciudadanos. Los principales obstáculos se concentran en una cultura institucional resistente al cambio, presupuestos de inversión intermitentes y una escasez de visión estratégica en la alta dirección para integrar la tecnología como un activo misional y no solo como un soporte operativo.

En materia de arquitectura empresarial, si bien la adopción del Marco de Referencia 3.0 (MAE) ha proporcionado una estructura legal, su aplicación efectiva en las entidades territoriales y sectores críticos muestra signos de fragmentación. La arquitectura aún no logra consolidarse como una herramienta de gobernanza que garantice la interoperabilidad real y la seguridad digital. El país se encuentra en un punto crítico donde el aumento de los ciberataques (con más de 37.000 millones de intentos en 2024) ha puesto a prueba la resiliencia de las infraestructuras actuales, revelando que muchas arquitecturas institucionales carecen de una capa de seguridad por diseño lo suficientemente robusta. En suma, el diagnóstico sugiere que el Estado colombiano ha priorizado la cobertura y la formalidad técnica sobre la profundidad de la transformación y la protección de su ecosistema digital.

1.3. Competitividad y Apropiación

Colombia se encuentra en una fase intermedia de consolidación de su ecosistema digital y de Inteligencia Artificial (IA), caracterizada por avances relevantes en formulación de políticas públicas, construcción de marcos habilitantes y adopción progresiva de tecnologías emergentes, pero también por brechas estructurales persistentes en infraestructura, datos, talento humano y gobernanza efectiva.

El país ha formulado instrumentos estratégicos orientados a impulsar la transformación digital y el aprovechamiento de tecnologías avanzadas, como la Estrategia Nacional Digital (END) 2023–2026, el documento CONPES 4144 de 2025 (Política Nacional de Inteligencia Artificial), y la iniciativa Colombia PotencIA Digital, que buscan cerrar brechas territoriales, fortalecer el ecosistema empresarial e incrementar la competitividad económica mediante la adopción tecnológica.

- Ranking Global: El país ocupa el puesto 54 de 134 economías en el World Digital Competitiveness Ranking 2025, con un puntaje de 49,66% en preparación para el futuro.
- Índice de Apropiación Digital (Centro Nacional de Consultoría): En una escala de 0 a 1, Colombia puntúa 0,31. La distribución de la ciudadanía digital es: 18% avanzada, 32% intermedia, 37% básica y un 13% de no usuarios. El reto es movilizar al 69% de la población que se encuentra en niveles básicos o intermedios hacia el nivel avanzado.
- Confianza en IA: El 69% de los colombianos confía en que sus datos están protegidos con la IA, cifra que sube al 78% entre quienes ya la utilizan

1.4. Infraestructura y Conectividad (Cifras a 2T-2025)

A pesar del despliegue progresivo de tecnologías móviles como 5G, del impulso a programas públicos de transformación digital y del fortalecimiento de la digitalización estatal, Colombia mantiene rezagos significativos frente a estándares internacionales. Entre las principales limitaciones identificadas se encuentran la baja cobertura en zonas rurales, la insuficiencia de talento especializado, la baja adopción de tecnologías emergentes en sectores productivos, y un entorno regulatorio aún desarticulado y poco adaptativo frente a los cambios tecnológicos. Estas limitaciones dificultan la consolidación de una economía digital sólida y reducen el impacto potencial de la

tecnología como instrumento para el cierre de brechas sociales, la mejora de servicios públicos y el fortalecimiento institucional.
El despliegue de infraestructura digital en Colombia enfrenta múltiples barreras regulatorias, administrativas, energéticas, fiscales, sociales y territoriales que limitan la expansión de las redes de telecomunicaciones. La diversidad de procesos de aprobación en los más de 1.100 municipios, sumada a la falta de articulación normativa, continúa retrasando los proyectos estratégicos, a pesar de esfuerzos legislativos y reglamentarios, como el Procedimiento Único para el Despliegue de Infraestructura (Decreto 1031 de 2024). Además, la inestabilidad de las redes eléctricas, los impuestos locales como el de alumbrado público, el rechazo comunitario por desinformación y las restricciones de los Planes de Ordenamiento Territorial incrementan los costos de operación, afectando la cobertura, la calidad del servicio y ampliando la brecha digital.

El despliegue de infraestructura es el pilar fundamental para el crecimiento, pero la brecha rural sigue siendo el mayor obstáculo.

- Internet Fijo: 9,68 millones de accesos.
- Internet Móvil: 21,7 millones de accesos móviles. La tecnología 4G se ha consolidado como la principal en todos los municipios del país, mostrando un crecimiento constante,
- 65,6 % de los hogares colombianos cuentan con acceso a Internet, fijo o móvil. 72.5% en cabeceras municipales vs 41,9% en centros poblados y rural disperso (Encuesta de Calidad de Vida, 2024).
- Brecha de Dispositivos: Solo el 35,1% de los hogares nacionales posee un computador o tableta; en zonas rurales, esta cifra cae drásticamente al 16,5%. El 58% .de los hogares sin estos equipos cita el alto costo como la principal barrera.
- Energía Verde: Colombia ocupa la posición 49 global en sostenibilidad energética para infraestructura digital (puntaje 19,2), lo que representa un reto para la expansión de centros de datos.

1.5. Talento Humano y Educación

Colombia destaca por una ciudadanía proactiva, pero carece de formación técnica especializada masiva.

- Liderazgo en Aprendizaje: Colombia es el líder regional en demanda de cursos de IA en plataformas como Coursera, con una tasa de inscripción casi 5 veces superior al promedio de América Latina.
- Déficit de Especialización: A pesar del interés, el país tiene una baja proporción de graduados en áreas tecnológicas comparado con naciones avanzadas. La formación avanzada es crítica: Colombia solo cuenta con 1 programa de doctorado en IA por cada millón de habitantes (puntaje de 4,7), muy lejos de los estándares de países como Chile o Uruguay.
- Habilidades Críticas: Solo el 30,8% de los usuarios sabe usar hojas de cálculo complejas y apenas el 9,3% domina algún lenguaje de programación.

Adicional a este panorama, se resalta que según el Foro Económico Mundial (2026), la inteligencia artificial y la automatización transformarán profundamente el empleo hacia 2030, con la creación de cerca de 170 millones de nuevos puestos, pero también la desaparición de aproximadamente 92 millones, lo que implica una reconfiguración estructural del mercado laboral. En este contexto, el 54% de los líderes empresariales anticipa que la IA reemplazará empleos existentes, mientras que solo una minoría prevé una creación significativa de nuevos roles, reflejando un escenario de alta incertidumbre

y una creciente presión sobre los sistemas educativos y de formación para preparar el talento del futuro.

1.6. Inteligencia Artificial y Gobernanza

El país es reconocido como un referente regional en la estructuración institucional de la tecnología.

- Liderazgo en Gobernanza: Colombia se ubica entre los cinco primeros de la región en gobernanza de IA, con un puntaje de 76,01.
- Instrumentos Clave: Contamos con la Estrategia Nacional Digital 2023-2026 y el CONPES 4144 de 2025 (Política Nacional de IA).
- Ecosistema de Datos: Colombia tiene un ecosistema de datos en desarrollo (60 puntos), por encima de países como Argentina o Perú en gestión y gobernanza para IA.
- Gobernanza de Datos: En el Barómetro de Datos, Colombia destaca en gobernanza (68,9 puntos), superando a la mayoría de sus pares regionales en la gestión ética y técnica de la información.

1.7. Ciberseguridad

La creciente digitalización de la economía también aumenta los riesgos asociados a ciberataques. El Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT) señala que los países deben fortalecer cinco dimensiones clave:

- marcos legales de ciberseguridad
- capacidades técnicas
- cooperación internacional
- desarrollo de talento especializado
- cultura de seguridad digital

De acuerdo con la UIT, fortalecer estas capacidades será fundamental para proteger infraestructuras críticas como sistemas financieros, energía, transporte y servicios gubernamentales. Colombia destaca en capacidades técnicas pues tiene buen desempeño técnico, con infraestructura y capacidades operativas relativamente desarrolladas en comparación regional.

También en desarrollo de capacidades relacionadas con campañas de concientización, formación en ciberseguridad y desarrollo de capacidades institucionales.
Colombia tiene tres áreas principales de mejora en coordinación institucional e implementación efectiva de estrategias nacionales. En cuanto a marco institucional, el país aún requiere mayor coordinación entre instituciones, fortalecimiento de las agencias de ciberseguridad y mejor gobernanza del ecosistema digital.
Además, en Colombia existen al menos 20 CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática), pero la articulación entre ellos es limitada, lo que reduce la eficacia de la respuesta ante ciberataques.

1.6. Limitaciones de la tecnología para las mujeres

En Colombia, las mujeres enfrentan barreras estructurales que limitan su participación en la economía digital. Aunque más del 52% de las niñas muestra interés en áreas STEM, solo el 25% de los empleos en el sector TI son ocupados por mujeres y apenas 3 de cada 10 graduados en estas áreas son mujeres. Esta brecha se amplía por el bajo

dominio de programación y el acceso limitado a la tecnología. Cerrar estas brechas no solo es un imperativo de equidad, sino una condición clave para el desarrollo económico y social del país.

La vulnerabilidad de las mujeres en Colombia sigue en aumento: en 2024 se registraron más de 131.000 casos de violencia de género, el 75,6% contra mujeres, y en los primeros meses de 2025 ya se superaban los 120 feminicidios. A esto se suma que el 62,8% de las mujeres desconoce los canales de denuncia, lo que impide activar a tiempo mecanismos de protección, aun cuando muchas víctimas habían sufrido agresiones previas que pudieron evitar desenlaces más graves. La tecnología es fundamental para evitar situaciones que ponen en riesgo a las mujeres.

Paralelamente, las mujeres enfrentan importantes barreras económicas: aunque representan aproximadamente el 42% del tejido empresarial en Colombia y cerca del 42%–46% de las nuevas empresas creadas, la gran mayoría de estos emprendimientos son microempresas con baja escalabilidad. Esta situación es aún más crítica en zonas rurales, donde el acceso a mercados es limitado.

2. ENFOQUE SECTORIAL, PROPUESTAS Y PROGRAMAS DE LA MESA DIGITAL

2.1. Enfoque sectorial

Las Tecnologías de la Información y las Comunicaciones (TIC) comprenden el conjunto de herramientas, infraestructuras y sistemas que nos permiten crear, procesar y compartir información para potenciar el desarrollo humano. Este ecosistema abarca desde los dispositivos físicos y sensores que tocamos (hardware) y los programas que utilizamos (software y aplicaciones), hasta la nube que almacena datos a escala global (big data).

Actualmente, su frontera más avanzada es la **Inteligencia Artificial (IA),** que no solo crea contenido nuevo (IA generativa), sino que es capaz de actuar y resolver problemas de forma autónoma (IA agencial).

Para un país, las Tecnologías de la Información y las Comunicaciones no constituyen únicamente un sector tecnológico; representan una política de Estado orientada a promover igualdad de oportunidades, fortalecer la competitividad nacional y cerrar brechas históricas.

Las TIC son un instrumento estratégico para democratizar el acceso al conocimiento, modernizar el aparato productivo, impulsar la innovación y consolidar un desarrollo económico, social y cultural incluyente, conectando a cada ciudadano y territorio con las oportunidades del siglo XXI.

