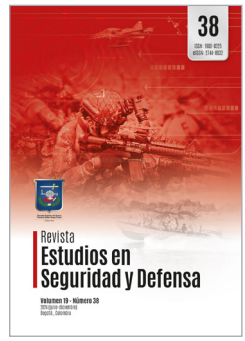
EDITORIAL ESDEG

Revista
Estudios en Seguridad y Defensa
Volumen 19, número 38, julio-diciembre 2024
Bogotá, D.C, Colombia
ISSN: 1900-8325 • eISSN: 2744-8932
Página web: https://esdegrevistas.edu.co/index.php/resd



Revisión del estado actual de la ciberseguridad en Colombia

Review of the current status of cybersecurity in Colombia

Martín Díaz Acevedo
Álvaro Cremades Guisado

CITACIÓN APA:

Díaz Acevedo, M., & Cremades Guisado, A. (2024). Revisión del estado actual de la ciberseguridad en Colombia. *Estudios en Seguridad y Defensa, 19*(38), 179-203. https://doi.org/10.25062/1900-8325.1999

Publicado en línea: **Diciembre 30 de 2024**

Enviar un artículo a la Revista

Revista **Estudios en Seguridad y Defensa**
Volumen 19, número 38, julio-diciembre 2024 (pp. 179-203)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Revisión del estado actual de la ciberseguridad en Colombia

Review of the current status of cybersecurity in Colombia

DOI: https://doi.org/10.25062/1900-8325.1999

Martín Díaz Acevedo
Universidad Antonio de Nebrija, España

Álvaro Cremades Guisado
Universidad Antonio de Nebrija, España

Resumen

Este artículo evalúa el estado actual de la ciberseguridad en Colombia. Para ello, se analiza la política pública en tres momentos clave. En primer lugar, se revisan los CONPES 3701 de 2011 y 3854 de 2016 para comprender las acciones iniciales del país en este tema. En segundo lugar, se estudian el CONPES 3995 de 2020 y la Estrategia Nacional de Ciberdefensa y Ciberseguridad, como evolución de la política pública en materia de ciberseguridad. Posteriormente, se examinan las amenazas digitales surgidas entre 2019 y 2021, en el contexto de la pandemia, y la reacción del Estado frente a ellas. Los resultados evidencian que, aunque las capacidades técnicas han mejorado, las capacidades organizacionales no han avanzado al mismo ritmo, lo que indica que la estrategia debe fortalecerse para que sea exitosa. Finalmente, se revisan las propuestas del gobierno actual en materia de ciberseguridad.

Palabras Clave: ciberseguridad; estrategia; política pública; seguridad multidimensional

Abstract

This article evaluates the current state of cybersecurity in Colombia. To do so, it analyzes public policy at three key moments. First, CONPES 3701 of 2011 and 3854 of 2016 are reviewed to understand the country's initial actions on this issue. Second, CONPES 3995 of 2020 and the National Strategy for Cyber Defense and Cybersecurity are studied as an evolution of public policy on cybersecurity. Subsequently, the digital threats that emerged between 2019 and 2021, in the context of the pandemic, and the State's reaction to them are examined. The results evidence that, although technical capabilities have improved, organizational capabilities have not advanced at the same pace, indicating that the strategy must be strengthened to be successful. Finally, the current government's proposals on cybersecurity are reviewed.

Key words: cybersecurity; multidimensional security; public policy; strategy

Artículo de investigación científica
Recibido: 22 de febrero de 2024 • **Aceptado:** 29 de julio de 2024
Contacto: Martín Díaz Acevedo mdiaza7@alumnos.nebrija.es

Introducción

Esta investigación tiene como objetivo exponer de manera clara y asequible la evolución de la estrategia de ciberseguridad en Colombia, e identificar los vacíos que pueden ser objeto de futuras discusiones académicas y decisiones gubernamentales.

La ciberseguridad no es un tema reciente ni novedoso; por el contrario, desde hace mucho tiempo se ha venido hablando de seguridad informática. Sin embargo, el tema adquirió relevancia singular desde hace catorce años, cuando ocurrió el que se considera el mayor ataque cibernético de la historia: Estonia fue objetivo de un ataque por parte de Rusia. A partir de entonces, tanto a nivel interno como a nivel internacional, los Estados empezaron a trabajar en políticas para fortalecer su ciberseguridad y evitar ataques semejantes.

El contexto internacional actual ha dado lugar a nuevas formas de conflictos, lo que ha llevado a una evolución en los conceptos de seguridad y defensa. La concepción clásica de la seguridad consideraba al Estado como el actor principal del Sistema Internacional y, en consecuencia, como el garante de su seguridad ante amenazas de carácter militar (Álvarez et al., 2018).

En ese sentido, las amenazas provendrían solamente de otros Estados. Sin embargo, la aparición del fenómeno de la globalización, entre otros detonantes, con nuevas formas de integración, exige una revisión del concepto de amenaza, entendiéndolo como una serie de situaciones que pueden afectar la calidad de vida de la población y de las entidades públicas y privadas de un Estado (Álvarez et al., p. 33).

Un ataque masivo y coordinado a algún sector como el financiero, los servicios vitales o el transporte, por mencionar solo algunos, puede colocar a una nación entera en un estado crítico de inestabilidad. Se trata de nuevas amenazas diferentes a la guerra tradicional.

Nace así una nueva función del Estado frente a la defensa de su soberanía en el espacio digital y la protección de los derechos de sus ciberciudadanos ante las amenazas emergentes en el escenario de una vida más digital y gobernada por la información (Cano, 2011).

En Colombia, de acuerdo con el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la ciberseguridad se define como el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para garantizar la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio (MinTIC, 2021).

Según el Índice Global de Ciberseguridad (IGC) de 2020, Colombia ocupa el puesto 81, con un puntaje de 63,72, y a nivel regional se posiciona en el noveno lugar. Esto indica que, aunque Colombia tiene capacidades de ciberseguridad, sigue siendo vulnerable a ataques cibernéticos.

Teniendo en cuenta el contexto anterior, vale la pena preguntarse: ¿cuál es el estado actual de la ciberseguridad en Colombia? Para responder esta pregunta, como se expresó en el acápite anterior, el texto analiza lo realizado en materia de ciberseguridad, su evolución y la respuesta ante las amenazas digitales surgidas durante la pandemia. En la última parte, se estudian las propuestas presentadas por el actual presidente de Colombia durante su campaña presidencial, las cuales están incluidas en el Plan Nacional de Desarrollo (PND) publicado en febrero de 2023. Finalmente, se presentan unas conclusiones.

En cuanto a la metodología, se emplea un método de investigación cualitativo basado en el análisis de contenido. La principal razón para esta elección es que la fuente principal de investigación son documentos oficiales de diversas entidades gubernamentales, particulares y textos académicos que han abordado este tema (fuentes primarias y secundarias). Así, se recopilan documentos organizados en tres grupos:

1. Documentos oficiales de entidades internacionales como la Unión Internacional de Telecomunicaciones y la Organización de los Estados Americanos, y de entidades nacionales como el Ministerio de Defensa, la Dirección Nacional de Inteligencia, la Policía Nacional, la Dirección Nacional de Planeación y la Presidencia de la República, entre otros.
2. Informes y reportes de organizaciones regionales e internacionales, los cuales serán claves para entender la posición de Colombia en términos de ciberseguridad y analizar las acciones del país en el ámbito internacional.
3. Publicaciones académicas, especialmente las que analizan la política de ciberseguridad colombiana y el estado del cibercrimen en Colombia.

Las bases normativas de la ciberseguridad en Colombia

Para entender la situación actual de ciberseguridad, es necesario hacer un recuento de los documentos que han fundamentado la ciberseguridad en Colombia. La Tabla 1 muestra lo que se ha hecho en la implementación de políticas y estrategias para proteger el ciberespacio de Colombia.

