Gobierno de Colombia

ESTRATEGIA NACIONAL DE

SEGURIDAD DIGITAL DE COLOMBIA 2025 - 2027

Gobierno de Colombia

Presidencia de la República

Saúl Kattan Cohen
Coordinador Nacional de Seguridad Digital

Ingrid Paola Hernández Sierra
Coordinadora del Grupo de Transformación Digital

Manuel Humberto Sierra López
Asesor del Grupo de Transformación Digital

Diana Marcela Arias Rojas
Asesora del Grupo de Transformación Digital

Pedro Pablo Gonzalez Barrera
Asesor del Grupo de Transformación Digital

Agradecimientos:
Viviana Vanegas
Directora de Desarrollo Digital del Departamento Nacional de Planeación

Grupo Interno de Trabajo de Prevención del Delito del Ministerio de Relaciones Exteriores

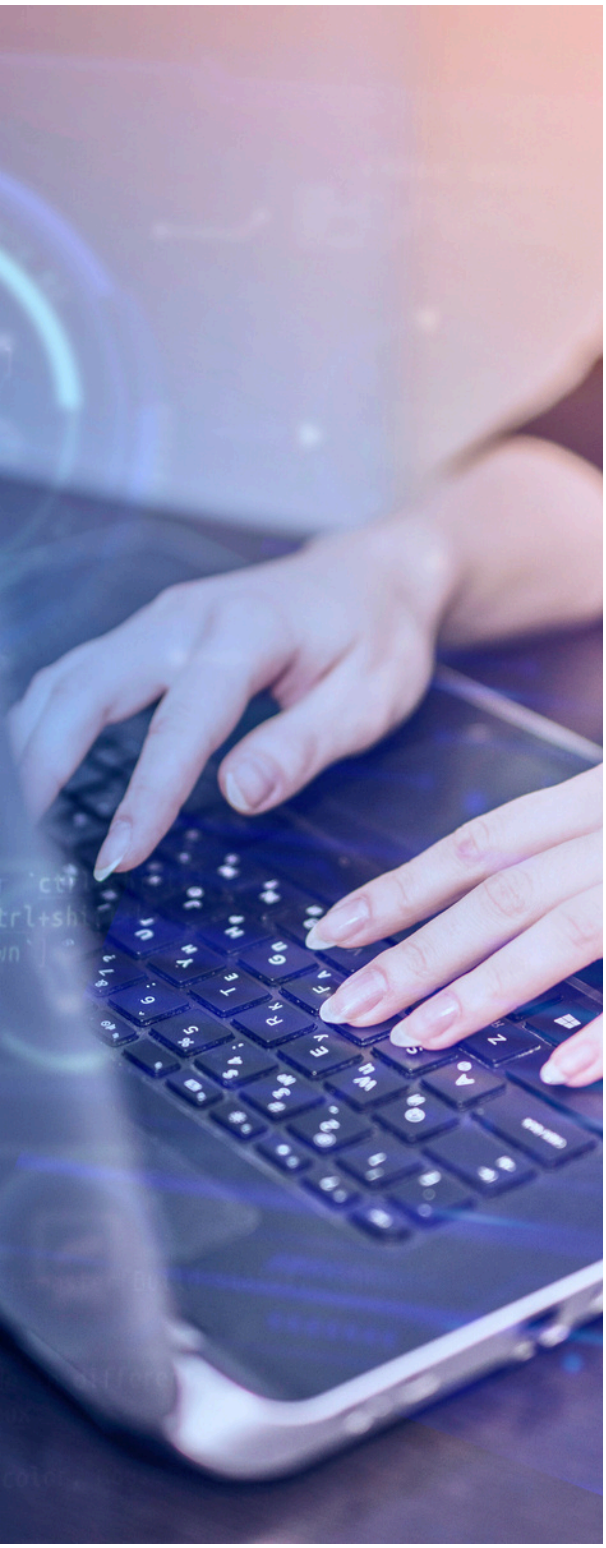
Con el objetivo de fortalecer la seguridad digital del país, el Coordinador de Seguridad Digital, presenta recomendaciones a través de la Estrategia Nacional de Seguridad Digital a todas las partes interesadas. Esta iniciativa permitirá, en un mundo hiperconectado donde los riesgos cibernéticos amenazan todas las infraestructuras críticas y servicios esenciales, establecer una política de protección integral del ecosistema digital del país y de sus ciudadanos. Para lograrlo, se ha tenido en cuenta el estado actual de las capacidades de seguridad digital en Colombia, así como las mejores prácticas internacionales y regionales para mejorar las capacidades nacionales en esta materia. Todo ello, teniendo como enfoque central el bienestar del ser humano y la sociedad en su conjunto.

La colaboración y el apoyo de la sección de ciberseguridad de la Secretaría del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos, así como del sector público, las diversas entidades del Estado, la academia y la sociedad civil, fueron fundamentales para lograr una Estrategia Nacional de Seguridad Digital sólida y coherente, que respalde las políticas públicas del Gobierno Nacional y su Plan de Desarrollo. Su participación y compromiso han sido esenciales para el éxito de esta iniciativa, garantizando un futuro más seguro y próspero para todos.

“LA SEGURIDAD NO ES ALGO QUE SE ESPERA, ES ALGO QUE SE PLANEA.”

Anónima

Marzo 2025



CONTENIDO

I. INTRODUCCIÓN

En la era digital actual, la seguridad digital se ha convertido en un pilar fundamental para el desarrollo socioeconómico y la estabilidad nacional de Colombia. **La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027** se presenta como una respuesta integral y proactiva a los desafíos y oportunidades que surgen en un entorno digital en constante evolución.

Esta estrategia se construye sobre los cimientos establecidos por los documentos CONPES 3701 de 2011, 3854 de 2016 y 3995 de 2020, los cuales han guiado la política de seguridad digital del país en la última década. Reconociendo los avances logrados y las lecciones aprendidas, esta nueva estrategia busca **fortalecer la postura de Colombia en materia de seguridad digital, adaptándose a las amenazas emergentes** y aprovechando las innovaciones tecnológicas para crear un ciberespacio más seguro y resiliente.

La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 se fundamenta en cuatro enfoques rectores: el **enfoque de "Toda la Sociedad"**, que promueve la colaboración multisectorial; el **enfoque Centrado en el Ser Humano,** que prioriza la protección de los derechos digitales; el **enfoque de Gestión de Riesgos cibernéticos,** que fortalece la resiliencia nacional; y el **enfoque de Innovación y Desarrollo de Capacidades,** que impulsa la investigación y la formación en ciberseguridad.

A partir de estos enfoques, se busca lograr cuatro objetivos específicos: consolidar la gobernanza de seguridad digital, mejorar la ciber resiliencia nacional, desarrollar la fuerza laboral de seguridad digital, y adaptar y adecuar el marco normativo cibernético. Cada uno de estos objetivos se desglosa en líneas de acción concretas, diseñadas para abordar los desafíos identificados y aprovechar las oportunidades emergentes en el panorama digital.

Al adoptar un enfoque integral que abarca desde la protección de infraestructuras críticas cibernéticas y servicios esenciales, hasta el desarrollo de capacidades humanas, esta estrategia busca no solo fortalecer la seguridad digital de Colombia, sino también **posicionar al país como un referente regional** en la materia. Con un compromiso firme con la innovación, la colaboración multisectorial y la protección de los derechos digitales, Colombia se prepara para enfrentar los retos del ciberespacio y aprovechar las oportunidades de la era digital, contribuyendo así a un futuro más seguro y próspero para todos sus ciudadanos.

El Gobierno de Colombia confirma su compromiso para mantener un ciberespacio seguro a partir de la formulación de este documento estratégico, y agradece el apoyo técnico especializado de la Sección de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA/CICTE).

II. CONTEXTO

En el contexto global, la seguridad digital se ha convertido en una preocupación primordial para gobiernos, empresas y ciudadanos en todo el mundo. El año 2024 ha sido testigo de un aumento significativo en la sofisticación y frecuencia de los incidentes cibernéticos y ciberataques, impulsados en gran medida por la adopción generalizada de tecnologías emergentes como la Inteligencia Artificial (IA) y la computación cuántica. **Actualmente, se aprecia un incremento en el uso de IA por parte de los atacantes para evadir los sistemas de detección,** así como un aumento en las actividades de hacktivismo relacionadas con conflictos globales. Además, la escasez global de profesionales de seguridad digital sigue siendo un desafío crítico, con una fuerza laboral que lucha por mantenerse al día con la evolución constante de las amenazas.