De acuerdo con lo anterior, el enfoque que proponemos consta de **dos aspectos:** promover el mayor despliegue de infraestructura tecnológica y la conectividad por un lado; y la apropiación de la tecnología en los sectores productivos de la economía y la población para promover un significativo impulso al desarrollo sostenible en sus dimensiones económica, social y cultural.

Sin embargo, no toda la propuesta se basa en desarrollo de infraestructura de conectividad, computacional y sistemas robustos de datos e Inteligencia Artificial. Para poder aprovechar, difundir y transformar digitalmente el Estado y el aparato productivo,

se deberá preparar el talento digital, para lo cual se deberá fortalecer desde la escuela, las matemáticas, el pensamiento computacional, y la lectura crítica, si se quiere formar ciudadanos competentes para entender, usar, aprovechar y desarrollar tecnología digital. Lo anterior se complementará con programas masivos de formación y certificación de competencias digitales, para lo cual nos apalencaremos en todos los contenidos y programas desarrollados por las compañías tecnológicas de clase mundial y local que quieran apoyar el reentrenamiento y desarrollo de la fuerza laboral del país.

Además, para disminuir las barreras de acceso a la tecnología y fomentar la apropiación, se reducirán los impuestos que encarecen dispositivos y servicios (hoy hasta 40% del costo).

PROPUESTAS

En línea con el diagnóstico del sector, las propuestas de la mesa de digitalización e Inteligencia Artificial están dirigidas a lograr el mayor desarrollo de la conectividad, disminuir las barreras de entrada para adquirir medios de acceso, fomentar la educación digital y utilizar efectivamente la IA en cada sector económico, apoyado en el uso estratégico de los datos.

El país necesita dar un salto digital estructural, en una agenda que combine la conectividad total, desarrollar un Estado Digital, adoptar la ciberseguridad, promover el mayor despliegue de infraestructura de datos y formar masivamente en habilidades tecnológicas.

Cada propuesta sectorial ha sido construida por un equipo interdisciplinario de expertos en cada área programática, apoyados por el grupo de tecnología y desarrollo digital, para asegurar que las propuestas sean viables, ejecutables y promuevan el desarrollo y el crecimiento de cada sector, al servicio de la ciudadanía en general.

Lo anterior estará apoyado por una **innovadora arquitectura institucional** dentro del Estado para asegurar que este ambicioso enfoque cuente con los recursos, el talento necesario y el apoyo político requerido para lograr la modernización y transformación digital.

2.1. Arquitectura institucional

La implementación de un marco de arquitectura empresarial para el Estado colombiano representa el paso definitivo hacia una administración pública integrada, eficiente y orientada al valor público. Este proceso no debe entenderse como un proyecto tecnológico aislado, sino como una hoja de ruta estratégica que alinea la visión del gobierno con sus capacidades de ejecución mediante la armonización de cuatro dominios fundamentales: Infraestructura, negocio, datos y aplicaciones.

En el nivel de la **arquitectura de negocio** y operación, el objetivo principal es la estandarización de los servicios ciudadanos. Esto implica el diseño de un modelo de referencia que permita a las entidades territoriales y nacionales hablar un lenguaje común. Al definir procesos transversales, el Estado puede operar como una plataforma única, eliminando la fragmentación administrativa y permitiendo que los trámites se desarrollen de manera fluida entre diferentes organismos sin que el ciudadano deba actuar como el mensajero entre oficinas estatales.

La **arquitectura de datos** se constituye como el sistema circulatorio de esta propuesta. Se requiere el establecimiento de un ecosistema de interoperabilidad donde el dato se capture una sola vez y se comparta de forma segura y ética. Bajo este esquema, se definen estándares de metadatos y modelos de referencia semántica que garantizan que la información sea consistente en todo el territorio. La soberanía y gobernanza del dato aseguran que la información pública se convierta en un activo para la toma de decisiones basadas en evidencia, respetando siempre los marcos legales de privacidad y protección de datos personales.

En cuanto a la **arquitectura de aplicaciones**, el enfoque debe migrar hacia la modularidad y el uso de microservicios gubernamentales. En lugar de adquirir sistemas cerrados y monolíticos que generan dependencia de proveedores, el Estado colombiano debe fomentar el desarrollo de componentes reutilizables y software público. Esto permite que una solución de gestión documental o una pasarela de pagos desarrollada por una entidad líder pueda ser adoptada y adaptada por un municipio pequeño, optimizando el gasto público y acelerando la transformación digital en las regiones menos favorecidas.

Finalmente, la **arquitectura de infraestructura** proporciona el soporte físico y lógico necesario para sostener esta estructura. La implementación de una estrategia de nube híbrida gubernamental es esencial para equilibrar la escalabilidad y la seguridad. Esto implica centralizar la infraestructura crítica en centros de datos con altos estándares de resiliencia, mientras se aprovechan las capacidades de la nube pública para servicios que requieren alta concurrencia.

La ciberseguridad se integra de forma transversal, estableciendo perímetros de defensa coordinados que protegen la infraestructura crítica nacional contra amenazas globales.

Este enfoque integral de arquitectura empresarial permite que el Estado colombiano evolucione de una suma de entidades independientes hacia un organismo articulado que responde con agilidad a las necesidades de la sociedad, garantizando que cada inversión en tecnología tenga un impacto directo en la calidad de vida de los habitantes.

2.2. Ejes Principales

2.2.1. Conectividad territorial para el desarrollo y la equidad en Colombia

La conectividad digital significativa es un habilitador esencial del desarrollo económico, social y territorial de Colombia. Sin embargo, el país mantiene brechas persistentes entre zonas urbanas y rurales, así como en áreas rurales dispersas, territorios de frontera, selva y regiones de difícil acceso. Estas brechas no se explican únicamente por la ausencia de infraestructura, sino por un modelo histórico que ha privilegiado el despliegue físico de redes sobre la calidad, el uso real del servicio y su sostenibilidad en el tiempo. La compleja geografía colombiana y la dispersión poblacional hacen inviable una solución tecnológica única para todo el territorio.

La falta de conectividad efectiva limita el acceso a educación, salud digital, servicios públicos, mercados y oportunidades productivas, debilita la competitividad rural y restringe la capacidad del Estado para ejercer presencia institucional y garantizar derechos. Cerrar la brecha digital es, por tanto, un imperativo y una condición necesaria para avanzar en equidad territorial, productividad, inclusión social y cohesión nacional.

Esta política tiene como objetivo garantizar conectividad universal, resiliente y medible para toda la población colombiana, utilizando la tecnología más eficiente según las condiciones de cada territorio. La conectividad se concibe como un servicio habilitante

y un bien público estratégico, cuyo éxito se mide por la capacidad real de las personas, comunidades e instituciones para conectarse con calidad, continuidad y a costos asequibles. Allí donde la conectividad lo permita, el país avanzará hacia un uso intensivo de tecnologías digitales avanzadas, incluida la inteligencia artificial, para mejorar la provisión de servicios públicos, la productividad y la toma de decisiones basadas en datos.

El modelo se fundamenta en la neutralidad tecnológica y en un enfoque de última milla centrado en el usuario. En territorios con mayor densidad poblacional, presencia de anclajes institucionales o alto retorno social, la fibra óptica es prioritaria. En amplias zonas rurales y periurbanas, las redes móviles 4G y 5G constituyen la solución principal por su capacidad de escalar cobertura de manera eficiente. En territorios remotos, de frontera, selva o difícil acceso, la conectividad satelital se integra como componente estructural. Estas soluciones se articulan en una arquitectura híbrida e interoperable que garantiza continuidad del servicio y evita la fragmentación del territorio en zonas conectadas y desconectadas.

Un eje central de la política es la transformación del esquema de incentivos públicos. El Estado deja de pagar únicamente por infraestructura instalada y pasa a remunerar resultados verificables de conectividad efectiva. Los subsidios, contratos y mecanismos de financiación se vinculan al cumplimiento de estándares mínimos de velocidad real, disponibilidad del servicio, latencia y estabilidad, medidos de forma independiente y continua mediante herramientas técnicas y mecanismos de reporte ciudadano. De esta manera, los recursos públicos se orientan a garantizar que la conectividad funcione en la práctica, incorporando correctivos y penalidades cuando exista infraestructura sin servicio efectivo.

La política reconoce y fortalece el rol de las redes comunitarias y los operadores locales como actores clave para cerrar brechas en zonas donde los modelos de negocio tradicionales no resultan viables. Se establece un marco legal, técnico y financiero que permita su operación sostenible, su integración a la red nacional mediante acceso a backhaul, espectro y soporte técnico, y su articulación con operadores regionales y nacionales. Este enfoque se complementa con programas de formación técnica local que fortalecen capacidades, generan empleo y promueven la apropiación comunitaria de la conectividad como bien público.

La conectividad se define explícitamente como infraestructura social estratégica. Se prioriza la conexión efectiva de escuelas rurales, sedes educativas, puestos y centros de salud, puntos de atención al ciudadano, centros comunitarios y productores rurales. Así, la conectividad habilita la educación híbrida, la telemedicina, la digitalización del agro, la formalización productiva y los trámites públicos sin fricción, maximizando el impacto social y económico de la inversión.

El modelo incorpora criterios de resiliencia y continuidad del servicio como elementos obligatorios de diseño, promoviendo la redundancia de enlaces, soluciones de energía de respaldo y protocolos de recuperación rápida ante fallas técnicas, eventos climáticos extremos o afectaciones al orden público, especialmente en zonas críticas.

La implementación se articula desde una autoridad nacional de conectividad y gobierno digital, en coordinación con el Ministerio TIC, entidades territoriales, operadores nacionales y regionales, comunidades y cooperación internacional. La planeación y el despliegue se apoyan en información geoespacial, catastro multipropósito y gemelos digitales del territorio, y la contratación se basa en resultados y desempeño.

El seguimiento se realiza mediante indicadores claros y verificables, como el porcentaje de población rural con conectividad efectiva, la velocidad real promedio, la disponibilidad del servicio, el costo por usuario conectado y la sostenibilidad de las redes comunitarias. Estos indicadores garantizan transparencia, rendición de cuentas y mejora continua, asegurando que la conectividad contribuya de manera efectiva al desarrollo integral y equitativo de Colombia.

Además, se reducirán los impuestos que encarecen los dispositivos de acceso a Internet y sus servicios.

2.2.2. Interoperabilidad de datos: un solo Estado conectado (principio “solo una vez”)

La transformación digital del Estado no se logra con más portales ni con más trámites “en línea”. Se logra cuando el Estado deja de funcionar como islas y empieza a operar como una sola red coordinada, capaz de intercambiar información de forma segura, automática y en tiempo real. Hoy el ciudadano pierde tiempo probando lo que el Estado ya sabe; esa fricción alimenta costos, corrupción, exclusión y decisiones públicas tomadas con información incompleta o desactualizada.

Nuestro gobierno implementará un **Marco Nacional de Interoperabilidad** como el “idioma común” del Estado: un conjunto de reglas, estándares y componentes compartidos que obligan a las entidades a **hablar entre sí** y a prestar servicios ciudadanos sin que la gente tenga que ser el mensajero entre oficinas. La meta es clara: **principio de “solo una vez”**. Ningún ciudadano deberá entregar dos veces la misma información, ni cargar certificados en papel que ya reposan en bases públicas.

Este marco será un habilitador directo del **Estado AI-First**: la inteligencia artificial solo puede operar con escala y justicia si el dato fluye con calidad, trazabilidad y gobernanza. Por eso, la interoperabilidad no será un proyecto técnico opcional, sino la **norma operativa** del Estado y un requisito para el rediseño de servicios.