Tabla 1. Implementación de políticas y estrategias en ciberseguridad

Año	Documento	Descripción
2011	Documento CONPES 3701	Lineamientos de política para ciberseguridad y ciberdefensa
2012	Ley 1581	Disposiciones para la protección de datos personales
2016	Documento CONPES 3854	Política Nacional de Seguridad Digital
2018	Política de Gobierno Digital	Establece la seguridad digital como habilitador transversal de la política
2019	Plan Nacional de Desarrollo 2018-2022	Las políticas de seguridad y confianza digital como uno de los principios orientadores de la transformación digital.
	Plan TIC 2018-2022	Traza proyectos e iniciativas relacionados con seguridad digital.
	Política de Defensa y Seguridad	Acciones y estrategias para fortalecer las capacidades en ciberseguridad y protección de infraestructura crítica.
	Documento CONPES 3975	Establece dentro de sus acciones, la formulación de una política pública sobre ciberseguridad.

Fuente: Elaboración propia con base en Presidencia de la República (2020)

Como se puede apreciar, Colombia ha tenido un gran avance en la implementación de políticas para fortalecer el ciberespacio. Con el paso de los años, el país ha concentrado esfuerzos en el desarrollo de estrategias orientadas a reforzar la ciberseguridad. Desde 2011, los diferentes gobiernos han dado creciente importancia a este tema, acometiendo tareas como la elaboración de lineamientos de política de seguridad, la protección de datos personales, el diseño de políticas de seguridad digital, la integración de la seguridad digital como eje transversal, el desarrollo de políticas de confianza digital, la implementación de proyectos en seguridad digital, el fortalecimiento de capacidades y la formulación de una política pública en ciberseguridad.

CONPES 3701 de 2011

En el documento CONPES 3701 se destacan las definiciones que se otorgan a los conceptos de ciberseguridad y ciberdefensa. En este, la ciberseguridad se entiende como: "Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética". Por su parte, la ciberdefensa se define como: "Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional" (Presidencia de la República, 2011).

Lo más importante del CONPES 3701 es que establece las bases para construir la estrategia nacional de ciberseguridad. El documento propone crear una comisión intersectorial conformada por el ColCERT, el Centro Cibernético Policial y el Comando

Conjunto Cibernético (CCC), cada uno con funciones específicas que no se solapan. Mientras que el ColCERT coordina la ciberseguridad y la ciberdefensa del país, el CCC y el Centro Cibernético Policial tienen como objetivo principal garantizar la defensa del territorio nacional y la seguridad ciudadana en el ciberespacio. Para lograr estos objetivos y fortalecer sus actividades respectivas, las tres entidades colaboran estrechamente.

CONPES 3854 de 2016

El gobierno colombiano publicó en 2016 el documento CONPES 3854, titulado *Política Nacional de Seguridad Digital*. Este documento tiene como objetivo general fortalecer las capacidades para identificar, gestionar y mitigar los riesgos de seguridad digital (Presidencia de la República, 2016). Con este fin, el documento tiene en cuenta diversos aspectos.

Por un lado, se basa en marcos institucionales internacionales, como los de la Organización para la Cooperación y el Desarrollo Económico (OCDE), que en 2015 publicó el documento *Recomendaciones sobre gestión de riesgos de seguridad digital para la prosperidad económica y social*. Este texto gira en torno a la categoría de *seguridad digital*. Entre los conceptos destacados se encuentra el de *riesgo de seguridad digital*, usado "para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital" (OCDE, 2015). Este concepto sugiere que un riesgo en seguridad digital puede afectar los intereses nacionales, ya que dichos riesgos son dinámicos.

Otro concepto relevante es el de *gestión de riesgos de seguridad digital*, definida como "el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades" (OCDE, 2015). Este enfoque conlleva implementar diferentes procesos para asegurar que las medidas adoptadas efectivamente logren reducir los riesgos. Con base en este documento de la OCDE, Colombia incorporó varios conceptos en el CONPES 3854, como seguridad digital, infraestructura crítica cibernética y economía digital, entre otros. El concepto principal que el documento aborda es el de *seguridad digital*, definido así:

> La situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado 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 de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (Presidencia de la República, 2016)

El CONPES 3854 considera tanto las definiciones presentadas como el contexto actual del país, admitiendo la ausencia de una visión estratégica basada en la gestión de riesgos. Esto se debe principalmente a que el país no cuenta con una instancia de

coordinación nacional específica en seguridad digital. Si bien el ColCERT y el CCC coordinan acciones para proteger al Estado frente a ciberamenazas, la comisión intersectorial existente resulta insuficiente para desarrollar una visión estratégica sólida y con entidades especializadas en seguridad digital.

Además, la falta de un organismo que coordine toda la estrategia en seguridad digital limita el avance de Colombia en el entorno digital, ya que no hay una entidad dedicada exclusivamente a alcanzar los objetivos propuestos. El documento también señala que la política de seguridad digital se enfoca principalmente en el sector defensa, dejando de lado otros sectores que también dependen de esta seguridad. Una política que integrara a todos los sectores, tanto públicos como privados, permitiría una detección y respuesta más efectiva frente a incidentes de seguridad digital.

Por todo lo anterior, en este CONPES se decide crear, a corto plazo, el Coordinador Nacional de Seguridad Digital, cuya principal función será dirigir la implementación de la política en seguridad digital. Además, el documento contempla fortalecer las instituciones existentes. Dentro de este plan, el Ministerio de Defensa busca reforzar entidades como el ColCERT. También evalúa las capacidades existentes para determinar qué se debe mejorar y qué se debe crear desde cero.

Este es el recuento de lo que el Gobierno colombiano ha hecho desde el 2011 para estructurar su estrategia de ciberseguridad. Con esto en mente es más fácil entender el impacto que tienen los documentos que se analizarán en la construcción de una estrategia de ciberseguridad. Para continuar con una adecuada construcción del contexto colombiano, enseguida se revisan algunos hechos que esclarecen la situación del país frente a la ciberseguridad, específicamente algunos de los ataques cibernéticos que ha sufrido.

Antecedentes de la ciberseguridad en Colombia

En agosto de 2021, la Aeronáutica Civil de Colombia reportó un ciberataque dirigido a vulnerar los servicios internos de la entidad. Ante esta situación, la Aeronáutica, junto con el Ministerio de Defensa, la Fuerza Aérea Colombiana y MinTIC, decidió suspender todos los servicios internos de la entidad (*El Tiempo*, 1.º de septiembre de 2021). Las medidas adoptadas permitieron evitar daños a los servicios de la organización. Sin embargo, surgió una pregunta crucial: ¿por qué atacar a la Aeronáutica Civil?

La Aerocivil es responsable de garantizar el adecuado desarrollo de la aviación civil y de administrar el espacio aéreo. Sus sistemas contienen información sensible sobre todos los vuelos, como detalles de los pasajeros, horarios y destinos. El acceso a este tipo de información puede proporcionar una ventaja significativa a cualquier ciberterrorista, ya que les permite conocer los movimientos de sus objetivos.

Otro caso notable ocurrió en noviembre de 2021, cuando el Departamento Administrativo Nacional de Estadística (DANE) sufrió un ataque cibernético que provocó la caída de uno de sus servidores de almacenamiento de datos. En ese momento, el director del DANE explicó que:

El atacante ingresó al sistema informativo del DANE, se dedicó a bajar cada uno de los servidores, para tener una posición de administrador. Eso indica que este ataque no era solo una extracción, sino que el atacante logró borrar unos conjuntos de información. (*Semana*, 4 de marzo de 2022)

> Ante este ataque, el sistema de alertas de la entidad suspendió todos sus sistemas del mundo digital para garantizar que los atacantes no fueran exitosos. Aunque el ataque logró borrar algunos conjuntos de información, el DANE tenía *back-ups* de lo que se perdió.

En el 2022, 34 empresas fueron atacadas, lo que representa un 133% más que el 2021 (Figura 1). Algunas empresas que vale la pena destacar son Caracol TV, Viva Air y la EPS Sanitas.