En América Latina y el Caribe, la situación de la seguridad digital refleja tanto avances como desafíos persistentes. Los países de la región han mostrado progresos dispares en sus capacidades de seguridad digital. No obstante, la región en su conjunto enfrenta desafíos críticos en áreas como la implementación de políticas nacionales coherentes y el desarrollo de capacidades tecnológicas para proteger infraestructuras críticas cibernéticas y servicios esenciales.

En el contexto nacional, Colombia ha demostrado un compromiso activo en la formulación de políticas nacionales que tienen relación con la ciberseguridad,la ciberdefensa y la seguridad digital, como lo evidencian los documentos CONPES 3701 de 2011[1], 3854 de 2016[2] y 3995 de 2020[3]. El país ha sido reconocido como uno de los líderes regionales en el desarrollo de marcos normativos y estrategias de seguridad digital. Sin embargo, Colombia enfrenta desafíos significativos en la implementación efectiva de estas políticas.

Los recientes incidentes cibernéticos tanto a organizaciones públicas como privadas han puesto de manifiesto la vulnerabilidad persistente de las infraestructuras críticas cibernéticas y servicios esenciales. Estos incidentes evidencian la brecha entre la formulación de políticas y su ejecución práctica, revelando debilidades en la coordinación institucional, la capacidad de respuesta a incidentes y la protección de infraestructuras críticas cibernéticas y servicios esenciales. A pesar de los esfuerzos normativos, Colombia continúa luchando para traducir sus ambiciosas políticas en acciones concretas y efectivas, evidenciando la dificultad del país para pasar de la planificación a la implementación robusta de medidas de seguridad digital.

Según los resultados de la aplicación del Modelo de Madurez de Capacidades de Seguridad Cibernética[4] por parte de la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), se evidenció un avance integral entre 2016 y 2020 de todas las dimensiones que, en conjunto, constituyen la amplitud de la capacidad nacional que un país requiere para ser eficaz en la prestación de servicios de seguridad digital.

De manera similar y según las mediciones del Global Cybersecurity Index (GCI[5] de la Unión Internacional de Telecomunicaciones-UIT), se aprecia una evolución positiva entre 2020 y 2024 en aspectos relacionados con Medidas Legales. Sin embargo, existen áreas con progresos limitados e incluso retrocesos, como es el caso de las Medidas Técnicas y Medidas de Cooperación, donde se observa un decremento en el nivel de madurez.

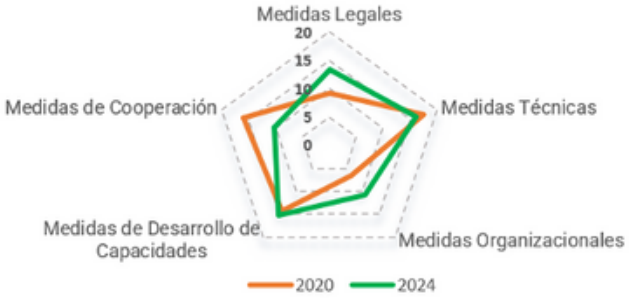
[1] La política nacional expedida en el año 2011 (CONPES 3701) concentró los esfuerzos del país en la creación y aplicación de unos lineamientos orientados a desarrollar una estrategia nacional en materia de ciberseguridad y ciberdefensa, con el fin de fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando la institucionalidad, el ambiente y las condiciones necesarias para brindar protección en el ciberespacio. Estos avances permitieron un posicionamiento importante de Colombia a nivel internacional en torno al tema. En consonancia con la evolución del panorama de amenazas, dicha estrategia nacional se revisó durante los años 2014 y 2015, logrando expedir una nueva política nacional en torno al tema.

[2] La política nacional de seguridad digital en Colombia expedida en el año 2016 (CONPES 3854) articuló una visión estratégica en el Gobierno nacional, diferenció los objetivos de prosperidad económica y social con los objetivos de defensa del país y de lucha contra el crimen y la delincuencia en el entorno digital, inició el establecimiento de un marco institucional articulado e inició un proceso para que los ciudadanos en el país hicieran un uso responsable del entorno digital y fortalecieran sus capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

[3] La política nacional de confianza y seguridad digital en Colombia expedida en el año 2020 (CONPES 3995) El documento CONPES 3995 de 2020 establece la Política Nacional de Confianza y Seguridad Digital en Colombia, con el objetivo de fortalecer la confianza y la seguridad en el entorno digital. Esta política busca desarrollar un ambiente digital seguro y confiable que maximice los beneficios económicos y sociales para todos los actores públicos y privados, impulsando la competitividad y productividad en todos los sectores de la economía13. El documento propone medidas para fortalecer las capacidades en seguridad digital de los ciudadanos, el sector público y el sector privado, actualizar el marco de gobernanza en materia de seguridad digital, y analizar la adopción de modelos, estándares y marcos de trabajo con énfasis en nuevas tecnologías para preparar al país ante los desafíos de la Cuarta Revolución Industrial24. Además, establece un plan de acción a corto plazo para implementar en los siguientes dos años, con actuaciones concretas para lograr estos objetivos1.

Mediciones CMM de OEA & BID (2016 y 2020)

Mediciones GCI de UIT (2020 y 2024)



Fuente: Elaboración propia a partir de (OEA & BID, 2016), (OEA & BID, 2020), (OEA & BID, 2024), (ITU, 2023) y (ITU, 2024)

A partir de lo anterior, se evidencia que **Colombia presenta un progreso leve en la madurez de sus capacidades de protección, detección y respuesta ante incidentes cibernéticos.** Esta situación debe revisarse, ya que el entorno digital continúa evolucionando rápidamente con la aparición de nuevas vulnerabilidades y vectores de ataque cada vez más sofisticados.

El contexto nacional actual sugiere la necesidad de redoblar esfuerzos en ciertos ámbitos específicos para abordar los respectivos retos y desafíos para alcanzar un desarrollo integral y sostenido en todas las dimensiones de la seguridad digital.

[4] El Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM, por sus siglas en inglés, Cybersecurity Capacity Maturity Model for Nations) es un marco metódico diseñado por el Centro de Capacidad de Seguridad Cibernética Global del Departamento de Ciencias de la Computación de la Universidad de Oxford para revisar la capacidad de ciberseguridad de un país (https://gcscc.ox.ac.uk/the-cmm).

[5] El Global Cybersecurity Index (GCI) es un referente de confianza que mide el compromiso de los países con la ciberseguridad a nivel global (https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx).

III. RETOS Y DESAFÍOS

Colombia enfrenta actualmente una serie de desafíos críticos en materia de seguridad digital que ponen en riesgo la integridad de sus sistemas de información, la privacidad de sus ciudadanos y la estabilidad de sus instituciones. Estos retos se manifiestan en cuatro áreas principales: debilidad institucional y falta de coordinación, vulnerabilidad frente a amenazas cibernéticas sofisticadas, escasez de talento especializado y desactualización del marco normativo.

1 **En primer lugar, la debilidad institucional y la falta de coordinación efectiva en materia de seguridad digital** representan un obstáculo significativo para la protección del ciberespacio colombiano.

1.1 **La ausencia de una institución nacional especializada y robusta para coordinar los esfuerzos de seguridad digital** ha resultado en una fragmentación de las iniciativas y una dispersión de los recursos. Esta situación se ve agravada por la falta de un marco de coordinación efectivo entre las distintas entidades involucradas en la seguridad digital a nivel nacional, lo que dificulta la implementación de estrategias coherentes y efectivas.

1.2 **La insuficiente capacidad de respuesta ante crisis cibernéticas a gran escala** es otra manifestación de esta debilidad institucional. Colombia carece de mecanismos eficientes para el intercambio de información sobre amenazas cibernéticas entre entidades públicas y privadas, lo que limita la capacidad de anticipación y respuesta ante incidentes. Además, la falta de análisis estratégico y monitoreo continuo de las amenazas y tendencias en seguridad digital, especialmente considerando aspectos de género y diversidad, deja al país vulnerable ante nuevas formas de ataques.

1.3 **La limitada cooperación internacional en materia de seguridad digital,** especialmente frente a amenazas transfronterizas y el cibercrimen, presenta desafíos para Colombia en el escenario global. Esta situación se ve agravada por la falta de suficiente colaboración entre el sector público, privado y académico para impulsar la innovación en seguridad digital, lo que dificulta el desarrollo de soluciones locales y adaptadas al contexto nacional.