El enfoque se apoya en aprendizajes internacionales (como Estonia con XRoad y otros modelos de estándares abiertos) pero adaptado a Colombia: una interoperabilidad que no dependa de convenios puntuales entre entidades, sino de un **estándar nacional obligatorio**. El resultado será un Estado que reduce burocracia, ahorra tiempo y dinero, y convierte la digitalización en bienestar real.

Para lograrlo, pondremos en marcha cuatro decisiones de fondo:

I. **Plataforma única de interoperabilidad del Estado.** Consolidaremos una infraestructura común para el intercambio de datos entre entidades nacionales y territoriales, con servicios de interoperabilidad reutilizables y escalables. Esto permitirá consultas y validaciones internas en segundos (por ejemplo, afiliación a salud, licencias, estado tributario, elegibilidad de programas), eliminando el “certificado como trámite”.

II. **Calidad, disponibilidad y organización del dato como política pública.** La interoperabilidad funciona solo si los datos están estandarizados, representativos, actualizados y legibles por máquina. Por eso exigiremos que las entidades conviertan sus bases en datos “aprovechables”, con estándares mínimos y responsabilidades claras. Así el Estado podrá tomar decisiones con evidencia, anticipar necesidades y reducir fugas del gasto.

III. **Seguridad, privacidad y trazabilidad por diseño.** El dato público es un activo estratégico y debe tratarse con el mismo rigor que la infraestructura crítica: acceso con control, registro de consultas, auditoría permanente y sanciones por uso indebido. La interoperabilidad no significa "abrir" datos sin reglas: significa compartirlos con seguridad y propósito, protegiendo derechos y construyendo confianza.

IV. **Interoperabilidad + identidad digital como llave universal.** La interoperabilidad requiere una base de confianza: una identidad digital que permita al ciudadano acceder a servicios y al Estado validar información sin fricción. Al integrar identidad digital con sistemas que "hablan entre sí", eliminamos filas, presencialidad y desplazamientos costosos, y devolvemos tiempo a la gente.

Este Marco Nacional de Interoperabilidad hará posible la **Carpeta Ciudadana** como punto de interacción único y la consolidación de una operación estatal basada en datos y resultados en tiempo real. Cada trámite se transforma: menos formularios, más validaciones internas; menos esperas, más automatización; menos discrecionalidad, más reglas claras. Y, al digitalizar de punta a punta la operación, se fortalecen transparencia y control social: cada decisión deja rastro auditable y se reducen espacios para la opacidad.

Mediremos el avance con resultados concretos: porcentaje de trámites donde aplica "solo una vez", reducción de certificados en papel, número de servicios interoperables activos entre entidades, tiempos de validación (de días a segundos), y ahorro de costos administrativos para Estado y ciudadanía.

2.2.3 Plan Nacional de Inteligencia Artificial (PNIA): un Estado en el IA tiene la mayor prioridad (AI-First)

Colombia necesita un Plan Nacional de Inteligencia Artificial que convierta la IA en una política de Estado para mejorar la vida diaria de la gente, mejorar la productividad y modernizar el país, con reglas claras de confianza, privacidad y transparencia. La IA ya no es futurismo: es una tecnología de propósito general que define competitividad, eficacia estatal y oportunidades. Hoy Colombia tiene avances normativos y condiciones habilitantes, pero persisten brechas críticas en implementación, infraestructura de cómputo, inversión en I+D+i, talento avanzado y adopción efectiva en territorios y sectores.

Nuestro gobierno ejecutará un PNIA con una visión simple y transformadora: un Estado AI-First, es decir, un Estado que piensa, decide y actúa digitalmente desde el diseño, para que los servicios públicos sean rápidos, predecibles y casi instantáneos. En un Estado AI-First, la IA no es un conjunto de pilotos aislados o chatbots sueltos: es la capa transversal que conecta identidad digital, interoperabilidad, datos, conectividad, salud digital, talento y ciberseguridad. El Estado deja de pedir, esperar y revisar; el Estado anticipa, valida y entrega, siempre con control, trazabilidad y derechos garantizados.

Los servicios públicos siguen diseñados para procesos manuales y verificación humana; la digitalización suele ser "papel escaneado" que no reduce tiempos; y los funcionarios pierden capacidad en tareas repetitivas. El ciudadano enfrenta fricción, incertidumbre y demoras incluso en trámites simples. El problema no es falta de tecnología: es un modelo operativo que no está diseñado para operar con datos, automatización y decisiones rápidas.

El objetivo es transformar al Estado en AI-First para habilitar servicios críticos que respondan en segundos o minutos, reducir drásticamente tiempos y costos, mejorar la focalización del gasto público y aumentar la productividad nacional. La IA será un instrumento para un Estado más productivo, eficiente y transparente, no más grande.

AI-First no es reemplazar funcionarios, ni automatizar sin control, ni tomar decisiones opacas. AI-First sí es: automatizar lo repetible, escalar lo inteligente, mantener humano en el circuito en decisiones sensibles, asegurar transparencia y trazabilidad algorítmica, y tratar el tiempo del ciudadano como un bien público.

2.2.3.1. Componentes del PNIA

El Plan Nacional de Inteligencia Artificial (PNIA) se concibe como una política pública orientada a incorporar la inteligencia artificial como un habilitador estructural del Estado, con el propósito de mejorar la eficiencia, la calidad de los servicios públicos y la experiencia ciudadana. En este marco, **la IA se adopta como una capa transversal obligatoria para el diseño y desarrollo de nuevos servicios públicos**, integrada sobre pilares como la **identidad digital, la interoperabilidad y el uso estratégico de los datos del Estado.** Este enfoque permite evitar la fragmentación institucional, reducir costos operativos y facilitar la escalabilidad de soluciones exitosas.

Uno de los objetivos centrales del PNIA es avanzar hacia la **provisión de servicios públicos casi instantáneos**, especialmente en aquellos de alto impacto para la ciudadanía. Esto implica la automatización de procesos como afiliaciones, habilitaciones, validación de requisitos y renovaciones, de manera que el ciudadano no deba gestionar activamente un trámite cuando no existan cambios en su situación. En estos casos, el sistema estará en capacidad de verificar el cumplimiento de condiciones y actuar de forma proactiva, garantizando respuestas ágiles y oportunas.

De manera complementaria, se promoverá el desarrollo e implementación de **asistentes digitales oficiales del Estado**, disponibles a través de múltiples canales y claramente identificables como sistemas automatizados. Estos asistentes estarán diseñados para orientar a los ciudadanos, explicar derechos y obligaciones, y resolver solicitudes simples de principio a fin, siempre integrados con los sistemas institucionales y bajo criterios de trazabilidad y transparencia.

El PNIA también contempla la incorporación de herramientas de inteligencia artificial para fortalecer la **operación interna del Estado**. En este sentido, la IA servirá de apoyo a los servidores públicos en tareas como la clasificación y priorización de casos, el análisis de antecedentes, la elaboración de documentos y el seguimiento de procesos. Esto permitirá optimizar la gestión administrativa, reducir significativamente los tiempos de respuesta y mejorar la calidad de las decisiones, liberando capacidades humanas para la atención de casos complejos.

Asimismo, se impulsará un rediseño de los servicios públicos bajo un **enfoque de "cero fricción"**, basado en eventos de vida como el nacimiento, la educación, el empleo, la enfermedad o la vejez. A través de la articulación entre datos, reglas y sistemas de decisión, la IA permitirá que la interacción del ciudadano con el Estado se limite a los momentos estrictamente necesarios, facilitando una experiencia más simple, integrada y centrada en sus necesidades.

La implementación de estas capacidades se sustentará en un **marco robusto de gobernanza y confianza en la inteligencia artificial**. Para ello, se establecerán reglas

claras que definan los ámbitos de actuación de los sistemas automatizados y los casos en los que debe intervenir una persona. Igualmente, se garantizará el registro y la auditoría de las decisiones algorítmicas, así como los derechos de los ciudadanos a recibir explicaciones, solicitar revisiones y acceder a mecanismos de recurso.

Finalmente, el PNIA reconoce que el despliegue efectivo de la inteligencia artificial depende de la existencia de condiciones habilitantes en materia de **datos, conectividad e infraestructura**. En consecuencia, se promoverá el desarrollo de redes de conectividad con capacidad para soportar el tránsito de grandes volúmenes de información, incluyendo el fortalecimiento de tecnologías como 5G y la exploración de futuras generaciones como 6G. Paralelamente, se avanzará en la consolidación de una infraestructura de datos interoperable, inspirada en modelos internacionales de referencia, que permita disponer de conjuntos de datos de alta calidad y preparados para su uso en sistemas de inteligencia artificial.

2.2.3.2. Talento, adopción y productividad.

El Plan Nacional de Inteligencia Artificial solo será exitoso si Colombia convierte su principal activo —la gente— en la infraestructura más importante de la era de la IA: el **talento digital**.

Es básico para la creación del talento digital, **cerrar la brecha que existe en dispositivos de acceso a Internet**, fundamentalmente por el costo alto al que conlleva su adquisición. **Se disminuirá por tanto la carga impositiva en estos medios.**

La estrategia se implementará con un principio rector: aprender haciendo. La formación en IA no será teórica ni desconectada del trabajo; estará orientada a tareas reales (reducir tiempos, mejorar calidad, aumentar eficiencia y elevar ingresos). El éxito no se medirá por cuántas personas “asistieron” a un curso, sino por cuánto más productivas se vuelven en su trabajo y por su mejora efectiva en empleabilidad. Para asegurar velocidad y escala, el programa se organizará en rutas cortas, modulares y continuas, basadas en microcredenciales acumulables y verificables con valor laboral, articuladas al Marco Nacional de Cualificaciones y a la Clasificación Única de Ocupaciones.

El programa tendrá rutas diferenciadas para docentes, funcionarios públicos, PYMES y emprendedores, y estudiantes y jóvenes. La ejecución será mediante alianzas público-privadas con universidades, SENA/centros técnicos, ed-techs y empresas tecnológicas, con contenidos codiseñados según demanda laboral y actualizados de manera permanente.

Adicionalmente, el programa incorpora de manera estructural la **Transformación del Sistema Educativo para la Inteligencia Artificial**, con el propósito de preparar a las nuevas generaciones para desenvolverse con solvencia, criterio ético y capacidad productiva en una economía digital.

El objetivo será **modernizar y actualizar los currículos de educación básica, media y superior**, integrando de forma transversal y progresiva competencias avanzadas en matemáticas, inteligencia artificial, pensamiento computacional, programación, ciencia de datos y ética digital. Esta transformación no se limitará a la creación de nuevas asignaturas, sino que implicará la incorporación de estas competencias en distintas áreas del conocimiento —matemáticas, ciencias, humanidades, emprendimiento y formación técnica— para desarrollar habilidades analíticas, creativas y críticas desde etapas tempranas.

Asimismo, el programa promoverá la formación docente especializada, la actualización de estándares de calidad educativa y el fortalecimiento de alianzas entre el sector educativo, el sector productivo y el ecosistema tecnológico. Este esfuerzo tendrá enfoque territorial y modalidad híbrida para no dejar por fuera zonas con baja conectividad, y se complementará con formación en ética, seguridad digital y protección de datos. Mediremos avances con indicadores claros: número de personas reentrenadas por perfil (docentes, funcionarios, PYMES, jóvenes), porcentaje de micro credenciales con reconocimiento empresarial, inserción laboral o mejora salarial asociada, incremento de productividad en PYMES participantes, y ahorro de tiempo/costos en entidades públicas que adopten IA en sus procesos.