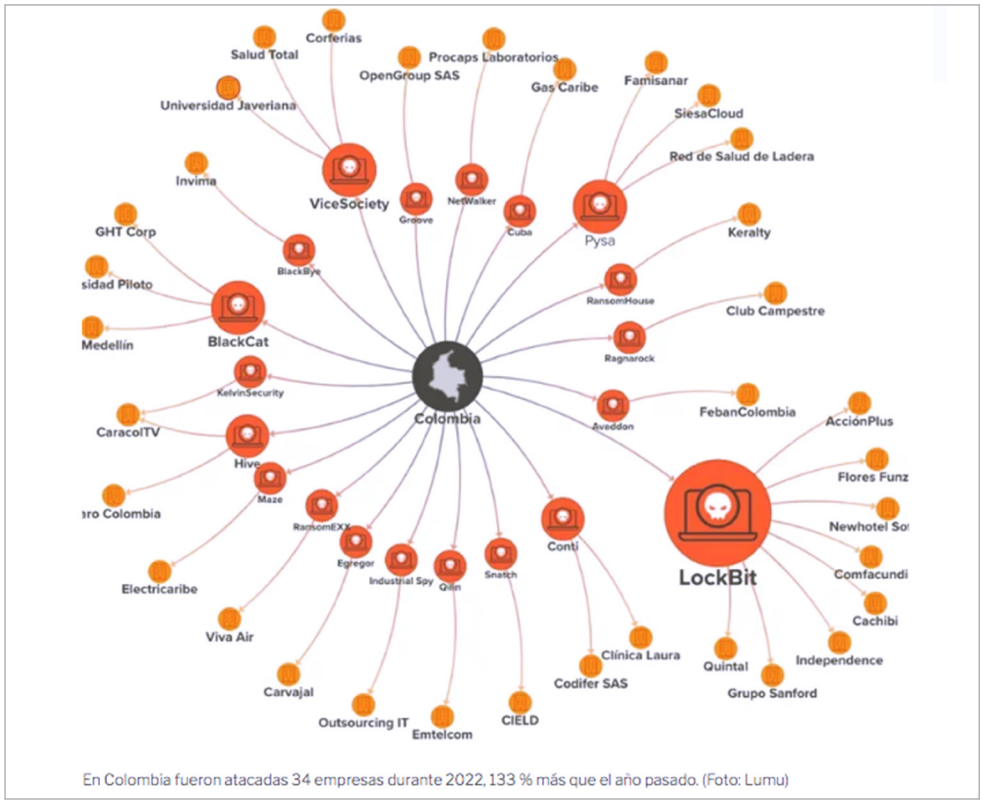


Figura 1. En Colombia fueron atacadas 34 empresas durante 2022, 133 % más que el año pasado.

Fuente: Infobae (2023).

En mayo de 2022, cibercriminales atacaron Caracol TV, uno de los principales canales de televisión en Colombia. El ataque afectó programas de diseño y graficación, así como aplicaciones operativas, que estuvieron fuera de servicio durante algunas horas. No obstante, los atacantes no lograron acceder ni comprometer información sensible del canal (Noticias Caracol, 22 de mayo de 2022).

En el segundo semestre del mismo año, la aerolínea Viva Air también fue víctima de un ciberataque que ocasionó la interrupción de algunos de sus sistemas durante varias horas. La empresa negó que la información sensible de sus clientes hubiera sido comprometida (Caparroso, 2023).

A finales de 2022, la EPS Sanitas sufrió un ataque cibernético ejecutado por el grupo Ransom House, que afectó sus servicios digitales. Según el grupo Keralty, que incluye las empresas Sanitas y Colsanitas:

> "El grupo criminal afirma tener en su poder 0,7 teras de información institucional, de los cuales han compartido 13 archivos que contienen estados financieros, balances, presupuestos, así como información personal. Hasta el momento, nuestra investigación nos ha permitido identificar que no están comprometidos datos financieros de terceros, ni historias clínicas de nuestros usuarios", detalló la compañía. (*Portafolio*, 21 de diciembre de 2022)

Estos son solo algunos ejemplos de los ciberataques que ha sufrido Colombia en los últimos años. Como se puede observar, estos ataques no discriminan y pueden impactar tanto a entidades públicas como a empresas privadas. Sin duda, se trata de un problema grave que pone en evidencia la vulnerabilidad de las instituciones colombianas y de todas aquellas que carecen de recursos suficientes para prevenir ciberataques o que no cuentan con personal capacitado para implementar sistemas de protección adecuados.

Muchas entidades públicas ni siquiera son conscientes de su vulnerabilidad informática, lo cual constituye una alarma sobre lo que podría suceder en el país si se enfrenta a ciberataques exitosos. Esto demuestra, una vez más, que Colombia tiene mucho por hacer para mejorar sus capacidades y garantizar que el Estado, las empresas y los ciudadanos no se conviertan en víctimas de ciberataques.

El fortalecimiento de la ciberseguridad

El 2020 trajo nuevos desafíos a los que el país debió adaptarse y perfeccionar su estrategia con un nuevo documento CONPES y con la Estrategia Nacional de Ciberdefensa y Ciberseguridad 2020-2030, publicada por la Escuela Superior de Guerra. Antes de profundizar en este tema, es necesario analizar un documento publicado por la Unión Internacional de Telecomunicaciones (UIT) en el 2018 titulado *Guía para la elaboración de una estrategia nacional de ciberseguridad* (UIT et al., 2018). Este documento se ha convertido en un referente para los países al momento de desarrollar sus estrategias en ciberseguridad.

El texto, creado por la UIT con la colaboración de organizaciones como el Banco Mundial, Deloitte y Microsoft, tiene como finalidad "orientar a los dirigentes y poderes públicos nacionales en la elaboración de una estrategia nacional de ciberseguridad y en la reflexión estratégica sobre la ciberseguridad, la preparación para el ciberespacio y la resiliencia" (UIT et al., 2018). Con el apoyo de esta guía, los Estados pueden desarrollar y fortalecer sus estrategias en ciberseguridad de manera más eficiente.

El documento cuenta con varias secciones que abarcan desde la planeación de la estrategia hasta su evaluación, con puntos clave que vale la pena destacar. El primero es su definición de ciberseguridad, entendida como:

> El conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, acciones, formaciones, prácticas idóneas, garantías y tecnologías que pueden utilizarse para proteger la disponibilidad, integridad y confidencialidad de los activos de la infraestructura conectada pertenecientes al gobierno, a las organizaciones privadas y a los ciudadanos; estos activos incluyen los dispositivos informáticos conectados, el personal, la infraestructura, las aplicaciones, los servicios, los sistemas de telecomunicaciones y los datos en el mundo cibernético. (UIT et al., 2018)

Esta definición es, hasta este momento, la más completa que ha creado esta organización, ya que incluye diversas herramientas y acciones necesarias para proteger a entidades estatales, empresas privadas y ciudadanos. Se comprende que todos forman parte del mundo cibernético y, por ende, deben ser resguardados de estas nuevas amenazas.

En segundo lugar, se destaca el apartado de supervisión y evaluación de la estrategia. Además de contar con bases sólidas en el plan, resulta esencial realizar evaluaciones regulares para identificar áreas de mejora y consolidar los aspectos que funcionan adecuadamente. Para ello, el rendimiento debe ser medible, lo que requiere establecer métricas o indicadores específicos para evaluar los objetivos a corto, mediano y largo plazo. La guía enfatiza que estos indicadores deben ser específicos, cuantificables, alcanzables, con asignación de responsabilidades y plazos definidos (UIT et al., 2018).

Finalmente, el monitoreo constante del entorno debe ser transversal en toda estrategia de ciberseguridad. La identificación continua de riesgos y amenazas en los ámbitos internacional, regional y local resulta fundamental para garantizar que la estrategia se adapte y pueda cumplir con sus objetivos sin contratiempos.

Tras analizar los puntos más importantes de esta guía, a continuación se estudian los documentos más recientes en materia de ciberseguridad publicados por el Estado: el CONPES 3995 y la Estrategia Nacional de Ciberdefensa y Ciberseguridad 2020-2030.

CONPES 3995 del 2020 y la Estrategia Nacional de Ciberdefensa y Ciberseguridad

El CONPES **3995,** expedido en 2020 bajo el mandato del presidente Iván Duque, a diferencia de los anteriores, cuenta con una nueva definición de *ciberseguridad*:

> La capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin. (Presidencia de la República, 2020)

Es posible observar que esta definición presenta puntos en común con la propuesta por la UIT. En ambas se identifica claramente a quiénes se debe proteger y qué mecanismos se implementan para garantizar esa protección. Al analizar esta definición, se evidencia que el documento guía fue revisado y efectivamente utilizado en la elaboración del nuevo CONPES. Con esta definición, junto a otras que aparecen en el glosario, se construye una base más sólida para el resto del documento, lo que lo diferencia considerablemente de otros CONPES.