1.4 **La falta de un enfoque que considere la equidad de género y la diversidad** en todos los aspectos de la gobernanza de seguridad digital es otra debilidad significativa. Esta omisión no solo perpetúa las desigualdades existentes en el campo tecnológico, sino que también limita la capacidad del país para aprovechar plenamente el talento y las perspectivas diversas en la lucha contra las amenazas cibernéticas.

2 **En segundo lugar, Colombia enfrenta una preocupante falta de preparación frente a amenazas cibernéticas cada vez más sofisticadas.** La insuficiente capacidad para identificar, evaluar y mitigar riesgos cibernéticos de manera integral y efectiva deja al país expuesto a ataques que podrían tener consecuencias devastadoras.

2.1 **La falta de un sistema robusto de respuesta a incidentes cibernéticos,** especialmente en entidades públicas, agrava esta situación, permitiendo que los ataques se propaguen y causen daños significativos antes de ser contenidos.

2.2 **La escasez de personal capacitado en gestión de incidentes de seguridad digital,** particularmente en roles de liderazgo, es un factor crítico que limita la capacidad de respuesta del país. Esta carencia se hace especialmente evidente en la vulnerabilidad de las infraestructuras críticas cibernéticas y servicios esenciales frente a incidentes cibernéticos, poniendo en riesgo la continuidad de servicios fundamentales para la sociedad.

2.3 **La falta de coordinación efectiva entre los equipos de respuesta a incidentes cibernéticos (CSIRT)** dificulta una reacción rápida y coordinada ante amenazas complejas. Además, la insuficiente innovación y desarrollo tecnológico en el campo de la seguridad digital deja a Colombia rezagada en la carrera por desarrollar herramientas y soluciones de vanguardia para proteger sus activos digitales.

2.4 **La falta de preparación para enfrentar riesgos asociados al desarrollo de tecnologías emergentes,** como la Inteligencia Artificial (IA), representa un desafío adicional. La ausencia de directrices claras y estándares para la implementación segura de la IA en los sectores público y privado abre la puerta a vulnerabilidades que podrían ser explotadas por actores malintencionados.

2.5 **Las brechas de género y diversidad en el campo de la seguridad digital,** desde la formación hasta la participación en roles clave, limitan la capacidad del país para abordar de manera integral los desafíos de seguridad digital. La falta de consideración de los impactos diferenciados de las amenazas cibernéticas en diferentes grupos poblacionales deja a sectores vulnerables expuestos a riesgos específicos que no son adecuadamente abordados por las estrategias actuales.

3 **En tercer lugar, la escasez de talento especializado y la falta de una cultura de seguridad digital** generalizada representan un obstáculo significativo para el fortalecimiento de las defensas digitales de Colombia.

3.1 **La falta de conciencia y conocimiento sobre seguridad digital en la población general** y en diversos sectores profesionales, crea un entorno propicio para la propagación de amenazas y la explotación de vulnerabilidades.

3.2 **La escasez de profesionales especializados en seguridad digital,** particularmente en roles de liderazgo para la atención de incidentes de seguridad digital y en áreas emergentes como la IA aplicada a la seguridad, limita la capacidad del país para desarrollar e implementar soluciones avanzadas de protección de infraestructuras criticas cibernéticas y servicios esenciales frente a ciberataques. Esta situación se ve agravada por la baja representación de mujeres y grupos diversos en el campo de la seguridad digital, lo que no solo perpetúa las desigualdades existentes, sino que también priva al sector de perspectivas y talentos valiosos.

3.3 **La insuficiente integración de habilidades de seguridad digital en la educación básica y media** deja a las generaciones futuras mal preparadas para enfrentar los desafíos digitales. La falta de programas de formación y certificación en seguridad digital adaptados a las necesidades del sector público y privado dificulta el desarrollo de una fuerza laboral especializada y actualizada.

3.4 **La dificultad para retener talento especializado en seguridad digital, especialmente en el sector público,** crea una brecha de conocimiento y experiencia que debilita las defensas del país. La falta de liderazgo en TI con conocimientos avanzados en seguridad digital limita la capacidad de las organizaciones para implementar estrategias efectivas de protección.

3.5 **El insuficiente conocimiento y aplicación de normativas de protección de datos y privacidad expone a los ciudadanos y organizaciones a riesgos significativos.** La falta de preparación para abordar los desafíos de privacidad relacionados con tecnologías emergentes como IA, el Big Data, IoT y edge computing deja al país vulnerable ante nuevas formas de explotación de datos personales.

3.6 **La vulnerabilidad de las pequeñas y medianas empresas frente a amenazas cibernéticas,** debido a la falta de recursos y conocimientos en seguridad digital representa un riesgo significativo para la economía nacional. La ausencia de una cultura de seguridad digital que aborde los riesgos específicos asociados con la violencia digital basada en género y el ciberacoso, deja a grupos vulnerables expuestos a formas específicas de victimización digital.

Gobierno de Colombia

4 **Finalmente, la desactualización y falta de adecuación del marco normativo colombiano** frente a los desafíos cibernéticos actuales y emergentes representa un obstáculo significativo para la protección efectiva del ciberespacio nacional.

4.1 **La obsolescencia normativa, evidenciada por leyes como la Ley 1273 de 2009 sobre delitos informáticos,** genera riesgos para enfrentar las amenazas cibernéticas modernas. Adicionalmente, existen dificultades para ratificar integralmente la adopción y adhesión a convenios y medidas internacionales para combatir el ciberdelito.

4.2 **La falta de mecanismos de actualización periódica para revisar y actualizar la normativa de seguridad digital de manera regular** resulta en un marco legal que se queda rápidamente atrás frente al acelerado avance tecnológico. La desalineación con estándares internacionales dificulta la cooperación transfronteriza y la adopción de mejores prácticas globales en materia de seguridad digital.

4.3 **Los continuos retos en materia de protección de datos personales y los desafíos de privacidad** relacionados con tecnologías emergentes como IA y el Big Data deja a los ciudadanos vulnerables ante nuevas formas de explotación de su información personal. Se requiere regulación específica para nuevas tecnologías como IA, IoT y computación en la nube crea vacíos legales que pueden ser explotados por actores malintencionados.

4.4 **La ausencia de un enfoque inclusivo en las normativas actuales, que no consideran adecuadamente las perspectivas de género** y diversidad en su diseño e implementación, perpetúa las desigualdades existentes en el ámbito digital. Las debilidades en la persecución del cibercrimen, debido a la falta de herramientas legales suficientes para combatir eficazmente las nuevas formas de ciberdelincuencia, dejan al país vulnerable ante amenazas criminales sofisticadas.

4.5 **La falta de claridad en las responsabilidades de los ejecutivos en materia de seguridad digital** dificulta la implementación de medidas efectivas de protección a nivel organizacional. La necesidad de actualización en la protección de infraestructuras críticas cibernéticas y servicios esenciales frente a amenazas cibernéticas modernas pone en riesgo servicios esenciales para la sociedad y la economía.

En conclusión, Colombia enfrenta un panorama complejo y desafiante en materia de seguridad digital. La combinación de debilidades institucionales, vulnerabilidades técnicas, escasez de talento especializado y un marco normativo desactualizado, crea un entorno propicio para la proliferación de amenazas cibernéticas. Abordar estos desafíos requerirá un esfuerzo coordinado y sostenido que involucre a todos los sectores de la sociedad, así como una inversión significativa en recursos, educación y desarrollo tecnológico. Solo a través de un enfoque integral y proactivo, Colombia podrá fortalecer su postura de seguridad digital y proteger eficazmente sus activos digitales en un mundo cada vez más interconectado y vulnerable.

Gobierno de Colombia

IV. MARCO ESTRATÉGICO

La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 se ha diseñado para abordar de manera integral y efectiva los desafíos críticos que enfrenta el país en materia de seguridad digital. **Esta estrategia se enfoca en cuatro áreas principales que han sido identificadas como fundamentales para fortalecer la postura cibernética del país:** i) la consolidación de la gobernanza de seguridad digital para superar la debilidad institucional y la falta de coordinación; ii) la mejora de la ciber resiliencia nacional para hacer frente a la vulnerabilidad ante amenazas cibernéticas sofisticadas; iii) el desarrollo de una fuerza laboral robusta en seguridad digital para abordar la escasez de talento especializado; y iv) la adaptación y adecuación del marco normativo cibernético para actualizar el marco legal frente a los desafíos emergentes.