Para llevar a cabo la implementación, el PNIA se ejecutará con liderazgo central (gobierno digital + autoridad de IA) y obligatoriedad progresiva: todo nuevo servicio debe diseñarse AI-First, reutilizando componentes y evitando compras aisladas. Se priorizarán pilotos rápidos en servicios de alto volumen con escalamiento nacional cuando demuestren impacto.

Mediremos éxito por resultados concretos: tiempo promedio de resolución de servicios, porcentaje de servicios con entrega automática, reducción de trámites presenciales, ahorro de horas de funcionario y satisfacción ciudadana.

El PNIA será la base para lograr la transformación digital agresiva, que exige un cambio de paradigma que desplace el modelo de operación tradicional, basado en la autonomía aislada de las entidades, hacia un modelo de gobierno como plataforma. Esta transición busca que el estado funcione como un organismo coordinado, donde la tecnología no sea un accesorio de la burocracia, sino el motor que simplifica la relación entre la administración y la ciudadanía, garantizando la eficacia en el cumplimiento de los fines sociales y la eficiencia en el uso de los recursos públicos.

El nuevo modelo de operación se fundamenta en la automatización integral de procesos y en la eliminación de la presencialidad innecesaria. Al rediseñar los servicios bajo una lógica digital, el estado deja de ser un receptor pasivo de documentos para convertirse en un gestor proactivo de soluciones. Esto implica que los trámites internos y externos se ejecutan mediante flujos de trabajo inteligentes que conectan automáticamente a las entidades responsables, reduciendo los tiempos de respuesta de semanas a minutos y minimizando el margen de error humano o la duplicidad de funciones.

Colombia tendrá una política integral de talento digital que permita cerrar la brecha entre formación y demanda laboral en un contexto de transformación digital impulsada por la inteligencia artificial. Se fortalecerá la formación desde la educación básica en pensamiento crítico y la alfabetización digital y en inteligencia artificial, acompañada de un programa nacional de formación, certificación y acompañamiento continuo a docentes, que los reconozca como actores clave en la transformación educativa y garantice sus capacidades pedagógicas y tecnológicas. Se transformará la educación técnica y tecnológica con rutas ágiles hacia el empleo digital y se impulsarán programas de reconversión laboral para trabajadores que desarrollen roles en riesgo de automatización. Así mismo, se ampliará la formación avanzada en áreas como ciencia de datos e inteligencia artificial y se cerrarán brechas en mujeres al margen de la tecnología y territorios rurales mediante acceso a conectividad, formación pertinente y oportunidades laborales.

Se fortalecerán las capacidades del Estado mediante la certificación masiva de funcionarios públicos en el uso y apropiación ética de la inteligencia artificial, junto con

la creación de un sistema nacional de certificación de competencias digitales y en inteligencia artificial que conecte la formación con empleo.

2.2.4. Identidad digital ciudadana interoperable (cédula digital + credenciales verificables + "Carpeta Ciudadana")

Hoy la relación entre el ciudadano y el Estado es fragmentada, lenta y opaca: la información está dispersa entre múltiples entidades (salud, movilidad, educación, justicia, impuestos, programas y subsidios), se repiten trámites y certificados en papel, y la verificación manual abre espacio a demoras, exclusión y corrupción. En consecuencia, el Estado no tiene una visión confiable y en tiempo real del estatus del ciudadano (derechos, obligaciones y habilitaciones), y el gasto público se vuelve menos eficiente y menos justo. El Estado debería saber quién es cada ciudadano. Por eso en nuestro gobierno el ciudadano no tendrá que perder tiempo probándolo una y otra vez. Pero además una estructura de datos robusta, completa y de calidad, es el núcleo litante que se debe garantizar para operacionalizar las demás iniciativas del sector.

Por eso implementaremos una **Identidad Digital Ciudadana única, segura e interoperable**, que funcione como la **llave universal** para acceder a servicios del Estado sin filas, sin fotocopias, sin certificados y sin intermediarios. Esta identidad será la base para que el Estado opere bajo el principio de **"solo una vez"**: la información se captura una sola vez y el Estado la consulta internamente, con trazabilidad y control, para que ningún trámite le robe tiempo a la gente.

La identidad digital se apoyará en tres pilares:

I. **Cédula digital y autenticación fuerte.** Fortaleceremos y masificaremos la cédula digital (ya existente), superando sus barreras actuales de implementación y uso. La identidad estará asociada a la cédula y contará con autenticación robusta (por ejemplo, biometría y factores digitales), con despliegue progresivo obligatorio en trámites estatales de alto volumen. El objetivo es que identificarse ante el Estado sea tan simple como abrir el celular, sin perder seguridad. En el estado ideal, las bases biométricas estatales operaran bajo un **modelo de interoperabilidad total**, permitiendo la validación cruzada entre registros civiles, migración, policía, salud, justicia y autoridades electorales, entre otros.

   La interoperabilidad biométrica será un estándar, reduciendo duplicidades, evitando fraudes y garantizando un ciclo de vida único para cada identidad.

   Reconociendo las brechas tecnológicas entre instituciones, el ecosistema incorporará un modelo **BaaS (***Biometrics as a Service***)** administrado por el Estado, que permite que municipios, hospitales regionales, notarías o entidades con baja capacidad tecnológica utilicen servicios biométricos avanzados sin necesidad de infraestructura propia. Esto democratiza el acceso a tecnologías de verificación y estandariza la calidad de los procesos de identidad en todo el país.

II. **Credenciales verificables en una "billetera" ciudadana.** En lugar de depender de bases centralizadas indiscriminadas, el ciudadano contará con credenciales verificables (por ejemplo: afiliación y estado en salud, títulos académicos, licencias y permisos de tránsito, certificados

laborales/profesionales). Estas credenciales permitirán verificación instantánea sin intercambio de documentos, reduciendo fraude y acelerando servicios.

III. **Carpeta Ciudadana como punto único de interacción.** Consolidaremos la Carpeta Ciudadana como el lugar donde el ciudadano ve y gestiona su relación con el Estado: qué derechos tiene activos, qué obligaciones están al día, qué beneficios recibe, qué trámites puede hacer y en qué estado se encuentran.

    Esta política además permitirá construir un "CRM del Estado" para uso institucional: una vista integral, actualizada y verificable del ciudadano (programas en los que está, elegibilidad, alertas de cambios relevantes) para evitar pagos duplicados, mejorar focalización, reducir filtraciones y asegurar que los recursos lleguen a quien los necesita. El objetivo no es vigilar al ciudadano: es cuidar el dinero público y garantizar acceso oportuno a derechos.

La identidad digital será interoperable por diseño: se integra al Marco Nacional de Interoperabilidad para que las entidades "hablen entre sí" y el ciudadano no sea mensajero. También se articula con el enfoque de Estado AI-First-, porque la IA solo puede acelerar servicios si existe una identidad confiable, trazable y segura.

Como principio fundamental y garantista el ciudadano controla sus datos (consentimiento y trazabilidad), seguridad y privacidad por diseño, credenciales verificables (no centralización indiscriminada), interoperabilidad con entidades públicas y privadas autorizadas, e inclusión digital con alternativas para población sin conectividad o sin smartphone.

La ejecución tendrá liderazgo claro desde Gobierno Digital/MinTIC (o la entidad rectora definida), en coordinación con Registraduría y entidades misionales prioritarias (salud, tránsito, educación, justicia, programas sociales). Se impulsarán cambios normativos para reconocer legalmente las credenciales digitales como equivalentes al documento físico, y para exigir trazabilidad de accesos y sanciones por uso indebido.

Los avances se medirán contra resultados concretos: porcentaje de ciudadanos con identidad digital activa, porcentaje de trámites 100% digitales, tiempo promedio de verificación de información (de días a segundos), reducción de fraudes documentales y satisfacción ciudadana.

2.2.4.1 Carpeta Ciudadana

La pieza central de esta transformación es la consolidación de los servicios ciudadanos digitales, donde la Carpeta Ciudadana se convierte en el punto de interacción único. En este escenario, el modelo de operación estatal se rige por el **principio de "una sola vez",** lo que significa que el Estado asume la responsabilidad de consultar internamente la información que ya posee, liberando al ciudadano de la carga de aportar certificados, registros o documentos físicos que reposan en otras bases de datos públicas. La interoperabilidad deja de ser un proyecto técnico para transformarse en la norma operativa de todas las instituciones.

Para que esta modificación sea profunda, el Estado debe adoptar una cultura institucional basada en datos y resultados en tiempo real. El modelo de operación digital permite el seguimiento preciso de cada gestión, facilitando la identificación de cuellos de botella y la optimización constante de las políticas públicas. La infraestructura de datos se utiliza no solo para registrar el pasado, sino para predecir necesidades

sociales, permitiendo que el Estado se adelante a las demandas de la población en salud, educación o seguridad.

Finalmente, la transformación digital asegura la transparencia y el control social de manera nativa. Al digitalizar el ciclo completo de la operación estatal, desde la contratación hasta la ejecución presupuestal, se generan rastros auditables que fortalecen la confianza digital y reducen los espacios para la opacidad. En última instancia, este cambio de modelo busca un Estado que sea imperceptible en su complejidad, pero omnipresente en su efectividad, entregando valor público de forma ágil, segura y equitativa en todo el territorio nacional.

2.2.4.2. Estado Ideal: Identidad Digital Unificada y Ecosistema Nacional de Confianza

La consolidación de un ecosistema de identidad digital robusto, seguro e interoperable constituye el siguiente paso evolutivo en la transformación del Estado. En este estado ideal, la identidad digital se convertirá en el habilitador central de todos los servicios ciudadanos digitales, garantizando una experiencia fluida, confiable e integrada a lo largo de todos los sectores públicos y privados.

El estado adoptará una arquitectura de **Zero Trust**, tanto en el Gobierno como en colaboración con el sector corporativo.

Esto protege al Estado de amenazas cibernéticas, movimientos laterales y accesos indebidos en infraestructuras críticas.

Los documentos ciudadanos —incluyendo pasaporte, cédula y certificados oficiales— existirán en versiones **100% digitales**, firmadas criptográficamente y verificables mediante **tecnologías blockchain**.

Esto asegura trazabilidad, autenticidad y resistencia a falsificación, permitiendo controles automatizados en fronteras, servicios financieros, instituciones educativas y procesos judiciales.

El sistema operará bajo un marco de **protección de datos** garantizando transparencia, consentimiento informado, minimización de datos, derechos de rectificación/olvido y estrictas reglas de tratamiento.

El ciudadano mantiene control real sobre su identidad digital: quién la consulta, cuándo y para qué.

2.2.5. Innovación en la regulación: Sandboxes para acelerar soluciones sin sacrificar derechos

Colombia necesita reglas modernas para una economía y un Estado digitales, pero también necesita evitar un error frecuente: **regular primero y entender después**. Cuando la regulación llega tarde o llega mal, frena innovación, expulsa emprendimientos, consolida monopolios y obliga a las instituciones a improvisar. Y cuando llega “demasiado pesada”, mata la experimentación antes de que nazca. Nuestro gobierno impulsará una política de **innovación regulatoria** para que el país pueda probar, aprender y ajustar con evidencia, manteniendo siempre la protección de derechos, la seguridad y la transparencia.