La claridad en los conceptos resulta de gran importancia para que todos trabajen con una misma definición y, a partir de ella, se pueda avanzar de manera conjunta y coordinada. Además, es necesario que estas definiciones sean lo más claras posible. Este CONPES cumple con dichos requisitos y evidencia el avance de Colombia en estos temas.

En el CONPES 3854 de 2016 se había planteado la necesidad de crear un coordinador nacional de seguridad digital, lo que llevó a la creación de la Consejería de Asuntos Económicos y Transformación Digital de la Presidencia de la República. Sin embargo, entre las funciones de esta Consejería no se estableció que operara exclusivamente como una unidad transversal y vinculante de política de ciberseguridad en sus decisiones frente a las demás entidades del Gobierno nacional. La ausencia de esta función limita su papel como coordinador nacional para la toma de acciones (Presidencia de la República, 2020).

La claridad de conceptos es de gran importancia. Sirve para que todos tengan la misma definición y con base en eso se puede empezar el trabajo conjunto en una misma dirección. Además de tener los conceptos bien definidos, es necesario que esas definiciones tengan la mayor claridad posible. Este Conpes ha cumplido con esos requisitos y se nota el avance que Colombia ha tenido en estos temas.

En el Conpes 3854 del 2016 se había establecido que era necesario crear un coordinador nacional de seguridad digital y para eso se creó la Consejería de Asuntos

Económicos y Transformación Digital de la Presidencia de la República. Sin embargo, entre las funciones de esta Consejería no se establece que éste opere de manera exclusiva como una unidad de política de ciberseguridad de manera transversal y vinculante en sus decisiones frente a las demás entidades del Gobierno nacional. La ausencia de esa función limita el rol como coordinador nacional para tomar acciones. (Presidencia de la República, 2020).

Esta debilidad fue superada en mayo de 2022 con la publicación del Decreto 722 de 2022, mediante el cual se oficializó la designación del Coordinador Nacional de Seguridad Digital. En su primer artículo declara: "Desígnese al Consejero Presidencial para la Transformación Digital y Gestión y Cumplimiento, de la Presidencia de la República como Coordinador Nacional de Seguridad Digital" (Decreto 722, 2022). Esta designación oficial representa un avance positivo para el país, no solo porque permite que el trabajo de coordinación se lleve a cabo con mayor efectividad, sino también porque podría contribuir a que Colombia mejore su puntuación en la próxima evaluación del Índice Global de Ciberseguridad (IGC) en el ámbito de instituciones de ciberseguridad.

Ante las debilidades y el contexto del país en 2020, el objetivo del CONPES 3995 es desarrollar la confianza digital mediante el fortalecimiento de la seguridad digital. Este fortalecimiento abarca el desarrollo de capacidades, la actualización del marco de gobernanza y la adopción de modelos con énfasis en nuevas tecnologías (Presidencia de la República, 2020). Para alcanzar este objetivo, el plan de acción se estructura en tres ejes principales: fortalecimiento de capacidades, actualización en el marco de gobernanza y análisis de la adopción de modelos en seguridad digital.

En cuanto al fortalecimiento de capacidades, lo primero que se planea es reunir a instituciones como el Coordinador Nacional de Seguridad Digital, el MinTIC, el Ministerio de Educación, el Ministerio de Defensa, entre otras, para coordinar y diseñar una estrategia de formación de capacidades en seguridad digital para los sectores público y privado, enfocada en la ciudadanía. Esto permite que el trabajo sea coordinado y que no se realicen esfuerzos innecesarios. Cada entidad puede concentrarse en sus tareas específicas, las cuales, en su mayoría, incluyen la elaboración y ejecución de programas para fortalecer el conocimiento y las capacidades de los ciudadanos en ambos sectores.

En esta etapa, es importante destacar que la Dirección Nacional de Inteligencia se encargará de diseñar un proyecto de implementación del CSIRT con el objetivo de contribuir a la protección de la seguridad digital. Este proyecto también busca una armonización entre el CSIRT y las demás instancias nacionales que abordan la seguridad digital (Presidencia de la República, 2020). Esto evidencia que, con el tiempo, no solo se han creado nuevas entidades nacionales para abordar aspectos específicos de la ciberseguridad, sino que se busca también una mejor coordinación entre estas entidades.

En la segunda sección, relativa a la actualización del marco de gobernanza, en primer lugar, se plantea que el Departamento Administrativo de la Presidencia de la República (DAPRE), a través del Coordinador Nacional, propondrá la estructura oficial de la gobernanza de seguridad digital del país. Esta propuesta debe ser clara y definir los roles y responsabilidades de cada entidad. En 2015 se publicó el Decreto 1078, que contiene el reglamento del sector de tecnologías de la información y las comunicaciones, y define toda la normativa del sector. Sin embargo, era necesario adicionar un título que detallara aspectos específicos como funciones, definiciones y la organización de las entidades que abordan la seguridad digital.

En marzo de 2022 se publicó el Decreto 338, que adiciona al Decreto 1078 el título 21, denominado "Lineamientos Generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital". Este título incluye definiciones que no estaban presentes en el documento original, como CERT, CSIRT, ciberespacio y ciberdefensa, entre otros. Además, establece el modelo de gobernanza de seguridad digital, cuyo objetivo es:

> Facilitar la participación, articulación e interacción de las múltiples partes interesadas para fortalecer las capacidades en la gestión de riesgos de seguridad digital y de esta manera lograr un abordaje integral que promueva el adecuado aprovechamiento de las oportunidades que ofrece el entorno digital. (Decreto 338, 2022)

También se encuentra la composición del Comité Nacional de Seguridad Digital, que consta de 20 cargos ocupados por representantes de la Coordinación Nacional de Seguridad Digital, diversos ministerios, la Policía Nacional y las Fuerzas Armadas. Por último, este decreto establece la identificación de infraestructuras críticas. Un punto destacado es que el MinTIC deberá realizar cada dos años un inventario de las infraestructuras críticas nacionales (Decreto 338, 2022).

Estos puntos reflejan los aspectos más relevantes de este decreto. Su publicación refuerza la gobernanza en seguridad digital, ya que define objetivos claros, proporciona una estructura organizativa precisa para las entidades involucradas e identifica las infraestructuras críticas del país. Representa un avance significativo en la ciberseguridad de Colombia.

La última sección de este plan de acción aborda el análisis de la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital. Esta sección tiene como objetivo preparar al país para enfrentar los desafíos que plantea la cuarta revolución industrial.

Vale la pena destacar que una de las intenciones del MinTIC es emitir lineamientos y guías para facilitar a las entidades públicas la adopción y actualización de nuevas

tecnologías, con el fin de reducir sus vulnerabilidades. Para ello, se trabaja con base en el PND 2018-2022, específicamente en el artículo 147, que trata sobre la transformación digital pública. A este artículo, el Gobierno añadió una circular presidencial y dos directivas presidenciales. En la Circular 1 del 17 de febrero del 2022, el Gobierno nacional expresa que:

> Ha priorizado el uso de servicios de nube en las entidades de la Rama Ejecutiva del Orden Nacional, lo cual resulta relevante no solo para optimizar los recursos públicos en proyectos de tecnologías de la información, sino para aprovechar sus beneficios, entre ellos, los de obtener mayor escalabilidad, seguridad de la infraestructura, protección de los datos, actualización de las plataformas, redundancia, flexibilidad, oportunidad y disponibilidad. (Presidencia de la República, 2022a)

Esto evidencia que Colombia está avanzando en el ámbito del ciberespacio. El hecho de que el gobierno busque la actualización de las entidades públicas en el entorno digital es un paso significativo, principalmente porque fortalece la protección de la infraestructura y, por ende, la seguridad de la ciudadanía.

En cuanto a las directivas presidenciales, la 03 del 15 de marzo de 2021 aborda los lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos. El apartado relacionado con los servicios en la nube tiene como objetivo cumplir con las directrices en materia de computación publicadas por el MinTIC. Para ello, se requiere que estos servicios sean optimizados y evaluados, además de cumplir con las normas de la política de gobierno digital y otros parámetros establecidos.