A través de un conjunto de acciones estratégicas y líneas de acción específicas en cada una de estas áreas, la estrategia busca transformar el panorama de la seguridad digital en Colombia, fortaleciendo las capacidades nacionales, fomentando la colaboración intersectorial e internacional, y promoviendo una cultura de seguridad digital inclusiva y equitativa. Con esta aproximación holística, Colombia se posicionará para enfrentar eficazmente las amenazas cibernéticas actuales y futuras, protegiendo los intereses nacionales y el bienestar digital de sus ciudadanos.

1. ARTICULACIÓN ESTRATÉGICA

La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027, se construye a partir de lo dispuesto en los principales instrumentos de política nacionales, junto con los planes y estrategias sectoriales e institucionales relacionadas.

Con instrumentos jurídicos:

La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 está diseñada para respetar y fortalecer el cumplimiento de los instrumentos jurídicos, tanto nacionales como internacionales, en el ámbito digital. **En su elaboración, se han alineado principios fundamentales de derechos humanos, no discriminación, combate a la violencia, y desarrollo sostenible con las prácticas de seguridad digital,** reafirmando el compromiso del país con los convenios y tratados internacionales que abordan estas áreas críticas. Al mantener un enfoque de derechos humanos y seguridad digital centrado en el ser humano, la estrategia busca proteger la privacidad, la libertad de expresión y la no discriminación, reforzando así el derecho de cada ciudadano a un entorno digital seguro e inclusivo.

La estrategia también establece un marco sólido de cooperación internacional que incluye la colaboración con organismos transcontinentales, regionales y multilaterales, así como el fortalecimiento de acuerdos multilaterales y bilaterales, tales como el Convenio de Budapest, junto con iniciativas conjuntas como la Ransomware Task Force. Estas alianzas estratégicas permiten a Colombia contar con apoyo internacional en la respuesta a incidentes de seguridad digital, intercambio de inteligencia sobre amenazas, y adopción de mejores prácticas. En el ámbito nacional, la estrategia tiene en cuenta regulaciones específicas para sectores estratégicos, alineándose con directrices sectoriales y directivas regulatorias que aseguran una implementación efectiva y una respuesta unificada frente a las amenazas cibernéticas emergentes.

Con instrumentos de política:

La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 se articula de manera integral con los principales instrumentos de política nacionales, asegurando coherencia y alineación con las directrices establecidas en los Documentos CONPES 3701 de 2011, CONPES 3854 de 2016 y CONPES 3995 de 2020. También con el Plan Nacional de Desarrollo (PND) 2022-2026 "Colombia, Potencia Mundial de la Vida" y la Estrategia Nacional Digital de Colombia (END) 2023-2026. En este marco, la estrategia no solo se fundamenta en los objetivos de crecimiento digital y transformación

del país, sino que refuerza las capacidades de seguridad digital como un eje transversal para el desarrollo sostenible y la inclusión digital.
En cuanto a las políticas y planes sectoriales, la estrategia se alinea con la Política de Gobierno Digital, la Política de Seguridad, Defensa y Convivencia Ciudadana, y el Plan Estratégico de TIC 2023-2026 del sector defensa, fortaleciendo así los sistemas de respuesta ante incidentes y promoviendo la cooperación interinstitucional en temas de seguridad digital. Asimismo, el Plan Decenal de Justicia y el Plan Estratégico de Tecnologías de la Información del Ministerio de Justicia (PETI), proveen una estructura sólida para abordar los desafíos en cibercrimen y seguridad digital en el ámbito judicial, asegurando la protección de infraestructuras críticas cibernéticas y servicios esenciales y la salvaguarda de información sensible.

Estos planes sectoriales se complementan con la Hoja de Ruta para la Adopción Ética y Sostenible de la Inteligencia Artificial, la Política Nacional de Inteligencia Artificial, y el Plan Estratégico de Seguridad de la Información, los cuales garantizan una adopción responsable de tecnologías emergentes y promueven un entorno digital ético y sostenible en el país.

Con esta articulación, la Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 no solo apoya la digitalización de servicios esenciales, sino que también **fomenta una cultura de seguridad integral, protegiendo los derechos fundamentales de los ciudadanos** y respondiendo a las amenazas crecientes en el ciberespacio de manera ética y efectiva.

2. ENFOQUES RECTORES

La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 se formula para ser implementada bajo enfoques estratégicos nacionales, que fundamentan el accionar de las actuaciones que se realicen y ayuden a guiar la toma de decisiones:

Enfoque de "Toda la Sociedad" (Whole of Society):

Promoviendo la colaboración entre todos los sectores de la sociedad, incluyendo el sector público, el sector privado, la academia, la sociedad civil y los ciudadanos. En Colombia se contará con una cultura de seguridad digital que involucre a todos los actores del ecosistema digital, fomentando la cooperación y el intercambio de información para fortalecer la resiliencia cibernética del país.

Enfoque Centrado en el Ser Humano:

Priorizando la protección de los derechos digitales, la privacidad y la seguridad de los ciudadanos en el entorno digital. En Colombia se garantizará un acceso seguro y equitativo a las tecnologías de información y las comunicaciones (TIC), promoviendo la educación y concientización en seguridad digital para todos los segmentos de la población.

Enfoque de Gestión de Riesgos cibernéticos:

Centrando los esfuerzos en identificar, evaluar, mitigar y monitorear continuamente las amenazas y las vulnerabilidades en el entorno digital nacional. En Colombia se fortalecerá la resiliencia cibernética de las infraestructuras críticas nacionales y se protegerán sus activos digitales críticos, asegurando la prestación de servicios esenciales.

Enfoque de Innovación y Desarrollo de Capacidades:

Promoviendo la inversión en investigación y desarrollo en seguridad digital, el fomento de la innovación tecnológica y la formación continua de profesionales en el campo. En Colombia se priorizarán los programas educativos especializados, el establecimiento de centros de excelencia en seguridad digital, y el apoyo a startups y proyectos de investigación en tecnologías emergentes de seguridad digital.

3. VISIÓN

En 2034, Colombia es una potencia regional en seguridad digital con un ecosistema ciberseguro y resiliente que impulsa la confianza digital, el crecimiento económico y el bienestar social, promoviendo una sociedad inclusiva, innovadora y competitiva en la era digital y garantizando la protección de las libertades, dignidad y desarrollo integral de las personas.

4. PRINCIPIOS ORIENTADORES

La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 aplica los siguientes principios orientadores:

Protección de los derechos humanos y la privacidad: Garantizar que todas las medidas de seguridad digital respeten y promuevan los derechos humanos fundamentales, incluyendo la privacidad, la libertad de expresión y la protección de datos personales.

Coordinación, colaboración y cooperación multisectorial: Fomentar la interacción entre el sector público, el sector privado, la academia y la sociedad civil, tanto a nivel nacional como internacional, para compartir información, recursos y mejores prácticas en seguridad digital.

Resiliencia: Desarrollar la capacidad de anticipar, resistir, recuperarse y adaptarse a las amenazas cibernéticas, implementando un enfoque basado en la gestión de riesgos para proteger la infraestructura crítica cibernética y los servicios esenciales.

Innovación: Promover la innovación tecnológica y la formación continua en seguridad digital, desarrollando las habilidades necesarias en el personal y fomentando la investigación y el desarrollo de soluciones de seguridad avanzadas.

Transparencia y confianza digital: Establecer mecanismos de transparencia y rendición de cuentas en la implementación de políticas de seguridad digital, fomentando la confianza en el entorno digital y promoviendo la participación ciudadana en la formulación y evaluación de estas políticas.

5. OBJETIVO GENERAL

Fortalecer y consolidar un entorno digital seguro, confiable y resiliente en Colombia que promueva el desarrollo económico, la inclusión social, la innovación tecnológica y la protección de infraestructuras críticas cibernéticas y servicios esenciales, garantizando la privacidad, integridad, disponibilidad y seguridad de la información de ciudadanos, empresas e instituciones.

6. OBJETIVOS ESPECÍFICOS

La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 establece acciones que se dedican a todos los sectores de la economía y la sociedad, desde las instituciones de la administración pública, hasta los líderes de la industria y la ciudadanía, con el fin de alcanzar el objetivo general y los objetivos específicos.

6.1. CONSOLIDAR LA GOBERNANZA DE SEGURIDAD DIGITAL

Colombia consolidará su gobernanza nacional de seguridad digital, a través de un enfoque integral y colaborativo que abarca tres pilares fundamentales. En primer lugar, se fortalecerá el liderazgo y la coordinación nacional, mediante la creación de una instancia especializada y la revisión y adecuación del Modelo de Gobernanza de la Seguridad Digital, asegurando una representación equitativa y diversa en todos los niveles. En segundo lugar, se fomentará la cooperación internacional, estableciendo mecanismos robustos para el intercambio de información y mejores prácticas, así como para la lucha coordinada contra amenazas cibernéticas transfronterizas. Finalmente, se impulsarán alianzas público-privadas estratégicas para promover la innovación y el desarrollo de soluciones avanzadas de seguridad digital, con un énfasis particular en el uso seguro y responsable de la inteligencia artificial.