La herramienta principal será los **sandboxes regulatorios y sectoriales** (“zonas libres de burocracia”): espacios de prueba supervisada, con reglas claras, alcance delimitado y evaluación obligatoria, donde startups, universidades, empresas y entidades públicas puedan probar soluciones nuevas en entornos controlados. Esto permite dos cosas a la vez: que la innovación avance sin parálisis y que el Estado regule con información real, no con intuición ni miedo.

Los sandboxes tendrán cuatro condiciones básicas. Primero, **objetivo público explícito**: cada sandbox se crea para resolver un problema concreto (por ejemplo, pagos y billetera digital, identidad digital, telesalud, compras públicas de innovación, LegalTech, o uso responsable de IA en servicios). Segundo, **reglas de juego claras**: qué se exime temporalmente, qué no se puede tocar, qué estándares mínimos aplican (protección de datos, ciberseguridad, trazabilidad, no discriminación, debido proceso cuando aplique). Tercero, **medición y rendición de cuentas**: métricas desde el día uno, evaluación expost- y publicación de resultados para aprender como país. Cuarto, **ruta de escalamiento**: si funciona, se escala rápido; si no funciona, se cierra sin costos hundidos ni captura regulatoria.

Esta política también protege a quienes innovan dentro del Estado. Hoy muchos equipos públicos no innovan por riesgo jurídico y por falta de rutas claras. Con sandboxes, el servidor público actúa dentro de un marco autorizado, con trazabilidad y criterios predefinidos. Eso reduce discrecionalidad, disminuye el miedo institucional y acelera soluciones útiles para la ciudadanía.

Finalmente, la innovación regulatoria se conectará con dos ejes del plan: **Compras Públicas Ágiles y Abiertas** y **GovTech**. Los sandboxes serán la puerta para pilotos controlados y compra pública por resultados: el Estado prueba, mide y luego compra y escala lo que demuestra valor. Así construimos un país que no se queda atrapado entre la parálisis y el abuso: **innovamos con control, y regulamos con evidencia**.

2.2.6 Sector audiovisual y radiodifusión

Reconociendo el dinamismo tecnológico y la innovación en el sector, proponemos modernizar el marco legal y regulatorio del sector audiovisual con el objetivo de (i) simplificar la operación de los proveedores de contenidos audiovisuales, televisión y radiodifusión; y (ii) promover la competencia, inversión y contenidos digitales y audiovisuales de calidad, apoyando la producción nacional y protegiendo la diversidad cultural y regional.

2.3. Programas

2.3.1 Compras públicas: modernizar la contratación para que el Estado pueda innovar sin parálisis y con transparencia

Un Estado que quiere ser digital, interoperable y AI-First- no puede seguir comprando tecnología con reglas y lógicas analógicas. Hoy, buena parte de la transformación digital se frena no por falta de ideas o de talento, sino por la rigidez y lentitud de la contratación: procesos largos, interpretaciones jurídicas dispares, pliegos hechos para soluciones cerradas y compras aisladas que se repiten en cada entidad. El resultado es predecible: innovación tardía, sobrecostos, dependencia de pocos proveedores y, en muchos casos, tecnología obsoleta al momento de entrar en operación.

Nuestro gobierno ejecutará un programa de **Compras Públicas Ágiles, Abiertas e Innovadoras** para convertir la contratación en un motor de innovación con control, y no en un cuello de botella. La idea central es simple: **agilidad con transparencia**. Comprar más rápido no significa comprar a ciegas; significa comprar con mejores reglas, con estándares claros, con trazabilidad digital y con evaluación por resultados. El miedo al riesgo normativo no puede seguir produciendo parálisis; el control real se logra con datos, auditoría continua y reglas predecibles.

La prioridad será fortalecer y expandir Acuerdos **marco estratégicos** para las categorías críticas de la transformación digital: nube (infraestructura y plataformas), servicios de datos (interoperabilidad, calidad, analítica), ciberseguridad (monitoreo, defensa y resiliencia) e inteligencia artificial/automatización (componentes reutilizables). Este enfoque, tipo "**buy once, use many**", permitirá que una compra bien diseñada y bien auditada se reutilice por entidades nacionales y territoriales, reduciendo tiempos, logrando mejores precios por escala y, sobre todo, elevando el estándar técnico y de seguridad en todo el Estado.

Para que la contratación sea realmente ágil, implementaremos un **catálogo nacional de estándares técnicos y legales pre-aprobados**: arquitecturas permitidas, requisitos mínimos de seguridad, cláusulas tipo, criterios de interoperabilidad y condiciones de portabilidad/evitar dependencia tecnológica. Con esto reducimos la discrecionalidad y la improvisación en los procesos, y damos seguridad jurídica a los equipos de compras y a los órganos de control. El objetivo es que los pliegos de tecnología dejen de "inventarse desde cero" en cada entidad y se conviertan en piezas consistentes, comparables y auditables.

Adicionalmente, crearemos un **sandbox de compras e innovación pública** para tecnologías emergentes (incluida IA): un espacio controlado que permita hacer pruebas de concepto, pilotos de duración limitada y evaluaciones expost rigurosas antes de escalar. El sandbox- no elimina el control; lo concentra, lo mide y lo vuelve aprendizaje institucional. Esto permitirá innovar de manera responsable, con reglas claras de alcance, protección de datos, seguridad, trazabilidad y criterios de éxito medibles.

El programa también abrirá la contratación a más actores, con mecanismos que faciliten la participación de **PYMES, startups y proveedores regionales**, sin bajar la vara de cumplimiento. El Estado debe convertirse en un **cliente inteligente**: capaz de comprar capacidades, evaluar desempeño y escalar lo que funciona, evitando atarse a soluciones cerradas o monolíticas. En tecnología, la competencia real se logra con estándares abiertos, interoperabilidad obligatoria y diseño modular.

Finalmente, llevaremos la transparencia al siguiente nivel mediante **trazabilidad digital completa**: registro de decisiones de compra, evaluaciones técnicas, ejecución contractual y resultados de pilotos; datos abiertos cuando aplique; y auditoría continua basada en información, no solo en papeles. Esto reduce espacios para la opacidad, mejora el control fiscal y disciplinario, y protege a los equipos públicos cuando actúan dentro de reglas claras.

2.3.2. Componente GovTech (Estado como primer cliente)

Además de modernizar reglas y contratos marco, nuestro gobierno convertirá la contratación pública en un motor de **GovTech**: el Estado dejará de ser un comprador lento y fragmentado y pasará a ser el **primer cliente** que acelera la innovación útil para la ciudadanía. Hoy muchas startups y proveedores innovadores no logran venderle al

Estado por barreras de entrada, pliegos hechos para incumbentes, ciclos de compra incompatibles con la velocidad tecnológica y riesgos jurídicos que terminan castigando al servidor público que intenta innovar. El resultado es doblemente costoso: el Estado se queda sin soluciones modernas y el país pierde una oportunidad de construir capacidades tecnológicas propias.

Por eso crearemos un **modelo de compra pública de innovación**, con reglas y rutas claras para adquirir software, analítica e IA por resultados, y no por promesas o licencias cerradas. Esto incluye pilotos cortos con criterios de éxito medibles, escalamiento rápido cuando demuestren valor, y una arquitectura de contratación que privilegie estándares abiertos, modularidad, interoperabilidad y portabilidad para evitar dependencia tecnológica. En la práctica, el Estado comprará capacidades reutilizables ("buy once, use many") para que lo que funciona en una entidad pueda escalarse a nivel nacional y territorial sin volver a contratar desde cero.

El componente GovTech también abrirá la contratación a más actores mediante mecanismos que faciliten la participación de **startups, PYMES tecnológicas y proveedores regionales**, manteniendo exigencias de seguridad y cumplimiento pero eliminando requisitos innecesarios que hoy excluyen a la innovación. Así, el Estado no solo se moderniza: **dinamiza la industria tecnológica nacional**, fortalece soberanía tecnológica y acelera la adopción de soluciones en sectores críticos como salud digital, justicia digital, ciberseguridad, lucha contra la corrupción y pagos digitales.

2.3.3. Lucha contra la corrupción: transparencia automática y control en tiempo real

La corrupción no se combate solo con discursos ni con controles que llegan tarde. Se combate **cerrando las puertas por donde se pierden los recursos**, haciendo que cada peso público deje rastro, y convirtiendo la transparencia en un acto **automático, permanente y verificable**. Hoy, la corrupción se alimenta de tres condiciones: información dispersa, contratación fragmentada y auditorías que reaccionan cuando el daño ya ocurrió. El resultado es un Estado que gasta más, entrega menos y pierde confianza ciudadana.

Nuestro gobierno pondrá en marcha una estrategia de **lucha contra la corrupción apoyada en datos e inteligencia artificial**, basada en un principio: **no esperaremos a que el dinero se pierda para investigar**. Implementaremos un **Sistema de Alertas Tempranas** que vigile cada contrato desde su formulación y durante su ejecución, para identificar en segundos señales de riesgo como "contratos con nombre propio", precios inflados, baja competencia, cambios reiterados, adiciones atípicas, proveedores recurrentes con patrones sospechosos o cronogramas y entregables inconsistentes. La prevención será la regla: cuando el sistema detecte anomalías, activará revisiones obligatorias y trazables antes de comprometer recursos.

Esta estrategia se apalancará en la transformación digital del Estado: **interoperabilidad, identidad digital y trazabilidad**. La interoperabilidad permitirá cruzar información entre SECOP, ejecución presupuestal, interventorías, pagos, registros empresariales, sanciones, antecedentes contractuales y cumplimiento. La identidad digital asegurará que cada actor (funcionario, proveedor, interventor, supervisor) quede claramente identificado, y que cada decisión tenga responsable, fecha y evidencia. La trazabilidad, por su parte, reducirá la discrecionalidad y elevará el estándar de control: cada paso del ciclo contractual quedará auditado por diseño.

La contratación pública será más transparente porque será **más comparable**. Estandarizaremos datos de pliegos, ofertas, precios de referencia y entregables, para que sea fácil detectar desviaciones y para que ciudadanía, medios, academia y órganos de control puedan vigilar con información completa, no con fragmentos. La meta es que el Estado deje de ser una caja negra: el ciudadano debe poder ver, de manera simple, qué se compra, a qué precio, quién ganó, cómo se ejecuta y qué se entregó.

Además, cerraremos espacios tradicionales de corrupción vinculando la estrategia anticorrupción con dos palancas que ya están en el documento: **compras públicas ágiles y abiertas** y **pagos digitales trazables**. La contratación moderna (contratos marco, estándares técnicos y sandboxes) reduce improvisación y dependencia; y los pagos digitales, integrados con identidad y trazabilidad, reducen intermediarios, aceleran tiempos y disminuyen fraude y pagos indebidos.

En esta visión, la lucha contra la corrupción no es un "programa paralelo": es el resultado natural de un Estado que opera como plataforma, con datos de calidad, interoperabilidad y control en tiempo real. La transparencia deja de depender de la voluntad del funcionario y pasa a ser una condición técnica del sistema. Así garantizamos que los recursos públicos se conviertan en obras, servicios y bienestar, y no en despilfarro.

2.3.4. Salud digital: historia clínica interoperable y atención sin papeles, donde estés y cuando la necesites

El sistema de salud en Colombia sigue operando con **información fragmentada**, con historias clínicas que no acompañan al paciente entre prestadores, decisiones médicas tomadas con datos incompletos y trámites presenciales que consumen tiempo, dinero y oportunidades de atención. Esta fragmentación produce **exámenes repetidos**, demoras en diagnósticos, fallas de continuidad en el tratamiento y espacios de fraude, además de elevar costos administrativos para EPS, IPS y el Estado. En paralelo, la telemedicina ha avanzado, pero muchas veces como un servicio aislado y no como parte de un cuidado continuo, integrado a la historia clínica y al seguimiento del paciente.