Por último, para complementar la estrategia de seguridad digital del PND 2018-2022, la Directiva 02 del 24 de febrero de 2022 garantiza la implementación de estrategias en seguridad digital mediante evaluaciones constantes. En primer lugar, en esta se reconoce que el sector público no ha estado exento del incremento de incidentes en el ámbito cibernético. Para enfrentar esta situación, establece que los sistemas de información, servicios, bases de datos e infraestructuras deben mantenerse actualizados, facilitando así la identificación de los activos críticos en las entidades (Presidencia de la República, 2022b). Además de la actualización de los sistemas, la directiva señala la necesidad de verificar los proveedores de servicios en la nube, crear equipos de seguridad digital que garanticen la correcta aplicación de políticas y estrategias, realizar evaluaciones del nivel de madurez en seguridad digital, entre otras medidas.

A continuación se analiza otro documento clave para la ciberseguridad en Colombia: la Estrategia de Ciberseguridad y Ciberdefensa 2020-2030. Este documento, elaborado por el Ministerio de Defensa, el Comando General de las Fuerzas Militares y la Escuela Superior de Guerra, detalla cómo se desarrollarán la ciberdefensa y la ciberseguridad en el país hasta el año 2030.

Estrategia Nacional de Ciberdefensa y Ciberseguridad 2020-2030

En septiembre de 2020, el gobierno publicó la primera edición de la Estrategia Nacional de Ciberdefensa y Ciberseguridad (ECDCS) para los siguientes diez años. Esta estrategia se destaca por su transversalidad, ya que busca integrar las políticas, planes e instituciones creadas hasta la fecha, con el objetivo de optimizar los resultados. Se fundamenta en cinco principio clave, esenciales para garantizar una armonización entre la estrategia y las acciones previamente desarrolladas en materia de ciberseguridad y ciberdefensa (Figura 2).

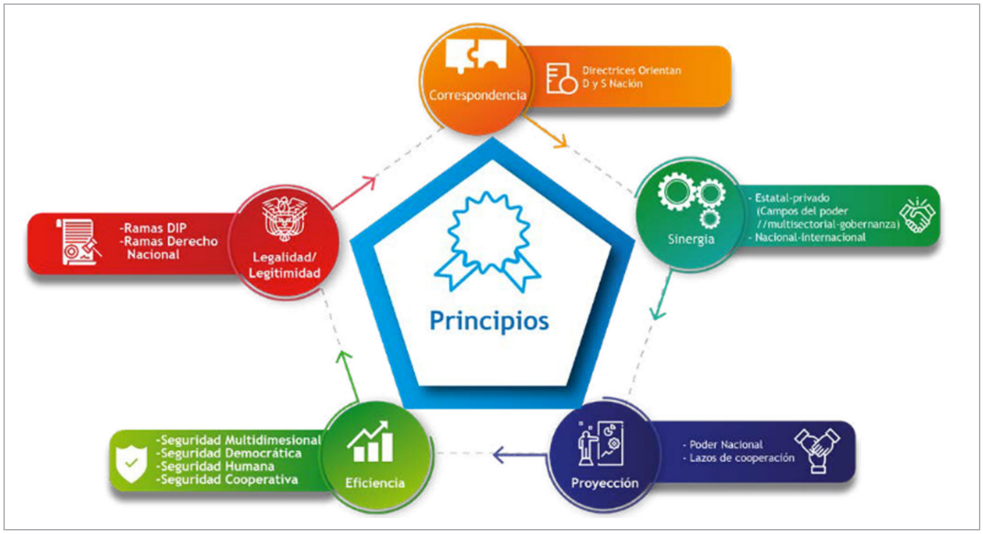


Figura 2. Principios de la Estrategia Nacional de Ciberdefensa y Ciberseguridad.
Fuente: Ministerio de Defensa Nacional et al. (2020)

En primer lugar, está la Correspondencia. Esto se refiere a que la ECDCS debe concordar con todas las directrices que se encuentran en los diferentes documentos del Gobierno relacionados con el tema. También está el principio de la Sinergia, para lograr un mayor involucramiento entre el sector público y privado; un trabajo multisectorial fortalecerá la gobernanza y traerá mejores resultados. Después está el principio de Proyección: al ser una estrategia transversal, tiene impacto en todos los sectores (político, económico, social y militar), por lo cual se busca una mejor prevención y respuesta a las amenazas. El cuarto principio es la Eficiencia: la ECDCS es multidimensional, es decir, hace uso de todos los tipos de seguridad para responder a las amenazas de la manera más completa posible. Por último, está la Legalidad/Legitimidad. Este principio busca adaptar las diferentes ramas del derecho para que siempre se esté actuando conforme a la ley (Ministerio de Defensa Nacional et al., 2020).

Además de estos principios, la ECDCS tiene un objetivo general:

> Garantizar y proteger la utilización segura del ciberespacio por parte de los ciudadanos y de la Nación, mediante el despliegue de las capacidades de defensa y seguridad del Estado, que permita mitigar los riesgos y amenazas mediante un trabajo coordinado y de cooperación, que contribuya al crecimiento económico y social del país. (Ministerio de Defensa Nacional et al., 2020)

Para buscar el éxito en la ECDCS, se consideran los principios, los objetivos y las indicaciones de la UIT sobre Colombia, además de su forma de evaluar las categorías pertinentes, con el fin de alinearse con este documento y fomentar una mejor coordinación entre las entidades públicas y privadas. Con base en ello, su propósito es:

> Diseñar una acertada política de Estado, con la visión de establecer el derrotero del país en el mediano y largo plazo, con el fin de orientar los esfuerzos e incrementar la protección de nuestros objetivos estratégicos, así como, la respuesta ante cualquier riesgo cibernético al interior de la Nación; además, en forma paralela, deberá trazarse como objetivo el desarrollo de la industria digital nacional y de gobernanza del internet, con un límite no superior al año 2024. (Ministerio de Defensa Nacional et al., 2020)

Este propósito reconoce que existen diversas amenazas cibernéticas capaces de afectar las infraestructuras nacionales, por lo cual resulta esencial fortalecer la industria digital y todo lo relacionado con el ciberespacio. En consecuencia, el documento enfatiza la importancia de que la legislación relacionada con el ciberespacio —incluidas las leyes, los documentos CONPES y otros planes nacionales— sea coherente, para facilitar el trabajo conjunto de todas las instituciones del país.

Un aspecto fundamental del documento es que, además de realizar un monitoreo constante de las amenazas cibernéticas a las que está expuesto el país, identifica los centros de poder del Estado y evalúa su criticidad. Para ello, evalúa tres elementos: el nivel de afectación, el grado de exposición y la capacidad de sobreponerse a un posible ciberataque. La ECDCS recomienda hacer un proceso a nivel nacional, en forma de autoevaluación, para generar mayor conciencia sobre las amenazas existentes y las medidas necesarias para contrarrestarlas.

Dicha evaluación no resulta difícil en la actualidad. En Colombia existen varias instituciones dedicadas a la ciberseguridad, como el ColCERT y el CSIRT, que pueden apoyar una evaluación exhaustiva de los centros de poder del país. Aunque ya se identifican las principales amenazas cibernéticas y se tienen nociones sobre las capacidades institucionales nacionales, resulta crucial realizar una evaluación más integral de los centros de poder. Considerando que en la segunda mitad de 2022 asumió un nuevo gobierno en Colombia, sería especialmente útil llevar a cabo esta nueva evaluación para establecer el estado actual de la ciberseguridad y estar mejor preparados para el futuro.

Amenazas cibernéticas surgidas en la pandemia

Si bien la pandemia trajo ciertos beneficios, como el incremento del comercio electrónico, también facilitó un aumento en los ataques de cibercriminales. Durante el período 2019-2021, las formas más comunes de ciberdelitos en Colombia fueron el hurto por medios informáticos, la violación de datos personales y el acceso abusivo a sistemas informáticos. Según el informe "Tendencias del Cibercrimen 2021-2022", para noviembre de 2021 se registraron 46 527 denuncias (TicTac, 2021). El informe concluye lo siguiente:

> Sin duda el ciberdelito se ha convertido en la tipología criminal de mayor crecimiento en Colombia durante los últimos tres años; impulsado por aceleradores como la pandemia y el consecuente incremento del comercio electrónico cuyo crecimiento alcanzó el 59,4% en las transacciones durante el periodo de cuarentena obligatoria y del 35% durante el 2021 con ventas estimadas en 37 billones de pesos al finalizar el año según cifras de la Cámara de Comercio electrónico de Colombia CCCE.