Este enfoque holístico no solo fortalecerá la resiliencia cibernética del país, sino que también posicionará a Colombia como un líder regional en materia de seguridad digital, promoviendo al mismo tiempo la inclusión, la equidad de género y la diversidad en todo el ecosistema de seguridad digital.

A continuación, las líneas de acción y sus respectivas acciones estratégicas.

Línea de Acción 1.1. Fortalecimiento del liderazgo y la coordinación nacional

- Crear una entidad nacional especializada para planificar, definir, coordinar y hacer seguimiento a las actividades de seguridad digital, asegurando una representación equitativa de género y diversidad en su estructura y liderazgo.

- Revisar el Modelo de Gobernanza de la Seguridad Digital establecido en el Decreto 338 de 2022, incorporando principios de igualdad de género y enfoque diferencial en su implementación. Con base en la revisión, proponer e implementar las modificaciones necesarias para adaptar el modelo al nuevo contexto nacional e internacional de ciberseguridad.

- Diseñar e implementar mecanismos de coordinación para la gestión de crisis cibernéticas a gran escala, incluyendo la realización de ejercicios de simulación interinstitucionales para mejorar la capacidad de respuesta ante incidentes, garantizando la participación activa de mujeres y grupos subrepresentados en estos ejercicios.

- Crear y poner en funcionamiento un sistema de intercambio de información sobre amenazas cibernéticas entre entidades públicas y privadas.

- Crear e implementar un observatorio nacional de seguridad digital para identificar patrones, crear acciones de respuesta y proporcionar inteligencia estratégica en materia de seguridad digital, con un enfoque específico en el análisis de brechas de género y diversidad en el ámbito cibernético.

- Establecer herramientas vinculantes para asegurar el cumplimiento y la acción coordinada de las entidades estatales en materia de seguridad digital.

Línea de Acción 1.2. Fomento de la cooperación internacional

- Generar espacios de cooperación técnica internacional para el intercambio de información sobre seguridad informática y el desarrollo de capacidades nacionales, promoviendo la participación equitativa de mujeres y grupos subrepresentados en estos intercambios.

- Diseñar e implementar mecanismos de cooperación internacional y regional para abordar amenazas cibernéticas transfronterizas y combatir el cibercrimen de manera coordinada, con especial atención a delitos cibernéticos, que generen cualquier forma de violencia basada en género.

- Fortalecer la participación en foros y organizaciones internacionales de seguridad digital, estableciendo convenios con actores internacionales expertos para el intercambio de información y mejores prácticas, asegurando la representación equitativa de mujeres y grupos diversos en estas delegaciones.

- Desarrollar e implementar un Marco Integral para la Acción contra el Ransomware, que ofrezca un conjunto de directrices y herramientas para mejorar la capacidad de respuesta y preparación de las organizaciones frente a ataques de ransomware con apoyo de la cooperación internacional y regional.

- Continuar los esfuerzos para impulsar la implementación de las medidas de fomento de la confianza en el ciberespacio regionales y globales.

Línea de Acción 1.3. Impulso de alianzas público-privadas

- Crear y poner en marcha una plataforma nacional de colaboración entre el sector público, el sector privado, la academia y la sociedad civil para fomentar la innovación, discutir iniciativas normativas y desarrollar soluciones de seguridad digital.
- Promover alianzas público-privadas estratégicas para la investigación, desarrollo e implementación de tecnologías de seguridad avanzadas, que fortalezcan la resiliencia cibernética nacional.
- Identificar y definir temas críticos y estratégicos para el Estado colombiano sobre el uso seguro y responsable de sistemas de IA, incluyendo el análisis de sesgos de género y diversidad en los algoritmos de IA y su impacto en la seguridad digital.

6.2 MEJORAR LA CIBER RESILIENCIA NACIONAL

Colombia mejorará su ciber resiliencia nacional a través de un enfoque multifacético y proactivo que abarca cinco áreas clave de acción. **En primer lugar,** se fortalecerá la gestión de riesgos y respuesta a incidentes, mediante la implementación de un sistema nacional integral que incorpora tecnologías avanzadas como la IA, asegurando la inclusión y equidad en todos los procesos. **En segundo lugar,** se priorizará la protección de infraestructuras críticas cibernéticas y servicios esenciales, implementando estrategias de seguridad de vanguardia como la arquitectura "Zero Trust". **Tercero,** se potenciarán las capacidades de ciberdefensa, integrando

tecnologías emergentes y realizando ejercicios de simulación regulares para enfrentar amenazas avanzadas. **Cuarto,** se fomentará la innovación y el desarrollo tecnológico en seguridad digital, estableciendo centros de excelencia y apoyando iniciativas de investigación diversas e inclusivas. Finalmente, se gestionarán los riesgos asociados con la adopción de tecnologías emergentes, desarrollando directrices éticas y mecanismos de monitoreo robustos.

Este enfoque integral no solo fortalecerá la capacidad del país para prevenir, detectar y responder a amenazas cibernéticas, sino que también promoverá un ecosistema digital más seguro, innovador e inclusivo, posicionando a Colombia como un referente regional en ciber resiliencia.

A continuación, las líneas de acción y sus respectivas acciones estratégicas.

Línea de Acción 2.1. Fortalecimiento de la gestión de riesgos y respuesta a incidentes

- Desarrollar e implementar un sistema nacional integral de identificación, evaluación y mitigación de riesgos cibernéticos, que incluya el uso seguro y responsable de IA para mejorar la detección y respuesta a incidentes, incorporando análisis de impacto diferenciado por género y grupos poblacionales.

- Establecer un plan de acción robusto para optimizar la respuesta ante incidentes en entidades públicas, incluyendo un manual nacional y protocolos de comunicación y coordinación interinstitucional para la gestión eficaz de crisis cibernéticas, asegurando la participación equitativa de mujeres y grupos diversos en los equipos de respuesta.

- Evaluar el estado de madurez de las capacidades de los equipos de respuesta rápida a incidentes cibernéticos (CSIRT), a nivel nacional, con el apoyo de actores de la comunidad técnica especializada como el CSIRT Américas Networks de la OEA, soportado bajo el Modelo de Madurez de Gestión de Incidentes de Seguridad (SIM3).

- Diseñar e implementar un programa de formación, entrenamiento y acompañamiento en gestión de incidentes de seguridad digital dirigido a líderes de Tecnologías de la Información (TI) públicos y privados, teniendo en cuenta la selección y utilización de herramientas y servicios acorde a las diferentes organizaciones, promoviendo activamente la participación de mujeres y grupos subrepresentados.

- Fortalecer las capacidades tecnológicas y el catálogo de servicios de seguridad digital del Estado colombiano, implementando arquitecturas de confianza cero en los sistemas gubernamentales y desarrollando capacidades avanzadas de análisis forense digital, con enfoque en la protección de datos sensibles de poblaciones vulnerables.

- Acompañar a las entidades públicas y evaluar el cumplimiento de los lineamientos y estándares del modelo de seguridad y privacidad de la información dispuestos en el marco de la Política de Gobierno Digital.

- Realizar evaluaciones periódicas de la efectividad de los planes de respuesta a incidentes, asegurando una mejora continua en la resiliencia cibernética nacional, incluyendo métricas específicas sobre la participación y el impacto en mujeres y grupos diversos.

- Elaborar un modelo técnico de capacidades mínimas en el uso seguro y responsable de IA para el sector público que permita la efectiva identificación, gestión, tratamiento y mitigación de riesgos y amenazas digitales, estableciendo mecanismos de compra pública para implementarlo en entidades nacionales, y revisando y estableciendo mecanismos para que entidades territoriales lo implementen,

- Elaborar recomendaciones sobre capacidades mínimas en el uso seguro y responsable de IA para el sector privado, que permita la efectiva identificación, gestión, tratamiento y mitigación de riesgos y amenazas digitales, realizando un estudio de viabilidad sobre mecanismos vinculantes de seguridad digital.

Línea de Acción 2.2. Protección de infraestructuras críticas nacionales y servicios esenciales

- Diseñar e implementar una estrategia integral para salvaguardar la infraestructura crítica cibernética y servicios esenciales del país, incluyendo la identificación, clasificación y elaboración de un inventario detallado.