Nuestro gobierno impulsará una **transformación estructural de la salud digital** para que el ciudadano esté en el centro del sistema y para que la tecnología se traduzca en acceso real, calidad clínica, eficiencia del gasto y transparencia. El corazón de esta transformación será la implementación de una **Historia Clínica Electrónica Nacional Interoperable**, obligatoria para todos los actores públicos y privados del sistema, con estándares únicos y con un principio rector: **la información debe circular con seguridad, no el paciente con papeles**.

La Historia Clínica Interoperable permitirá que, con autorización y bajo reglas claras, cualquier prestador habilitado pueda acceder de forma inmediata a la información relevante del paciente en cualquier lugar del país. Esto reducirá duplicidades, errores clínicos y demoras, y hará posible un modelo de atención verdaderamente continuo: la atención primaria, urgencias, especialistas y hospitalización conectados en un mismo flujo de información. En este modelo, el ciudadano no "pide" la historia clínica ni espera días; la historia clínica está disponible cuando el profesional de salud la necesita para tomar una decisión segura.

Esta transformación vendrá acompañada de un componente clave para cortar trámites y cerrar brechas: una **receta y orden médica electrónica nacional**, válida en todo el país, integrada con el ecosistema de farmacias, laboratorios e inventarios cuando aplique. Con ello se reducen errores de transcripción, se combate el fraude, se habilita

seguimiento y se agiliza la entrega de medicamentos, especialmente para pacientes crónicos.

La salud digital también debe llegar donde hoy el sistema no llega a tiempo. Por eso desplegaremos una **red nacional de telesalud** enfocada en cobertura territorial efectiva, priorizando zonas rurales y de difícil acceso. Pero no será telemedicina "de vitrina": será telemedicina integrada a la historia clínica y al plan de cuidado, con rutas claras de referencia y contrareferencia-, seguimiento y continuidad. La conectividad y la interoperabilidad dejarán de ser un discurso y se convertirán en atención concreta.

A partir de esta base de datos y continuidad clínica, Colombia podrá avanzar en una **estrategia nacional de datos en salud** para prevención y gestión del riesgo: modelos predictivos para detectar tempranamente enfermedades, mejorar el seguimiento de crónicos (diabetes, hipertensión, EPOC), priorizar población de riesgo y orientar recursos donde más impacto generan. En este punto, la **inteligencia artificial** se incorporará como herramienta de apoyo clínico (nunca reemplazo del médico): triage, alertas tempranas, apoyo a notas clínicas y seguimiento, siempre con trazabilidad y estándares éticos.

La implementación será progresiva, pero obligatoria y verificable. Se establecerán **estándares nacionales de interoperabilidad en salud** y un esquema de certificación para proveedores tecnológicos del sector, evitando la proliferación de "silos" incompatibles. Se articularán EPS, IPS, farmacias y laboratorios, y se acompañará al talento humano en formación clínica-digital para asegurar adopción real. La privacidad y la seguridad serán condiciones del sistema: consentimiento informado, control ciudadano sobre accesos y trazabilidad de quién consultó qué y cuándo.

Con esta agenda, la salud digital dejará de ser un conjunto de proyectos aislados y se convertirá en una reforma operativa del sistema: menos papel, menos filas, menos repetición y más oportunidad clínica. El mensaje es simple: **"Salud sin papeles: tu historia clínica donde estés, cuando la necesites."**

2.3.5. Estado seguro: SOC País, respuesta a ciberataques y continuidad de servicios esenciales

La transformación digital solo sirve si es confiable. Un Estado que opera con identidad digital, interoperabilidad, pagos instantáneos y datos en tiempo real se vuelve más eficiente, pero también más expuesto: cada trámite digital, cada base de datos y cada servicio en línea se convierten en un objetivo. Hoy los ataques cibernéticos ya no son un problema "de sistemas": pueden detener hospitales, interrumpir pagos, paralizar trámites, exponer datos sensibles y afectar la confianza ciudadana. Por eso, nuestro gobierno asumirá la ciberseguridad como **prioridad nacional**, entendida como el **sistema inmune del país**: protege servicios esenciales, datos ciudadanos, economía digital y continuidad del Estado.

La situación actual muestra una vulnerabilidad estructural: la seguridad está fragmentada por entidades, hay capacidades dispares y no existe una respuesta integrada con alcance nacional. En muchos casos, la detección es tardía, la coordinación es improvisada y el aprendizaje institucional no se consolida. Esto convierte incidentes puntuales en riesgo sistémico. Un Estado digital sin seguridad termina siendo un Estado frágil; y un Estado frágil abre espacio al crimen, al fraude y al caos operativo.

Nuestro gobierno construirá una capacidad nacional de ciberseguridad **preventiva, coordinada y medible**, con un foco práctico: que los servicios públicos sigan funcionando incluso bajo ataque. La meta es clara: pasar de la reacción tardía a la **detección temprana** y a la **respuesta coordinada**, con protocolos de continuidad operativa que protejan lo que más importa: salud, energía, telecomunicaciones, finanzas, justicia, identidad y pagos públicos.

El primer paso será la puesta en marcha de un **SOC País (Centro Nacional de Operaciones de Seguridad)** como cerebro civil de la ciberdefensa y la respuesta a incidentes. Este SOC tendrá un **modelo federado**: no busca centralizar indiscriminadamente datos ni reemplazar capacidades existentes, sino coordinar y elevar el estándar del Estado completo. Estará conectado con ministerios y entidades públicas, y articulado con operadores de infraestructura crítica (salud, energía, telecomunicaciones y sector financiero), con funciones concretas: monitoreo nacional de amenazas, emisión de alertas tempranas, análisis de riesgo sistémico, coordinación de respuesta, y acompañamiento técnico para contención y recuperación. El país necesita una sala de control digital que opere 24/7, con visión integral.

En paralelo, implementaremos un enfoque **Zero Trust** para el Estado: “nunca confiar, siempre verificar”. Esto significa identidad fuerte, accesos mínimos necesarios, segmentación de sistemas, verificación continua y control granular sobre privilegios de funcionarios, contratistas y proveedores. En un Estado interoperable, el mayor riesgo no es solo el ataque externo: es la combinación de credenciales débiles, accesos excesivos y falta de trazabilidad. Con Zero Trust reducimos la superficie de ataque y evitamos que una intrusión en un punto se convierta en un colapso general.

La tercera línea será la **resiliencia y continuidad operativa** como estándar obligatorio. Cada entidad crítica deberá contar con planes de continuidad digital, respaldos, redundancia y capacidad de recuperación rápida. Esto incluye protocolos de operación degradada (seguir prestando lo esencial, aunque un sistema caiga), pruebas periódicas, y acuerdos claros sobre tiempos máximos de recuperación. Así como existen simulacros físicos para emergencias, el país necesita simulacros digitales para garantizar que el Estado no se apaga cuando lo atacan.

Por eso, instauraremos **cibersimulacros- nacionales anuales** obligatorios, con participación de entidades públicas y operadores críticos. Estos ejercicios evaluarán capacidades reales, detectarán fallas de coordinación y forzarán mejoras con aprendizaje institucional. La ciberseguridad no se “declara”: se entrena y se prueba.

Finalmente, el país debe avanzar hacía un enfoque de **Ciberresilencia,** adoptando modelos y estándares, tales como el Cyber Resilence Act, y elevaremos el estándar del ecosistema completo con un esquema de **certificación de ciberseguridad para proveedores del Estado**. No es razonable exigir seguridad en entidades públicas si el software, la nube o los servicios contratados no cumplen requisitos mínimos verificables. La certificación será condición para contratar en categorías críticas (software, infraestructura, nube y servicios administrados), reduciendo dependencias riesgosas y mejorando la calidad del mercado.

Esta agenda se articulará con los demás ejes del plan: identidad digital (autenticación fuerte), interoperabilidad (trazabilidad y control de accesos), compras públicas (estándares preaprobados y cláusulas de seguridad) y lucha contra la corrupción (detección de fraude y anomalías). En conjunto, construiremos un Estado que digitaliza para servir mejor, pero que también **se protege para no fallar**.

2.3.6. Gemelo Digital de Colombia: el “tablero de control” para decidir con evidencia y coordinar el territorio

Colombia necesita pasar de planear con información fragmentada y desactualizada a gobernar con evidencia en tiempo real. Hoy, muchas decisiones de infraestructura, uso del suelo, gestión del riesgo, ambiente y productividad rural se toman con datos dispersos, en formatos incompatibles y con baja coordinación entre Nación y territorio. Eso hace que el Estado llegue tarde: se reacciona a desastres en vez de prevenirlos; se invierte sin priorización fina; se duplican esfuerzos; y se pierde capacidad de anticipar fenómenos como crisis hídricas, degradación ambiental, fallas en infraestructura o expansión desordenada del suelo. Además, los programas públicos suelen escalar sin un “laboratorio” previo para probar escenarios y medir impacto antes de gastar a gran escala.

Nuestro gobierno impulsará el **Gemelo Digital de Colombia (GDC)** como una herramienta estratégica: un **modelo digital vivo del territorio nacional** que integra datos oficiales y observaciones (catastro, infraestructura, sensores, satélite y clima) para **planificar, simular escenarios y monitorear en tiempo casi real** sectores críticos. La idea es simple y poderosa: **antes de construir, intervenir o escalar un programa, el país lo prueba en digital**. Menos improvisación, más resultados; menos intuición, más evidencia; menos reacción tardía, más prevención.

El Gemelo Digital no será “otro mapa” ni un repositorio adicional. Será una **arquitectura por capas**, modular y federada, construida sobre el **Marco Nacional de Interoperabilidad** y con reglas de gobernanza claras. Sus capas base incluirán el “territorio oficial” (catastro multipropósito, uso del suelo, límites, servidumbres, áreas protegidas, zonas de riesgo e inventario de infraestructura), y se complementarán con capas de observación (imágenes satelitales, señales de cambios en cobertura vegetal y cuerpos de agua, estaciones hidrometeorológicas y sensores donde aplique). Sobre esa base se construirán capas funcionales: clima-agua-riesgo; gestión de infraestructura; monitoreo ambiental; y un componente decisivo: un **simulador de políticas y pilotos** para evaluar exante y -expost- qué funciona, dónde y por qué.

El GDC permitirá focalizar inversiones y coordinar decisiones con transparencia. Por ejemplo, ayudará a priorizar vías terciarias con criterios combinados de productividad, conectividad y riesgo; a planear infraestructura de agua según demanda y escenarios climáticos; a mejorar la gestión del riesgo con alertas integradas y simulación de impacto; y a fortalecer el control ambiental con monitoreo de deforestación y detección temprana de cambios anómalos que ameriten inspección en campo. En el agro, el Gemelo Digital habilitará un enfoque de **agro de precisión como servicio público de datos**, con información sobre aptitud de suelos, humedad, estrés hídrico y alertas tempranas agregadas, conectadas con asistencia técnica y seguros agro, siempre con consentimiento cuando aplique a nivel predial.