Con el paso de los años, las víctimas de los cibercriminales han aumentado, y hoy en día incluso las instituciones de los gobiernos y las empresas privadas se ven afectadas igualmente por esos ciberataques.

Propuestas del gobierno actual (2022-2026) en ciberseguridad

El actual presidente de Colombia inició su gobierno el 7 de agosto de 2022 e incluyó en su programa de gobierno el tema de la ciberseguridad. En este apartado se revisarán, de manera general, tanto el Plan de Gobierno como el PND publicado en febrero de 2023, en aras de examinar las propuestas presentadas, la forma en que pretenden alcanzar sus objetivos y lo efectivamente logrado hasta la fecha en relación con lo planteado en ambos planes.

Para el actual gobierno, el principal enfoque de la ciberseguridad es la ciudadanía, razón por la cual busca promover una cultura de uso seguro de la tecnología en el país. En este contexto, no resulta sorprendente que propugne por cambios en las fuerzas de seguridad, avanzando hacia lo que denomina la "desmilitarización de la vida social" y afirmando la prevalencia de las autoridades civiles sobre las militares.

Es posible afirmar, entonces, que el actual gobierno se aleja del concepto clásico de defensa militar del Estado colombiano, en el que se enfatizaba la importancia de la intervención casi exclusiva de las Fuerzas Militares para la defensa estatal y de la sociedad a la vez. De acuerdo con la Ley 102 de 1994 de Colombia, estas fuerzas se definen como "las organizaciones armadas, instruidas y disciplinadas conforme a la técnica militar, y constitucionalmente destinadas a la defensa de la soberanía nacional y al mantenimiento del orden legal".

Es de recordar que la concepción tradicional de la seguridad nacional equipara la seguridad del Estado con la de la sociedad. Su objetivo es identificar las posibles amenazas al Estado provenientes del exterior, a través de hipótesis de guerra; es decir, se ubican los potenciales enemigos externos y se les anticipa un trato militar. En este contexto, la concepción tradicional de la seguridad confiere al Estado el papel de agente que proporciona seguridad a la colectividad, la nación o la sociedad (Tenorio, 2009).

Según esto, se puede deducir que este enfoque se centra en la seguridad militar, un concepto que aún persiste en la mentalidad colombiana, a pesar de la evolución global del término. Hace décadas, este concepto se ha quedado corto, pues en la actualidad se deben incluir nuevos aspectos en función de las circunstancias específicas de cada Estado. Entre estos se encuentran la defensa del medio ambiente, el progreso y la prosperidad del ser humano, la creación de un ambiente apropiado para vivir en paz, la protección del sistema económico, la ciberseguridad, la ciberdefensa, entre otros.

En concordancia con la estrategia del presidente sobre la seguridad del Estado, un artículo de la revista *Semana* destaca: "Una de las prioridades del presidente Gustavo Petro al llegar a la Casa de Nariño fue asegurar el sistema de comunicaciones para evitar fuga de información y garantizar la seguridad del Estado" (*Semana*, 6 de septiembre 2022).

Diez días después de la posesión del presidente, se gestionó la compra de 50 licencias únicas en el país para evitar interceptaciones o fugas de información a través de llamadas telefónicas o mensajes de texto. Estas licencias fueron instaladas en los teléfonos móviles de las personas más cercanas al mandatario. Las licencias de encriptación de teléfonos móviles cuentan con especificaciones claras, entre las que destaca la seguridad con grado militar. En la justificación del contrato se hace referencia a las falencias en materia de seguridad en las comunicaciones del Palacio de Nariño y el equipo de confianza del presidente.

La entidad encargada de realizar la compra, junto con el respectivo estudio preliminar, fue el DAPRE. Desde esta dependencia se explica que, aunque muchas organizaciones protegen sus datos e información mediante *firewalls*, aplicaciones antivirus y correo electrónico cifrado, aún persisten vulnerabilidades en los dispositivos inteligentes, que representan uno de los vectores de amenaza más significativos dentro de la infraestructura de las organizaciones. Retomando el tema de la ciberseguridad centrada en la ciudadanía, como se expresa en el programa de gobierno, el documento indica:

> La pandemia nos mostró el potencial de las TIC, en los momentos más difíciles de aislamiento y restricciones, permitió a muchas personas continuar estudiando y trabajando, también facilitó que pudiéramos tener contacto permanente con seres queridos. Sin embargo, muchas otras personas no tuvieron posibilidades de acceder las tecnologías digitales, lo que les impidió trabajar, estudiar, informarse, tener contacto con sus seres queridos y

> organizarse colectivamente para responder al contexto. Como resultado de esta exclusión digital millones de colombianos y colombianas vieron que su derecho a participar en la sociedad se veía restringido, y por consiguiente las brechas económicas y sociales de nuestro país se hicieron más profundas. (Bolívar & Gómez, 2019)

Como se puede apreciar en este apartado, el principal propósito en temas de telecomunicaciones es aumentar la conectividad. El objetivo es que el 100 % de la población colombiana tenga acceso a internet, sin importar su ubicación geográfica o estrato social. Para alcanzar esta meta, no solo serán necesarios considerables recursos, sino también un enfoque prioritario en una seguridad digital robusta. A medida que crezca el número de personas en el ciberespacio, será indispensable fortalecer las capacidades de seguridad digital.

La sección de ciberseguridad del plan de gobierno actual tiene como objetivo: "Promover un entorno digital seguro para que las y los ciudadanos y empresas puedan obtener los beneficios de las tecnologías de la información y las telecomunicaciones" (Bolívar & Gómez, 2019). Para lograr este propósito, el programa plantea cuatro propuestas: la promoción de una cultura digital, el fortalecimiento de estrategias de ciberseguridad, la creación de cargos como *Chief Security Officer* y la cofinanciación de equipos de respuesta ante incidentes cibernéticos.

Dado que este documento tiene un carácter más informativo que analítico, no incluye un análisis detallado de cómo se planea alcanzar este objetivo. No obstante, y con el fin de fomentar la discusión, considerando que el gobierno actual está en curso, se exponen a continuación algunas observaciones y propuestas que podrían contribuir al desarrollo de la estrategia de ciberseguridad.

Es el momento para que Colombia comience a construir una comunidad ampliada de inteligencia. Estos diez años de desarrollo de la estrategia han dado lugar a instituciones con buenas capacidades para afrontar amenazas cibernéticas. Si bien aún hay aspectos por mejorar, la ciberseguridad no debería depender exclusivamente del Gobierno, ni las únicas entidades que traten este tema deberían ser la Policía Nacional o la Dirección Nacional de Inteligencia.

Las empresas privadas, las universidades y los ciudadanos cuentan con capacidades para contribuir a la ciberseguridad del país. Por ejemplo, en colaboración con entidades estatales que gestionan temas económicos, como el Ministerio de Hacienda, el Ministerio de Industria y Comercio y el Banco de la República, podría crearse y ponerse en marcha una entidad que aborde exclusivamente cuestiones de inteligencia económica.

En la actualidad, el único centro educativo que enseña sobre inteligencia y ciberinteligencia es la Escuela Superior de Guerra. Aquí radica la primera recomendación: es necesario cambiar la percepción de que estos temas son exclusivamente militares.

Por ello, se debería ampliar la oferta académica a otras universidades y fomentar que los grupos de investigación desarrollen proyectos que profundicen en los conocimientos relacionados con estos asuntos.

Al estar la campaña del gobierno actual enfocada en la ciudadanía, resulta previsible que su primera propuesta para alcanzar un entorno digital seguro sea expandir la cultura digital para que más personas aprendan a utilizar dispositivos y aprovechar los beneficios que ofrece internet. Esta propuesta debería fortalecerse integrando una cultura de ciberseguridad, en la que se enseñen temas básicos a empleados de oficinas. De este modo, podrían identificar errores que facilitan a ciberdelincuentes atacar tanto a las empresas donde trabajan como a ellos mismos en caso de ser víctimas de un ciberataque.

Asimismo, como se mencionó, es fundamental extender el conocimiento sobre inteligencia y ciberinteligencia a todas las universidades, no limitándose únicamente a instituciones de carácter militar. Esto permitiría expandir la cultura de inteligencia e involucrar más a la academia. Una mayor participación académica fortalecería la investigación en estos temas cruciales.