- Implementar medidas de seguridad avanzadas, incluyendo arquitecturas basadas en el concepto de "Zero Trust", para proteger y fortalecer las infraestructuras críticas cibernéticas y servicios esenciales contra ciberataques, asegurando que estas medidas no exacerben brechas de género o exclusión digital.

- Establecer un sistema de monitoreo continuo y evaluación de vulnerabilidades para las infraestructuras críticas cibernéticas y los servicios esenciales, promoviendo alianzas público-privadas para mejorar la seguridad de aquellas operadas por el sector privado, en cumplimiento del manual nacional y los protocolos de comunicación y coordinación interinstitucional, y fomentando la participación equitativa de mujeres y grupos diversos en estos procesos.

- Desarrollar planes de resiliencia cibernética específicos para cadenas de suministro e impulsar el concepto de "seguridad digital por defecto" en los servicios públicos.

Línea de Acción 2.3. Fortalecimiento de las capacidades de ciberdefensa

- Mejorar las capacidades de defensa cibernética de las fuerzas armadas y organismos de inteligencia, integrando tecnologías avanzadas como IA y aprendizaje automático en los sistemas de defensa.

- Crear e implementar una estrategia para la coordinación de equipos de respuesta rápida a incidentes cibernéticos (CSIRT) del sector defensa con otros equipos de respuesta, implementando sistemas de detección temprana y prevención de amenazas cibernéticas.

- Realizar ejercicios regulares de simulación de ciberataques para evaluar y mejorar las capacidades de respuesta, incluyendo el desarrollo de capacidades de defensa contra amenazas emergentes como los deepfakes y ataques basados en IA, incorporando escenarios que aborden amenazas específicas basadas en género.

Gobierno de Colombia

Línea de Acción 2.4. Fomento de la innovación y desarrollo tecnológico

- Promover la investigación y el desarrollo de nuevas tecnologías de seguridad digital, ofreciendo incentivos para startups y proyectos de investigación en el campo de la seguridad digital, con énfasis en apoyar iniciativas lideradas por mujeres y grupos subrepresentados.

- Establecer centros de excelencia en seguridad digital, en colaboración con la academia y el sector privado, fomentando la adopción de tecnologías emergentes como la IA y el blockchain para mejorar la seguridad digital, asegurando la participación equitativa de mujeres y grupos diversos en estos centros.

- Desarrollar capacidades nacionales en computación cuántica y criptografía post-cuántica, creando e implementando un programa de innovación en seguridad digital centrado en la protección de IoT y dispositivos conectados.

Línea de Acción 2.5. Gestión de riesgos en la adopción de tecnologías emergentes

- Desarrollar directrices integrales para la implementación segura de IA en los sectores público y privado, incluyendo estándares para la auditoría y evaluación de riesgos de sistemas de IA.

- Establecer pautas éticas robustas para el uso de IA en seguridad digital e implementar mecanismos de monitoreo para amenazas impulsadas por IA.

6.3 DESARROLLAR LA FUERZA LABORAL DE SEGURIDAD DIGITAL

Colombia desarrollará su fuerza laboral de seguridad digital mediante un enfoque integral y multidimensional que abarca cuatro áreas estratégicas clave. En primer lugar, se fortalecerá la cultura de seguridad digital a través de programas nacionales de educación y sensibilización, abordando las necesidades específicas de diversos grupos demográficos y sectores, con un énfasis particular en la inclusión de mujeres y grupos subrepresentados. En segundo lugar, se impulsará el desarrollo del talento en seguridad digital mediante programas de formación, certificación y retención, estableciendo cuotas de participación para grupos diversos y creando entornos laborales inclusivos. Tercero, se reforzará la protección de datos y privacidad, implementando políticas robustas y desarrollando marcos de trabajo específicos para tecnologías emergentes como la IA y el Big Data. Finalmente, se brindará apoyo específico a las pequeñas y medianas empresas para mejorar su postura de seguridad digital, con un enfoque en la transformación digital segura y la inclusión de empresas lideradas por mujeres y grupos subrepresentados.

Este enfoque holístico no solo fortalecerá las capacidades técnicas del país en seguridad digital, sino que también promoverá una fuerza laboral diversa, inclusiva y altamente capacitada, posicionando a Colombia como un referente regional en el desarrollo de talento en seguridad digital.

A continuación, las líneas de acción y sus respectivas acciones estratégicas.

Línea de Acción 3.1. Fortalecimiento de la cultura de seguridad digital

- Crear e implementar un programa nacional integral de educación y sensibilización sobre seguridad digital incluyendo módulos específicos para diferentes demografías y sectores, asegurando la inclusión de contenidos que aborden las necesidades y perspectivas de mujeres y grupos diversos.

- Incorporar habilidades de protección y ciber higiene en los planes de educación básica y media, realizando campañas de concientización sobre riesgos cibernéticos, buenas prácticas de seguridad digital y uso seguro del entorno digital, con énfasis en la prevención de violencia digital basada en género.

- Capacitar sobre el uso seguro y responsable de sistemas de IA a los directivos, jefes de oficina TI, oficiales de seguridad y equipos de TI, promoviendo activamente la participación de mujeres y grupos subrepresentados en estos roles.

- Desarrollar y poner en marcha un programa de concientización sobre los riesgos asociados con la IA y las tecnologías emergentes, promoviendo la adopción de autenticación sin contraseñas en todos los sectores, considerando las barreras específicas que enfrentan las mujeres y grupos diversos en la adopción de nuevas tecnologías.

- Estructurar y ejecutar un programa integral para prevenir riesgos y delitos en Internet, con énfasis en la salud mental y emocional de la ciudadanía, incluyendo módulos específicos sobre ciberacoso y violencia digital de género.

- Desarrollar y poner en marcha un programa único de oferta institucional sobre uso seguro y responsable de sistemas de IA dirigido a personas, entidades públicas, organizaciones y entidades privadas, asegurando la representación equitativa de mujeres y grupos diversos en el diseño e implementación del programa.

Línea de Acción 3.2. Desarrollo del talento en seguridad digital

- Establecer programas de formación y certificación en seguridad digital para profesionales del sector público y privado, incluyendo programas específicos en IA aplicada a la seguridad digital y capacitación especializada en riesgos cibernéticos, con cuotas de participación para mujeres y grupos subrepresentados.

- Crear y poner en marcha programas de becas y pasantías para estudiantes en el campo de la seguridad digital, fomentando la colaboración entre la academia y el sector privado para desarrollar programas educativos relevantes, priorizando la inclusión de mujeres y grupos diversos en estos programas.

- Implementar programas de retención de talento en seguridad digital en el sector público y desarrollar iniciativas para aumentar la diversidad en el campo, con énfasis en la inclusión de mujeres y minorías, estableciendo metas específicas de representación y creando entornos laborales inclusivos.

- Formar líderes de TI públicos y privados mediante programas de entrenamiento avanzado en seguridad digital.

Línea de Acción 3.3. Protección de datos y privacidad

- Implementar y fortalecer políticas y procedimientos para asegurar el cumplimiento de normativas de protección de datos, estableciendo mecanismos de auditoría y control para garantizar la privacidad de los datos de los ciudadanos, con especial atención a la protección de datos sensibles de mujeres y grupos vulnerables.

- Desarrollar programas de capacitación en protección de datos para funcionarios públicos y empleados del sector privado, implementando tecnologías de cifrado y anonimización de datos en sistemas gubernamentales.

- Desarrollar marcos de trabajo para la protección de la privacidad en el contexto de la IA y el Big Data, implementando medidas específicas para tecnologías emergentes como IoT y edge computing, considerando los impactos diferenciados en mujeres y grupos diversos.

Línea de Acción 3.4. Apoyo a las pequeñas y medianas empresas

- Crear directrices y estándares de seguridad digital específicos para Pequeñas y Medianas Empresas (PYMES), desarrollando programas de apoyo para la implementación de medidas de seguridad y estableciendo estándares para la transformación digital segura, con énfasis en el apoyo a empresas lideradas por mujeres y grupos subrepresentados.

- Formular incentivos fiscales y financieros para fomentar la inversión en seguridad digital en el sector de las pequeñas y medianas empresas.

6.4 ADAPTAR Y ADECUAR EL MARCO NORMATIVO CIBERNÉTICO

Colombia adaptará y adecuará su marco normativo cibernético a través de un enfoque integral y dinámico que abarca tres áreas fundamentales. En primer lugar, se establecerá un mecanismo de revisión periódica de la normatividad relacionada con la seguridad digital, asegurando su actualización constante y la participación equitativa de diversos actores en el proceso.