Como principio central, el Gemelo Digital será un instrumento para **mejor política pública, no para vigilancia masiva**. Operará con minimización de datos personales, trazabilidad de accesos y una política de acceso por capas: componentes públicos (ambiente, riesgo, infraestructura) y componentes sensibles con acceso restringido, controlado y auditable (por ejemplo, ubicaciones críticas). Cualquier uso asociado a seguridad territorial deberá estar delimitado por reglas, debido proceso, supervisión y auditoría: el objetivo es coordinar presencia institucional y prevención basada en evidencia, no automatizar decisiones coercitivas.

La implementación será progresiva para evitar el error del "megaproyecto inmanejable". Iniciaremos con **pilotos de alto impacto en 2–3 territorios priorizados** (por ejemplo: un corredor de deforestación, una cuenca hídrica crítica y una región agroproductiva), con resultados medibles y escalamiento sectorial posterior. En paralelo, consolidaremos gobernanza: un consejo de gobernanza del Gemelo Digital (Nación–territorios–academia–privados) con roles claros, un catálogo nacional de datos con responsables y estándares de calidad, y mecanismos de auditoría para modelos predictivos.

Con el Gemelo Digital de Colombia, el Estado gana capacidad real de anticipar, coordinar y decidir mejor. El país planifica con datos reales, pruebas políticas antes de gastar, protege el territorio y mejora la inversión pública. En pocas palabras: **un tablero de control nacional para gobernar con evidencia.**

2.3.7. Pagos y billetera digital: el Estado paga y cobra en segundos, sin intermediarios y con trazabilidad total

En Colombia, demasiados pagos del Estado siguen llegando tarde, con costos ocultos, filas, intermediarios y espacios para el fraude. Lo mismo ocurre con cobros y recaudos: trámites innecesarios, canales dispersos y baja trazabilidad. Esa fricción castiga sobre todo a quien más necesita al Estado: hogares vulnerables, población rural y ciudadanos lejos de oficinas bancarias. Un Estado moderno no puede prometer eficiencia si no es capaz de **pagar a tiempo** y **cobrar de forma simple**.

Nuestro gobierno pondrá en marcha un programa nacional de **Pagos Digitales del Estado y Billetera Digital Interoperable**, para que el Estado pueda **girar transferencias, subsidios, devoluciones y apoyos en tiempo real (T+0)** y para que el ciudadano pueda pagar tasas, contribuciones y servicios públicos desde el celular, sin filas y sin costos abusivos. La idea es directa: **que los recursos públicos lleguen al ciudadano en segundos**, con claridad total y con auditoría permanente.

La billetera digital no será un monopolio estatal ni una aplicación obligatoria única. Será un **ecosistema interoperable**: el ciudadano podrá escoger su proveedor (banco, fintech u operador autorizado), pero todos deberán cumplir estándares comunes de interoperabilidad, seguridad, trazabilidad y protección de datos. El Estado se conectará a ese ecosistema para ejecutar pagos masivos y recaudos de bajo valor con reglas claras, evitando la fragmentación actual y reduciendo costos de operación.

Esta política se apoya en tres pilares que ya están en el plan: **identidad digital**, **interoperabilidad** y **lucha contra la corrupción**. Los pagos estarán asociados a **identidad verificada**, lo que reduce suplantación y filtraciones; la interoperabilidad permitirá validar condiciones y activar pagos automáticamente cuando se cumplan requisitos, sin trámites; y la trazabilidad digital permitirá detectar anomalías y prevenir pagos indebidos antes de que ocurran. En términos prácticos, el Estado deja de pedir papeles y empieza a operar con reglas y datos.

El programa también impulsará una transformación del gasto social: migrar de "pagos con intermediación y verificación manual" a **pagos automáticos basados en elegibilidad**, integrados a la Carpeta Ciudadana. Eso significa que el ciudadano podrá ver por qué recibe un beneficio, cuándo se paga, en qué estado va y qué hacer si hay un error. Más transparencia para la gente y mejor control para el Estado.

En territorio, el diseño tendrá enfoque de inclusión real. Habrá mecanismos para población sin smartphone o con conectividad limitada (canales asistidos, puntos de atención y esquemas de operación con sincronización posterior cuando aplique), porque

la digitalización no puede excluir. Y la ciberseguridad será condición de operación: autenticación fuerte, prevención de fraude, monitoreo continuo y coordinación con el **SOC País** para proteger pagos públicos como infraestructura crítica.

Con este programa, Colombia gana cuatro resultados inmediatos: (i) el ciudadano recibe recursos más rápido y con claridad; (ii) el Estado reduce pérdidas por fraude y pagos indebidos; (iii) se baja el costo de operación de programas masivos; y (iv) se acelera la formalización y la inclusión financiera, porque el Estado se vuelve un habilitador práctico de la economía digital.

2.3.8. Educación digital: escuelas conectadas, docentes fortalecidos y aprendizaje para el siglo XXI

La educación pública no puede seguir dependiendo de la suerte del territorio donde nace un niño. Hoy la brecha educativa también es una brecha digital: infraestructura desigual, conectividad intermitente o inexistente en miles de sedes, falta de equipos y plataformas sostenibles, y una adopción tecnológica que muchas veces se limita a entregar dispositivos sin garantizar uso pedagógico. Eso perpetúa desigualdad, baja productividad futura y desconexión entre lo que se enseña y lo que el mundo del trabajo exige.

Nuestro gobierno impulsará una política de **Educación Digital** centrada en resultados: que cada estudiante aprenda más y mejor, que cada docente tenga herramientas reales para enseñar, y que la tecnología se convierta en un puente para cerrar brechas, no en otra forma de exclusión. La meta es clara: pasar de “digitalizar por entregar” a **transformar por aprender**.

El primer eje será garantizar **conectividad educativa efectiva** como infraestructura social estratégica. Las sedes educativas —especialmente rurales— serán anclas prioritarias: conectividad con estándares medibles de disponibilidad y calidad, acompañada de soluciones de energía y continuidad donde se requiera. No se trata de “poner internet”, sino de asegurar que funcione para clases, contenidos y evaluación, y que se sostenga en el tiempo. La conectividad educativa será el punto de partida para habilitar educación híbrida, acceso a contenidos, formación docente y servicios digitales del Estado en la comunidad.

El segundo eje será un **salto en formación docente**, porque ninguna transformación educativa ocurre si el docente queda solo. Implementaremos un programa nacional de fortalecimiento docente para uso pedagógico de tecnología e inteligencia artificial: planeación de clases, evaluación formativa, personalización del aprendizaje y apoyo a estudiantes con dificultades, siempre con criterios éticos y de protección de datos. Construiremos una red de **docentes multiplicadores** para escalar capacidades por territorio y asegurar que la innovación llegue al aula, no se quede en documentos.

El tercer eje será un **currículo actualizado para el siglo XXI**. Actualizaremos el CONPES de “Tecnologías para educar” (3988 de 2020) y lo convertiremos en un Plan Nacional de Educación en Tecnología que prepare a estudiantes y trabajadores para los desafíos del trabajo moderno. Esto implica integrar de manera transversal competencias en pensamiento crítico digital, datos, programación, ciudadanía digital y fundamentos de inteligencia artificial. No para “formar programadores” únicamente, sino para formar ciudadanos y trabajadores capaces de usar tecnología con criterio, productividad y responsabilidad.

El cuarto eje será infraestructura y ecosistema digital con sostenibilidad: hardware, software y plataformas, pero bajo un modelo que evite compras fragmentadas y soluciones que no conversan entre sí. La educación digital debe apoyarse en interoperabilidad y estándares, para que los sistemas educativos puedan medir avance, identificar rezagos y orientar recursos con evidencia. La tecnología educativa debe ser simple para el usuario, segura, escalable y reutilizable entre territorios.

Finalmente, la educación digital estará conectada con empleo y productividad. Promoveremos **semilleros de talento**, rutas técnicas y tecnológicas, laboratorios y espacios de aprendizaje digital que conecten escuela, SENA, universidades y sector productivo. La apuesta es que los jóvenes salgan con capacidades demostrables y que el país reduzca la brecha entre educación y demanda laboral, especialmente en competencias digitales y de IA.

En síntesis: Educación digital no es repartir equipos; es garantizar conectividad real, docentes fortalecidos, currículo actualizado, aprendizajes significativos, competencias globales y un ecosistema interoperable.

2.3.9. Seguridad: tecnología como multiplicador de fuerza para proteger la vida y recuperar el territorio

Difícilmente existe un sector donde la tecnología pueda generar un impacto mayor e inmediato que en la seguridad. Colombia enfrenta redes criminales adaptativas, economías ilícitas y violencia que se alimentan de la falta de información integrada, de la reacción tardía y de la debilidad para anticipar y cerrar corredores de ilegalidad. Hoy, gran parte del Estado llega tarde: cuando el delito ya ocurrió, cuando la extorsión ya paralizó el comercio o cuando la minería ilegal ya destruyó el territorio. Para cambiar esta realidad, la seguridad debe pasar de ser una operación fragmentada y reactiva a una estrategia **proactiva, predictiva y coordinada**, apoyada en datos en tiempo real.

Nuestro gobierno impulsará una agenda de **Seguridad Inteligente**: un modelo donde la tecnología actúa como **multiplicador de fuerzas** para desmantelar redes criminales, proteger a la ciudadanía y fortalecer la presencia institucional. Esto no significa reemplazar a la Fuerza Pública: significa darle mejores capacidades para ver antes, decidir mejor y actuar con precisión. La prioridad será integrar analítica avanzada e inteligencia artificial para identificar patrones criminales, detectar anomalías en flujos financieros ilícitos, anticipar riesgos y optimizar la focalización operativa en puntos críticos.

El primer cambio será construir un sistema de **comando y control digital** con información oportuna y compartida. Fortaleceremos centros de mando que procesen y transmitan datos en tiempo real a las autoridades, articulando infraestructura de video, sensores y fuentes disponibles, con analítica que permita priorizar incidentes, asignar recursos y reducir tiempos de respuesta. Con ello, pasamos de operaciones basadas en reportes dispersos a operaciones basadas en evidencia, con trazabilidad y medición del impacto.

El segundo cambio será usar la IA para pasar de la reacción a la prevención estratégica. Al procesar grandes volúmenes de información, la analítica predictiva permite identificar zonas y ventanas de riesgo, patrones de movilidad criminal y señales tempranas de escalamiento. Esto habilita un despliegue más inteligente, evita improvisación y aumenta la eficacia: menos patrullaje “ciego”, más presencia focalizada donde el riesgo es mayor y donde la ciudadanía necesita protección real.

El tercer cambio será atacar las economías ilegales con herramientas modernas. La criminalidad se sostiene por financiamiento, logística y control territorial. Por eso, fortaleceremos capacidades para detectar flujos financieros anómalos, redes de lavado y patrones de contratación o provisión que alimentan ilegalidad, articulando esfuerzos con entidades de control y con el enfoque de lucha contra la corrupción. En paralelo, integraremos información territorial (incluyendo capacidades tipo Gemelo Digital donde aplique) para mejorar control sobre corredores, puntos de extracción ilegal y afectaciones ambientales, orientando intervención estatal con evidencia.

Esta estrategia se regirá por un principio innegociable: **seguridad con legalidad y derechos**. La tecnología debe aumentar la eficacia del Estado sin convertirse en abuso. Por eso, cualquier uso de analítica, sensores o automatización tendrá reglas claras de acceso, trazabilidad, auditoría y control institucional. La tecnología será un medio para proteger a la ciudadanía y reducir violencia, no un instrumento para decisiones opacas o discrecionales.