El segundo punto del programa de gobierno para alcanzar un entorno digital seguro es el fortalecimiento de "las estrategias de ciberseguridad de todas las entidades del Gobierno Nacional, en especial de aquellas que prestan servicios transaccionales a ciudadanos y empresas, con el objetivo de promover confianza en estos para relacionarse digitalmente con el Estado" (Bolívar & Gómez, 2019). En los últimos años, varias instituciones colombianas han sido blanco de ciberataques. Más allá de los daños internos que puedan ocasionar, el mayor impacto es que estos ataques generan desconfianza entre los ciudadanos, quienes perciben debilidades en las instituciones del Estado.

El plan de gobierno en telecomunicaciones es ambicioso y cuenta con propuestas que, si se desarrollan adecuadamente, podrían cumplir el objetivo de garantizar conexión para toda la población y proteger su seguridad en el ciberespacio.

Plan Nacional de Desarrollo 2022-2026

En febrero de 2023 se publicó el PND 2022-2026, titulado *Colombia, Potencia Mundial de la Vida*, que refleja los objetivos del presidente y las estrategias para alcanzarlos. Este plan se estructura en cinco grandes pilares:

1. Ordenamiento del territorio alrededor del agua y justicia ambiental
2. Seguridad humana y justicia social
3. Derecho humano a la alimentación
4. Transformación productiva, internacionalización y acción climática
5. Convergencia regional

Este análisis se centra en el segundo pilar, que abarca temas relacionados con la ciberseguridad. En dicho pilar, hay un apartado específico dedicado a la seguridad digital, donde se reconoce que las tecnologías de la información y las comunicaciones (TIC) son esenciales para la vida diaria y, por lo tanto, se resalta la necesidad de proteger el ciberespacio y a la ciudadanía de posibles amenazas en el entorno digital. Para lograrlo, se propone lo siguiente:

> Se creará la Agencia Nacional de Seguridad Digital y Asuntos Espaciales, a través de precisas facultades extraordinarias otorgadas por el Congreso de la República al Presidente, como parte de la estructura de la Presidencia de la República, cuya Dirección Nacional de Seguridad Digital tendrá como objeto alcanzar un ecosistema digital confiable y seguro e implementar acciones para la protección del Estado en general. Esta dirección será la encargada de planificar, coordinar, articular las actividades que fomenten la preparación y la resiliencia del país, la generación de hábitos de uso seguro y establecerá las propuestas de elementos vinculantes que aseguren el actuar de las entidades del Estado ante posibles amenazas y riesgos de índole digital. (Departamento Nacional de Planeación, 2023).

Es importante indicar que, en 2016, mediante el documento CONPES 3854, se creó la figura del Coordinador Nacional de Seguridad Digital, con funciones muy similares a las que tendría la Agencia Nacional de Seguridad Digital y Asuntos Espaciales. Sin embargo, esta figura presentaba limitaciones importantes, ya que los documentos CONPES y las acciones en ellos previstas no tienen carácter totalmente vinculante. Por ende, iniciativas fundamentales, como la adecuación institucional, solo podrán materializarse si están respaldadas por una ley.

Aunque es prematuro un análisis profundo sobre esta agencia, es importante destacar que ya se aprobó en primer debate el Proyecto de Ley 023 de 2023, que busca su creación. Aún faltan tres debates para su aprobación definitiva, pero se espera que esta iniciativa se construya sobre los avances logrados hasta ahora. Colombia ha tenido logros significativos en materia de ciberseguridad; las instituciones y planes existentes han mostrado resultados positivos, aunque todavía queda mucho trabajo por hacer. Es fundamental preservar y fortalecer lo ya construido, manteniendo la política de ciberseguridad como una política de Estado, no de gobierno.

El PND también contempla la creación y diseño de una estrategia para proteger la infraestructura crítica cibernética del país. Esta estrategia busca salvaguardar la información de las entidades gubernamentales y de la ciudadanía frente a posibles ciberataques y delitos informáticos, aplicando principios de resiliencia y rápida recuperación (Departamento Nacional de Planeación, 2023). Además, el PND menciona la creación de un observatorio de ciberseguridad, aunque no detalla su fecha de implementación, composición ni objetivos.

Actualidad de las propuestas del Gobierno Nacional (2023-2024)

Tomando como guía el documento denominado *Así avanzaron las TIC en Colombia durante el 2023* del MinTIC (2023a), los siguientes son los avances de las propuestas del actual gobierno.

Plan de Gobierno

En conectividad

1. *Tecnología 5G:* Cuatro operadores suministrarán mayor competitividad digital a Colombia. Este avance contribuirá al mejoramiento de la conectividad en 1191 escuelas y al aumento de la cobertura 4G en 34 carreteras primarias y secundarias, abarcando un total de 700 km de mejor conectividad en el país.
2. *Conectividad para cambiar vidas:* Se firmó una alianza con Internexa que permitirá que 384 000 hogares de estratos 1 y 2, ubicados en 36 municipios de los departamentos de Cauca, Chocó, La Guajira, Nariño, Valle del Cauca y la región del Urabá Antioqueño, accedan a internet.
3. *Zonas Comunitarias para la Paz:* Avanza el proceso para garantizar que 1180 escuelas rurales ubicadas en 162 municipios de 19 departamentos del país cuenten con acceso a internet.

En ecosistemas de innovación

1. *Colombia Potencia Digital:* El gobierno busca transformar a Colombia en una potencia digital: productiva, talentosa, exportadora, atractiva y justa. Para lograrlo, se ha destinado una inversión de 2 billones de pesos para acelerar ecosistemas entre 2023 y 2026.
2. *Hub de Ciberseguridad:* En convenio con BIOS, se está formando a 2550 colombianos en pro de fortalecer el ecosistema digital en capacidades y operación de la seguridad digital en el país.
3. *Centros de Inteligencia Artificial:* Se ha contratado el diseño de dos Centros de Inteligencia Artificial en Colombia. Los habitantes de Zipaquirá, en Cundinamarca, y Usme, en Bogotá, serán los primeros beneficiados con esta iniciativa del Gobierno Nacional.

En educación digital

1. *Computadores y laboratorios de innovación para la educación:* En alianza con Computadores para Educar, durante 2023 se entregaron más de 60 000 computadores para estudiantes y docentes, además de 1033 laboratorios de innovación educativa.

2. *Habilidades digitales para los colombianos:* En el marco de una apuesta por mejorar la educación tecnológica, 150 000 personas fueron beneficiadas durante 2023 con programas como Generación TIC, Talento Tech, Inicia con TIC y Mujeres TIC para el cambio, dirigidos a mujeres, jóvenes, niños y adultos mayores.
3. *La estrategia Colombia Programa:* Firmada a finales de 2023, está formando a 11 200 docentes y 896 000 estudiantes. Además, Sena Tech busca impactar a 100 000 estudiantes y docentes durante el cuatrienio.

Plan Nacional de Desarrollo

A la fecha, la Comisión Sexta de la Cámara de Representantes aprobó por unanimidad el primero de los cuatro debates necesarios para que el Proyecto de Ley 023 de 2023, que busca crear la Agencia Nacional de Seguridad Digital y Asuntos Espaciales, se convierta en una realidad en Colombia.

La Agencia Nacional de Seguridad Digital y Asuntos Espaciales será un organismo de carácter técnico y especializado, cuyo objeto será planificar, articular y gestionar los riesgos de seguridad digital en el país, con el fin de prevenir amenazas internas o externas contra el ecosistema digital. Asimismo, trabajará en fortalecer la confianza y seguridad de todas las partes interesadas en el ámbito digital y en establecer la gobernanza e institucionalidad de una política espacial (MinTIC, 2023b).

Conclusiones

Este artículo ha analizado diferentes documentos de política pública que muestran los avances de Colombia en términos de ciberseguridad desde 2011 y se ha realizado un pronóstico preliminar sobre lo que podría venir en el futuro. Si bien aún hay aspectos por mejorar, es evidente que el país ha evolucionado en este ámbito.