En segundo lugar, se actualizará y adaptará el marco sustantivo y procesal para combatir el ciberdelito, alineándolo con las obligaciones internacionales y abordando las nuevas amenazas digitales con una perspectiva inclusiva. Finalmente, se crearán reglas claras para la protección de datos y privacidad, alineando las regulaciones con estándares internacionales y desarrollando normativas específicas para tecnologías emergentes como la IA.

Este enfoque holístico no solo fortalecerá la capacidad legal del país para enfrentar los desafíos cibernéticos actuales y futuros, sino que también promoverá un entorno digital más seguro, equitativo y respetuoso de los derechos de todos los ciudadanos, posicionando a Colombia como un referente regional en materia de legislación cibernética.

A continuación, las líneas de acción y sus respectivas acciones estratégicas.

Línea de Acción 4.1. Revisar la normatividad relacionada con la seguridad digital

- Establecer un mecanismo de revisión periódica bienal para mantener actualizada la normativa en materia de seguridad digital, en coordinación con las múltiples partes interesadas, asegurando la participación equitativa de mujeres y grupos diversos en estos procesos de revisión.

- Crear una hoja de ruta interinstitucional que integre los esfuerzos normativos en seguridad digital, incluyendo medidas legislativas nacionales y de cooperación internacional para combatir el ciberdelito, incorporando perspectivas de género y diversidad en su diseño e implementación.

Línea de Acción 4.2. Actualizar y adaptar el marco sustantivo y procesal para combatir el ciberdelito

- Actualizar y fortalecer el marco legal y regulatorio nacional en materia de seguridad digital para abordar las nuevas amenazas digitales, cumplir con las obligaciones del Convenio de Budapest y robustecer la persecución del cibercrimen, considerando el impacto diferenciado de los ciberdelitos en mujeres y grupos vulnerables.

Línea de Acción 4.3. Crear reglas claras para la protección de datos y privacidad

- Alinear las regulaciones de privacidad con los estándares internacionales, atendiendo las necesidades nacionales, estableciendo requisitos claros de notificación de violaciones de datos e implementando principios de privacidad por diseño, con especial atención a la protección de datos sensibles de mujeres y grupos vulnerables.

- Desarrollar regulaciones específicas para la protección de datos en el contexto de tecnologías emergentes como la inteligencia artificial y el aprendizaje automático, incluyendo medidas para prevenir y mitigar sesgos de género y discriminación algorítmica.

- Implementar normativas para la responsabilidad ejecutiva en materia de seguridad digital, siguiendo tendencias globales de rendición de cuentas.

- Brindar acompañamiento técnico y jurídico a las entidades públicas para asegurar el cumplimiento de los lineamientos de seguridad y privacidad de la información.

- Actualizar el marco normativo de seguridad para la adopción de tecnologías cloud en el sector público, con énfasis en la nube pública gubernamental.

7. PLAN DE ACCIÓN

Colombia continuará avanzando en su desarrollo y empleará las oportunidades de optimización para reforzar su estrategia en la lucha contra los ataques informáticos, fomentando de esta manera una sociedad y economía estable y segura al definir áreas clave para la implementación de su Estrategia Nacional de Seguridad Digital de Colombia 2025-2027.

Colombia, consciente de que las amenazas informáticas son una realidad presente y no un riesgo futuro, asignará los recursos gubernamentales necesarios para garantizar el éxito de esta estrategia. Además, establecerá alianzas con todos los actores relevantes para avanzar en sus objetivos y metas. También se impulsará una cultura de seguridad digital en el sector público y fomentará la asignación de recursos para este propósito.

A continuación, se presentan las intervenciones públicas teniendo en cuenta el marco estratégico de la Estrategia Nacional de Seguridad Digital de Colombia 2025-2027.

CON EL FIN DE CONSOLIDAR LA GOBERNANZA DE SEGURIDAD DIGITAL:

N°	ACCIÓN	INDICADOR DE PRODUCTO	MÉTODO DE MEDICIÓN	CLASIFICACIÓN	PLAZO	ENTIDAD RESPONSABLE
1.1	Crear una entidad nacional especializada en seguridad digital con representación equitativa de género y diversidad	Entidad nacional de seguridad digital creada y operativa	Ley y Decreto de creación publicados y estructura organizacional establecida	Mediano plazo	18 meses	Presidencia de la República, MinTIC
1.2	Implementar el Modelo de Gobernanza de la Seguridad Digital (Decreto 338 de 2022) con enfoque de género y diferencial	Porcentaje de implementación del Modelo de Gobernanza	Informe de avance trimestral con métricas de inclusión	Mediano plazo	24 meses	MinTIC, Comité Nacional de Seguridad Digital
1.3	Diseñar e implementar mecanismos de coordinación para la gestión de crisis cibernéticas a gran escala	Número de ejercicios de simulación realizados anualmente	Informes post ejercicio y evaluaciones de desempeño	Mediano plazo	18 meses	Presidencia de la República, MinTIC.
1.4	Contar con un sistema de intercambio de información sobre amenazas cibernéticas	Sistema de intercambio de información implementado y activo	Métricas de uso del sistema y calidad de la información compartida	Corto plazo	12 meses	MinTIC
1.5	Realizar un estudio de seguridad digital con enfoque en análisis de brechas de género y diversidad	Observatorio creado y produciendo informes periódicos	Número y calidad de informes producidos, con métricas de inclusión	Mediano plazo	24 meses	MinTIC, DNP
1.6	Elaborar una guía de buenas prácticas contra el Ransomware teniendo como referencia marcos regulatorios y guías internacionales	Marco implementado y adoptado por organizaciones clave	Encuesta de adopción y eficacia del marco en organizaciones	Mediano plazo	18 meses	Presidencia de la República, MinTIC, DNP

Nº	ACCIÓN	INDICADOR DE PRODUCTO	MÉTODO DE MEDICIÓN	CLASIFICACIÓN	PLAZO	ENTIDAD RESPONSABLE
1.7	Crear una mesa nacional de colaboración entre sector público, sector privado y academia en seguridad digital a través del Comité Nacional de Seguridad Digital.	Mesa táctica con participación activa de los sectores	Número de proyectos colaborativos iniciados y completados	Largo plazo	36 meses	Presidencia, MinTIC, MinCiencias
1.8	Promover alianzas público-privadas para I+D en tecnologías de seguridad avanzadas	Número de alianzas establecidas y proyectos en ejecución	Informes de progreso de proyectos y patentes registradas	Largo plazo	48 meses	Presidencia de la República, MinCiencias, MinTIC,
1.9	Fortalecer la participación en foros internacionales de seguridad digital con representación equitativa	Participación activa en foros internacionales	Informes de participación y acuerdos alcanzados	Corto plazo	Continuo	Cancillería, MinTIC
1.10	Impulsar medidas de fomento de la confianza en el ciberespacio	Socialización permanente de las medidas de fomento de la Confianza.	Informes de socialización de medidas de fomento de la confianza	Mediano	continuo	Cancillería

CON EL FIN DE MEJORAR LA CIBER RESILIENCIA NACIONAL:

Nº	ACCIÓN	INDICADOR DE PRODUCTO	MÉTODO DE MEDICIÓN	CLASIFICACIÓN	PLAZO	ENTIDAD RESPONSABLE
2.1	Desarrollar e implementar un sistema nacional integral de gestión de riesgos cibernéticos con uso de IA	Sistema implementado y operativo.	Evaluación de efectividad del sistema y cobertura sectorial	Mediano plazo	24 meses	MinTIC, ColCERT
2.2	Establecer un plan de comunicaciones para el fomento del reporte de incidentes de seguridad digital.	Plan de acción implementado	Número de entidades que han adoptado el plan y simulacros realizados	Corto plazo	12 meses	MinTIC, ColCERT