Con Seguridad Inteligente, Colombia avanzará hacia un Estado que protege mejor: más rápido ante emergencias, más preciso contra estructuras criminales, más fuerte en control territorial y más confiable para la vida cotidiana, el comercio, el turismo y la convivencia. Si el Estado logra anticipar y coordinar, la ciudadanía recupera tranquilidad; y cuando la tranquilidad regresa, la economía y la vida social vuelven a florecer.

2.3.10. Justicia digital: expediente único, audiencias sin barreras y decisiones más rápidas con transparencia

La justicia en Colombia no puede seguir funcionando con la velocidad del papel. Hoy el ciudadano enfrenta demoras, trámites repetidos, información fragmentada entre despachos y jurisdicciones, y barreras de acceso que castigan más a quienes viven lejos de las cabeceras o no tienen capacidad de pagar intermediarios. Esa lentitud no es solo un problema administrativo: afecta seguridad jurídica, inversión, convivencia y confianza en el Estado. La justicia tardía es injusticia, y un país con justicia lenta pierde competitividad y cohesión social.

Nuestro gobierno impulsará una **Justicia Digital** para que el sistema responda con mayor oportunidad, transparencia y accesibilidad, respetando siempre el **Estado de Derecho, el debido proceso y la autonomía judicial**. La tecnología no será un fin; será el medio para que jueces y operadores judiciales puedan concentrarse en lo esencial: decidir mejor y a tiempo, con información completa y procesos menos burocráticos.

El corazón de esta transformación será el **Expediente Judicial Digital** como estándar nacional: un expediente único, trazable y seguro, que acompañe el caso de principio a fin y que elimine la dependencia del papel. Este expediente permitirá organizar grandes volúmenes de información, evitar pérdidas o duplicidades, y acelerar tareas administrativas que hoy consumen el tiempo de los despachos. Para lograrlo, estableceremos **estándares comunes de datos y de gestión documental** para que las diferentes jurisdicciones “hablen el mismo idioma” y la información no quede atrapada en sistemas incompatibles.

Sobre esa base, promoveremos la adopción de **herramientas de analítica e inteligencia artificial** para mejorar eficiencia sin afectar garantías. La IA se usará como apoyo en tareas repetitivas y de alto volumen —clasificación y priorización de documentos, búsqueda inteligente de antecedentes, organización de evidencias, alertas de vencimientos y control de términos—, de modo que el juez recupere tiempo para

deliberar y decidir. La regla será clara: la IA **no reemplaza la decisión judicial**, la fortalece con orden, trazabilidad y productividad.

La justicia digital también debe democratizar el acceso. Por eso, consolidaremos un modelo de **audiencias virtuales y servicios judiciales digitales** que reduzca desplazamientos y costos para ciudadanos, testigos y víctimas, especialmente en regiones apartadas. Esto no significa "virtualizar por virtualizar": significa que la virtualidad sea una opción robusta, segura y útil, integrada al expediente digital y con reglas claras para proteger derechos, confidencialidad y seguridad procesal.

Esta modernización se complementará con un impulso decidido a **LegalTech** y a la innovación regulada dentro del sistema judicial. Promoveremos soluciones tecnológicas que simplifiquen notificaciones, gestión de agenda, interoperabilidad de información relevante (cuando proceda) y atención al ciudadano. En paralelo, fortaleceremos competencias digitales de funcionarios y operadores para asegurar adopción real y sostenibilidad operativa.

Con Justicia Digital, Colombia avanza hacia un sistema más confiable: menos congestión, más transparencia, mejores tiempos y acceso real sin barreras físicas. En últimas, una justicia moderna no solo decide; **resuelve a tiempo**, protege derechos y entrega la seguridad jurídica que necesita la vida cotidiana y la economía del país.

2.3.11. Liderazgo tecnológico y construcción de capacidades tecnológicas, de ciencia y de innovación

Colombia no puede aspirar a liderar la transformación digital —ni a usar la inteligencia artificial para mejorar productividad, seguridad, salud o educación— si depende estructuralmente de tecnología, talento y capacidad computacional importada. El liderazgo tecnológico no es aislamiento ni proteccionismo: es **capacidad real de elegir**, de construir y de negociar en igualdad de condiciones; es poder adoptar tecnología global sin quedar atrapados en dependencias, y al mismo tiempo desarrollar capacidades propias que generen valor, empleo y exportaciones. Un país que no puede construir, adaptar y auditar su tecnología termina siendo un consumidor pasivo de soluciones externas, sin control pleno sobre costos, continuidad, seguridad y uso de datos.

Hoy el país enfrenta una "trampa de dependencia": inversión insuficiente en I+D, baja articulación entre universidad–empresa–Estado, barreras regulatorias que frenan experimentación, y una adopción desigual donde solo algunos sectores avanzan mientras la mayor parte del tejido productivo y los territorios quedan rezagados. A esto se suma un cuello de botella adicional: sin acceso democratizado a servicios de nube, datos de calidad y capacidad de cómputo, la IA se vuelve un privilegio de pocos. Por eso, nuestro gobierno impulsará un eje de soberanía tecnológica que no se quede en diagnóstico, sino que se traduzca en **capacidad instalada**, **instituciones habilitantes** y **mercados que compran innovación local**.

El primer frente será elevar de manera decidida la inversión y los incentivos a la innovación aplicada. Pondremos en marcha un **Pacto Fiscal por la Innovación** para movilizar inversión privada en I+D+i (especialmente en IA, ciberseguridad, datos, GovTech y tecnologías para salud, agro, educación y justicia), con incentivos tributarios claros y simples, y con cofinanciación orientada a resultados. No basta con convocatorias dispersas: se necesita una apuesta sostenida y medible para construir capacidades tecnológicas nacionales, aumentar patentes y convertir investigación en productos, servicios y empleo de calidad.

El segundo frente será crear condiciones para experimentar sin que la burocracia mate la innovación. Implementaremos **sandboxes regulatorios y sectoriales** ("zonas libres de burocracia") para que startups y empresas puedan probar soluciones en entornos controlados, con supervisión, reglas claras y evaluación, antes de escalar. Esto permite innovar con responsabilidad y, a la vez, ajustar regulación con evidencia real, evitando copiar modelos externos que superan nuestra capacidad institucional o frenan el emprendimiento.

El tercer frente será convertir al Estado en dinamizador del ecosistema tecnológico: el **Estado como primer cliente**. No hay industria tecnológica robusta si el comprador más grande del país compra tarde, compra aislada o compra cerrando la competencia. Por eso, alinearemos **compras públicas ágiles y abiertas** con soberanía tecnológica: estándares abiertos, modularidad, interoperabilidad obligatoria y requisitos de portabilidad para evitar dependencias. Además, se impulsarán esquemas de compra pública de innovación y pilotos de alto impacto para que soluciones con componente local puedan probarse y escalarse en salud, justicia, educación, seguridad y lucha contra la corrupción, incluyendo el fortalecimiento de SECOP con capacidades de analítica e IA para detectar anomalías.

El cuarto frente será democratizar el acceso a infraestructura digital crítica. La soberanía tecnológica también se construye garantizando que la base productiva —pymes, emprendimientos, universidades y territorios— pueda acceder a **servicios en la nube y cómputo** a costos razonables. Promoveremos esquemas de "nube para la base productiva" y capacidades compartidas donde aplique, articuladas con conectividad efectiva y ciberseguridad, para que la innovación no se concentre en pocas ciudades o en pocas empresas.

Finalmente, consolidaremos una estrategia de capacidades humanas y científicas alineada con las necesidades del país. La formación y el reentrenamiento en IA y tecnología (docentes, funcionarios, pymes y jóvenes) serán un pilar transversal, pero también lo será el fortalecimiento de capacidades avanzadas: investigación aplicada, transferencia tecnológica, centros de excelencia y redes regionales de innovación. El objetivo es que Colombia no solo "use" tecnología, sino que **la entienda, la audite, la adapte y la exporte**, elevando productividad, reduciendo dependencia y construyendo una economía del conocimiento con base territorial.

2.3.12. Fortalecimiento de la tecnología para las mujeres

Establecer acciones para combatir la violencia de género en entornos digitales o en entornos escolares, comunitarios, familiares y laborales con apoyo en las TIC requiere un enfoque multidisciplinario que combine **herramientas tecnológicas**, l**egislación, divulgación, educación y atención psicosocial a** fin de pasar de simples campañas a convertirse en políticas públicas sostenibles y de largo plazo

Una propuesta programática debe considerar por lo menos, 4 ejes estratégicos:

2.3.12.1 Eje de Prevención.

El objetivo es transformar la cultura con base en plataformas TIC o digitales, enfocándose en la educación y la sensibilización.

- **Programa "Escuelas de Ciber-Respeto":** Integraremos en el currículo nacional de educación básica y media módulos de alfabetización digital con enfoque de género. No solo enseñaremos a usar herramientas, sino a identificar el acoso, el *grooming* y la violencia simbólica en línea.
- **Laboratorio Audiovisual "Narrativas de Libertad y sin Violencias":** Se financiarán concursos para que creadores de contenido, *influencers* y cineastas, canales de televisión, programadoras, y en general el ecosistema audiovisual produzcan piezas (cortometrajes, TikToks, sketchs, podcasts) que desmitifiquen el amor romántico tóxico, promuevan la seguridad digital y trabajen contenidos para combatir la violencia de genero. Además de los premios otorgados, sus resultados deberán incorporarse en la radio, TV nacional y regional y en horas PRIME
- **Certificación de "Institución Segura":** Crearemos un sello gubernamental para plataformas y organizaciones que implementen protocolos internos estrictos contra el acoso laboral digital y promuevan entornos seguros para las mujeres y las niñas.

2.3.12.2 Eje de Respuesta Tecnológica y Atención a Víctimas

Utilizaremos la tecnología como una herramienta de protección y no solo como el escenario del riesgo.

- **App "Red de Cuidados 24/7":** Tendremos una plataforma oficial que incluya:
  - **Botón de pánico silencioso** con geolocalización.
  - **Bóveda segura de evidencia:** Espacio en la nube con validez legal para almacenar capturas de pantalla, audios y enlaces de ataques digitales, evitando que la víctima los borre por miedo.
  - **Chatbot de IA con perspectiva de género:** Para triage inicial y contención emocional inmediata.
- **Unidad Móvil de "Primeros Auxilios Digitales":** Crearemos equipos técnicos y legales que recorran comunidades para ayudar a mujeres a configurar la privacidad de sus dispositivos, eliminar contenido íntimo compartido sin consentimiento y rastrear brechas de seguridad.

2.3.12.3 Eje de Justicia y Fortalecimiento Institucional

Modernizaremos el aparato estatal para que la denuncia digital no termine en impunidad.

- **Fiscalía Especializada en Delitos Informáticos de Género:** Crearemos unidades fiscales con peritos informáticos capacitados específicamente en violencia contra las mujeres (rastreo de IPs, análisis forense de dispositivos).
- **Protocolo "Ventanilla Única contra la Violencia de Género":** Unificaremos digitalmente y en línea los sistemas de denuncia de la policía, la fiscalía, comisarías de familia y los Casas de justicia para que la víctima no tenga que repetir su historia (revictimización) y se pueda dar seguimiento en tiempo real al caso.
- **Observatorio Nacional de Violencia Digital:** Tendremos una plataforma de *Big Data* que analice tendencias de acoso en redes sociales y foros para generar alertas tempranas y diseñar políticas basadas en evidencia real.