En primer lugar, el desarrollo de la ciberseguridad en Colombia se ha manejado como una política de Estado, y no como una política de gobierno. Cada documento CONPES ha construido sobre lo previamente establecido, buscando siempre mejorar, lo que ha permitido un fortalecimiento continuo de la estrategia. El presidente Juan Manuel Santos (2010-2018), a través de los documentos CONPES 3701 de 2011 y CONPES 3854 de 2016, impulsó la creación de organismos clave para la protección del ciberespacio colombiano, como el ColCERT, encargado de coordinar la ciberseguridad y ciberdefensa del país; el Comando Conjunto Cibernético (CCC), y el Centro Cibernético Policial.

Por su parte, el presidente Iván Duque (2018-2022) dio continuidad a estas iniciativas y desarrolló un nuevo documento CONPES 3995 de 2020, que refuerza aspectos como la seguridad digital. Además, en septiembre de 2020, se publicó la primera edición

de la Estrategia Nacional de Ciberdefensa y Ciberseguridad (ECDCS) para los próximos diez años. Esta estrategia se caracteriza por su transversalidad, ya que busca articular todas las políticas, planes e instituciones existentes para lograr mejores resultados. Se trata de un plan integral y orientado al futuro de la seguridad del ciberespacio colombiano.

En segundo lugar, del análisis de las propuestas del actual gobierno en materia de ciberseguridad, se observa un enfoque que se aleja de la concepción tradicional de la seguridad nacional, todavía presente en la mentalidad colombiana, donde la misión de las Fuerzas Armadas se centra en identificar posibles amenazas externas al Estado mediante hipótesis de eventuales conflictos bélicos y en la preparación militar como estrategia de disuasión (Álvarez et al., 2018).

Lo que pretende el nuevo gobierno es construir y fortalecer un concepto multidimensional más acorde con las amenazas de esta época, en el que la seguridad y la ciberseguridad se centren especialmente en la seguridad de la población. Esto concuerda tanto con los documentos de campaña como con el PND, donde se aprecia que se pretende seguir construyendo sobre lo que ya existe y fortalecer aquellos puntos en los que la ciberseguridad colombiana debe trabajar.

Evidencia de lo anterior son los avances que, a la fecha, se han logrado bajo el actual mandato, evidenciados en el último apartado. Todos estos desarrollos surgen del Plan de Gobierno, junto con la aprobación en primer debate del Proyecto de Ley 023 de 2023, que busca crear la Agencia Nacional de Seguridad Digital y Asuntos Espaciales, en concordancia con lo dispuesto en el Plan de Desarrollo.

En consecuencia, el estado actual de la ciberseguridad en Colombia es positivo, sin desconocer que las medidas adoptadas por el gobierno requieren un esfuerzo concertado de todos los actores involucrados, avanzando en temas como el fortalecimiento de los sistemas de seguridad, la colaboración entre organizaciones y la priorización de la educación en ciberseguridad.

Agradecimientos

Los autores desean agradecer a la Universidad Antonio de Nebrija por su apoyo en la realización de este artículo, resultado del trabajo de grado para obtener el título de Máster en Análisis de Inteligencia y Ciber Inteligencia.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Autores

Martín Díaz Acevedo. Magíster en estudios políticos e internacionales e internacionalista, Universidad del Rosario; máster en análisis de inteligencia y ciberinteligencia, Universidad Antonio Nebrija, España.

https://orcid.org/0000-0003-1701-3687 - Contacto: mdiaza7@alumnos.nebrija.es

Álvaro Cremades Guisado. Candidato a doctor en Ciencia Política y de la Administración y Relaciones Internacionales, y licenciado, Universidad Complutense de Madrid; licenciado en ciencia política y de la administración. Máster en analista de inteligencia, Universidad Rey Juan Carlos y Universidad Carlos III.

https://orcid.org/0000-0001-9347-5061 - Contacto: acremades@nebrija.es

Referencias

Álvarez Calderón, C. E., Rosanía Miño, N. A., Sánchez Duque, D. P., & Jiménez Almeira, G. A. (2018). Seguridad y defensa: Conceptos en constante transformación. En C. E. Álvarez Calderón (Ed.), *Escenarios y desafíos de la seguridad multidimensional en Colombia* (pp. 29-83). Sello Editorial ESDEG. https://doi.org/10.25062/9789585652835.01

Bolívar Moreno, G., & Gómez, R. H. (2019). *Transformación social y económica de Colombia a través de las TIC*.

Cano M., J. J. (2011). Ciberseguridad y ciberdefensa: Dos tendencias emergentes en un contexto global. *Sistemas (Asociación Colombiana de Ingenieros de Sistemas)*, *119*, 4-7. http://acistente.acis.org.co/typo43/fileadmin/Revista_119/Editorial.pdf

Caparroso, J. (2023). Viva Air admite que fue víctima de un ciberataque, pero niega que hayan robado datos de 26 millones de clientes. *Forbes*.

Decreto 338. (2022). Por el cual se adiciona el Título 21 a la parte 2 del libro 2 del Decreto Único 1078 del 2015. Presidencia de la República. https://tinyurl.com/zbdhjmd6

Decreto 722. (2022). Por medio del cual se efectúa la designación del Coordinador Nacional de Seguridad Digital. Presidencia de la República. https://tinyurl.com/2bj5mdxe

Departamento Nacional de Planeación (DNP). (2023). *Plan Nacional de Desarrollo 2022-2026: Colombia, Potencia Mundial de la Vida*. https://tinyurl.com/2ef5cys7

El Tiempo. (2021, 1 de septiembre). Aeronáutica Civil recibió ataque cibernético. https://tinyurl.com/2ctgcvcs

Infobae. (2023, 2 de enero). *Las 34 empresas que fueron hackeadas en Colombia durante 2022*. https://tinyurl.com/255bemg3

Ministerio de Defensa Nacional. (2020). *Estrategia Nacional de Ciberdefensa y Ciberseguridad (ECDCS) 2020-2030*. Escuela Superior de Guerra "General Rafael Reyes Prieto". https://doi.org/10.25062/9789585254558

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2021). *Glosario*.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2023a). *Así avanzaron las TIC en Colombia durante el 2023*. https://tinyurl.com/2dbkcuj3

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2023b). *Proyecto del MinTic para la creación de la Agencia Nacional de Seguridad Digital y Asuntos Espaciales pasa el primer debate*. https://tinyurl.com/2by3524z

Noticias Caracol. (2022, 22 de mayo). *Caracol Televisión fue blanco de un ataque cibernético este domingo*. https://tinyurl.com/24a2pntf

OCDE. (2015). *Recomendaciones sobre gestión de riesgos de seguridad digital para la prosperidad económica y social*. http://www.ocde.org/sti/ieconomy/digital-security-risk-management.pdf

Portafolio. (2022, 21 de diciembre). Ataque informático a Sanitas no comprometió información de usuarios. https://tinyurl.com/24dtrgkr

Presidencia de la República. (2011). *Documento CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa*. https://tinyurl.com/37bl44w8

Presidencia de la República. (2016). *Documento CONPES 3854. Política Nacional de Seguridad Digital*. https://tinyurl.com/22dqflh6

Presidencia de la República. (2020). *Documento CONPES 3995. Política Nacional de Confianza y Seguridad Digital*. https://tinyurl.com/2dvmj229

Presidencia de la República. (2022a). *Circular 01 de 2022*.

Presidencia de la República. (2022b). *Directiva Presidencial 02 de 2022*.

Semana. (2022, 4 de marzo). Ataque cibernético al DANE: Director de la entidad reveló detalles del 'hackeo'. https://tinyurl.com/27jxm5k3

Semana. (2022, 6 de septiembre). El gobierno Petro compró sofisticado software de encriptación de llamadas y mensajes de texto; ¿cuánto costó y quiénes tendrán acceso? https://tinyurl.com/2357jedf

Tenorio, M. J. (2009). La evolución del concepto de seguridad y la transformación de la seguridad colectiva en la ONU. *Criterios, 2*(2), 171-197. https://doi.org/10.21500/20115733.1915

TicTac. (2021). *Tendencias del cibercrimen 2021-2022: Nuevas amenazas al comercio electrónico*.

Unión Internacional de Telecomunicaciones, Banco Mundial, Secretaría de la Commonwealth, Organización de Telecomunicaciones de la Commonwealth, & Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN. (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad. Participación estratégica en la ciberseguridad*. https://tinyurl.com/23ul7uqn