N°	ACCIÓN	INDICADOR DE PRODUCTO	MÉTODO DE MEDICIÓN	CLASIFICACIÓN	PLAZO	ENTIDAD RESPONSABLE
2.3	Establecer un plan de acción para la creación de los CSIRT Sectoriales	Plan de acción implementado bajo modelo de madurez SIM3	Número de CSIRT creados bajo el modelo de madurez SIM3	Mediano plazo	18 meses	MinTIC, Colcert
2.4	Diseñar e implementar un programa de formación en gestión de incidentes de seguridad digital	Número de profesionales capacitados, con desglose por género y grupo poblacional	Evaluaciones post-capacitación y seguimiento de aplicación de conocimientos	Mediano plazo	18 meses	MinTIC, SENA
2.5	Fortalecer las capacidades tecnológicas y el catálogo de servicios de seguridad digital del Estado	Porcentaje de sistemas gubernamentales con arquitectura de confianza cero implementada	Auditorías de seguridad y evaluaciones de capacidad	Largo plazo	36 meses	MinTIC
2.6	Implementar una estrategia integral para proteger la infraestructura crítica cibernética	Estrategia implementada y porcentaje de infraestructuras críticas cubiertas	Evaluaciones de seguridad periódicas y simulacros de ataque	Largo plazo	36 meses	MinTIC, ColCERT
2.7	Mejorar las capacidades de defensa cibernética de las fuerzas armadas y organismos de inteligencia	Nivel de preparación cibernética de las fuerzas armadas	Evaluaciones de capacidad y ejercicios de simulación	Mediano plazo	24 meses	MinDefensa
2.8	Promover y fortalecer centros de investigación, innovación y desarrollo en seguridad digital.	Número de centros I+D+I Fortalecidos.	Publicaciones científicas y transferencia de conocimiento al sector productivo	Largo plazo	36 meses	Minciencias

CON EL FIN DE DESARROLLAR LA FUERZA LABORAL DE SEGURIDAD DIGITAL:

N°	ACCIÓN	INDICADOR DE PRODUCTO	MÉTODO DE MEDICIÓN	CLASIFICACIÓN	PLAZO	ENTIDAD RESPONSABLE
3.1	Crear e implementar un programa nacional integral de educación y sensibilización sobre seguridad digital	Número de personas capacitadas, desglosado por género y sector	Encuestas post-capacitación y evaluación de conocimientos	Mediano plazo	24 meses	MinTIC, MinEducación

Nº	ACCIÓN	INDICADOR DE PRODUCTO	MÉTODO DE MEDICIÓN	CLASIFICACIÓN	PLAZO	ENTIDAD RESPONSABLE
3.2	Incorporar habilidades de protección y ciber higiene en los planes de educación básica y media	Porcentaje de instituciones educativas que han implementado el currículo	Evaluación anual de implementación y resultados de aprendizaje	Largo plazo	36 meses	MinEducación,
3.3	Estructurar y ejecutar un plan integral para prevenir riesgos y delitos en Internet	Actividades desarrolladas para prevenir ciberdelitos	Estadísticas de cibercrimen y encuestas de victimización	Largo plazo	36 meses	MinTIC, MinInterior, Policía Nacional
3.4	Establecer programas de formación en seguridad digital para servidores públicos.	Número de servidores certificados, con cuotas de participación para grupos subrepresentados	Registro de certificaciones emitidas y seguimiento de carrera	Mediano plazo	24 meses	Todas las entidades del orden nacional rama ejecutiva
3.5	Crear programas de becas y pasantías en seguridad digital	Número de becas otorgadas y pasantías completadas, con desglose por género	Informes de progreso y tasas de empleo post-programa	Largo plazo	48 meses	MinEducación, MinTIC
3.6	Implementar acciones de retención de talento humano en seguridad digital en el sector público.	Tasa de retención de profesionales de seguridad digital en el sector público	Encuestas de satisfacción laboral y seguimiento de carrera	Mediano plazo	24 meses	Presidencia de la República, MinTIC
3.7	Crear directrices y estándares de seguridad digital específicos para PYMES	Número de PYMES que adoptan los estándares, con énfasis en empresas lideradas por mujeres	Encuestas de implementación y proceso de autodiagnóstico	Corto plazo	12 meses	MinTIC, Mincomercio , MinTIC
3.8	Fortalecer las competencias de docentes y estudiantes de educación básica y media en temas de ciberseguridad, protección de datos y/o uso responsable de tecnologías digitales.	Número de docentes y estudiantes de educación básica y media capacitados en ciberseguridad, protección de datos y uso responsable de tecnologías digitales en los Centros de Interés.	Informe que relaciona la estrategia, el número de participantes y la caracterización de estos.	Mediano plazo	24 meses	MinEducación Mintic

CON EL FIN DE ADAPTAR Y ADECUAR EL MARCO NORMATIVO CIBERNÉTICO:

Nº	ACCIÓN	INDICADOR DE PRODUCTO	MÉTODO DE MEDICIÓN	CLASIFICACIÓN	PLAZO	ENTIDAD RESPONSABLE
4.1	Crear una hoja de ruta interinstitucional para integrar esfuerzos normativos en seguridad digital	Hoja de ruta desarrollada y adoptada	Evaluación de cumplimiento de hitos y objetivos de la hoja de ruta	Mediano plazo	18 meses	Presidencia de la República, Mintic
4.2	Brindar acompañamiento técnico y jurídico a entidades públicas en seguridad y privacidad	Número de entidades acompañadas y nivel de cumplimiento alcanzado	Auditorías de seguridad y privacidad en entidades públicas	Continuo	48 meses	MinTIC, ColCERT
4.3	Generar el lineamiento para la adopción de tecnologías cloud en el sector público	Marco normativo actualizado y adoptado	Tasa de adopción de tecnologías cloud en entidades públicas	Mediano plazo	18 meses	MinTIC, ColCERT

8. GLOSARIO

01 ***CERT:*** (Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas, por su sigla en inglés. Es el equipo que dispone de la capacidad centralizada para la coordinación de gestión de incidentes de seguridad digital.

02 ***Ciberespacio:*** Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias.

03 ***Ciberseguridad:*** Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguarda de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.

04 ***Ciberdefensa:*** Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. Implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética.

05 ***CSIRT:*** (Computer Security Incident & Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permitir minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.

06 ***CSIRT sectorial:*** Son los equipos de respuesta a incidentes de cada uno de los sectores, para el adecuado desarrollo de sus actividades económicas y sociales, a partir del uso de las tecnologías de la información y las comunicaciones.

07 ***CSIRT sectorial crítico:*** Son los equipos de respuesta a incidentes sectoriales de cada uno de los sectores identificados como críticos.

08 ***Gobernanza de la seguridad digital para Colombia:*** Corresponde al conjunto de interacciones y enfoques entre las múltiples partes interesadas para identificar, enmarcar, proponer, y

reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes e información que en conjunto constituyen el entorno digital.

09 ***Incidente de seguridad digital:*** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

10 ***Infraestructura crítica cibernética:*** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.

11 ***Modelo de Gobernanza de Seguridad digital:*** Es el esquema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país, con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad digital y para la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información que, en conjunto, constituyen el entorno digital en el país.

13 ***Múltiples partes interesadas:*** Corresponde al conjunto de actores que dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales. Comprende a las autoridades, las organizaciones privadas, los operadores o propietarios de las infraestructuras críticas cibernéticas nacionales, los prestadores de servicios esenciales, la academia y la sociedad civil.

14 ***Riesgo de seguridad digital:*** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.

Gobierno de Colombia

15 ***Seguridad de la información:*** Preservación de la autenticidad, confidencialidad, integridad, y disponibilidad de la información, en cualquier medio de almacenamiento: impreso o digital, y la aplicación de procesos de resiliencia operativa.

16 ***Seguridad digital:*** Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y mediante: (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades; que demanda la voluntad social y política de las múltiples partes interesadas.

17 ***Servicio esencial:*** En el marco de la gestión de riesgos de la seguridad digital es aquel servicio necesario para el mantenimiento de las actividades sociales y económicas del país, que dependen del uso de tecnologías de la información y las comunicaciones, y un incidente en su infraestructura o servicio podría generar un daño significativo que afecte la prestación de dicho servicio y la consecuente parálisis de las actividades.

18 ***Vulnerabilidad de seguridad digital:*** *Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización.*

9. BIBLIOGRAFIA

ITU. (2023b). Global Cybersecurity Index (GCI) 4th Edition. Obtenido de https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ITU. (2024). Global Cybersecurity Index 2024 5th Edition. Obtenido de https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

OEA & BID. (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? Obtenido de https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

OEA & BID. (2020). Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Obtenido de https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Se espera que estas recomendaciones fortalezcan el trabajo realizado hasta la fecha por Presidencia de la República para la formulación de la Estrategia Nacional de Seguridad Digital de Colombia 2025-2027. Esperamos que se adelante una consulta pública con el fin de aumentar la confianza digital de múltiples actores del país y fortalecer las capacidades nacionales en materia de seguridad digital.

La Sección de Ciberseguridad de la OEA/CICTE felicita nuevamente a la República de Colombia por su trabajo y expresamos nuestra disposición a seguir colaborando tanto en la formulación de este documento estratégico como en la formulación e implementación del plan de acción.