EVALUACIÓN DE LA POLÍTICA DIGITAL EN COLOMBIA 2020–2024: DESAFÍOS Y OPORTUNIDADES PARA EL FORTALECIMIENTO DE LA SEGURIDAD DIGITAL A PARTIR DE EXPERIENCIAS INTERNACIONALES

ALEXANDER PALACIOS PALACIOS

ESCUELA SUPERIOR DE ADMINISTRACIÓN PÚBLICA

MAESTRÍA EN ADMINISTRACIÓN PÚBLICA

BOGOTÁ

2025

Evaluación de la política digital en Colombia 2020–2024: Desafíos y oportunidades para el fortalecimiento de la seguridad digital a partir de experiencias internacionales

ALEXANDER PALACIOS PALACIOS

Trabajo de Grado presentado como requisito para optar al título de:

Magister en Administración Pública

Director:

Profesor Dr. Juan de Jesús Sandoval

Escuela Superior de Administración Pública

Maestría en Administración Pública

Bogotá D.C, Colombia

2025

Tabla de contenido

Lista de Figuras

Lista de Tablas

Resumen

Este análisis examina cómo se ha desarrollado la estrategia nacional dirigida a consolidar la seguridad de los datos y fortalecer la credibilidad electrónica (CONPE 3995), considerando los logros obtenidos durante el período 2020 a 2024 en Colombia. Se revisa su impacto en el fortalecimiento de las infraestructuras informáticas dentro del ámbito estatal y en la percepción institucional frente a los retos contemporáneos en materia de ciberseguridad. Adicionalmente se llevó a cabo una comparación entre las políticas y estrategias implementadas en México y España para identificar prácticas exitosas que podrían ser implementadas en el entorno colombiano. Utilizando el análisis documental como metodología y minería de texto, el estudio logra detectar progresos y áreas pendientes para potenciar la resiliencia digital a nivel nacional, aportando así al desarrollo de una comunidad digital más protegida y participativa.

Palabras clave: Confianza digital, seguridad digital, ciberseguridad, CONPES 3995, políticas públicas, análisis comparativo.

Abstract

This study examines how the Public Policy on Trust and Digital Security (CONPE 3995) has been implemented, the achievements obtained during the period 2020 to 2024 in Colombia. It evaluates its efficiency in strengthening trust and information security in public institutions in the face of current cybersecurity challenges. Additionally, a comparison between the policies and strategies implemented in Mexico and Spain was carried out to identify successful practices that could be implemented in the Colombian environment. Using documentary analysis as a methodology and text mining, the study is able to detect progress and pending areas to enhance digital resilience at across the country, which in turn supports the development of a more protected and participatory digital community.

Keywords: Digital trust, digital security, cybersecurity, CONPES 3995, public policies, comparative analysis.

Introducción

La tecnología ha progresado de forma rápida, así como el aumento de la reconfiguración digital de los procesos han transformado ya sea gestión pública o servicios a los ciudadanos en la actualidad. A pesar de esto, estos avances también exponen a los organismos públicos a nuevas vulnerabilidades en el sentido de protección informática. En este escenario, los ciberataques, el ingreso no autorizado a datos confidenciales y la propagación de información errónea constituyen peligros críticos que podrían comprometer tanto la seguridad nacional como la legitimidad que la sociedad otorga a las entidades públicas. En consecuencia, los gobiernos deben desarrollar políticas de seguridad digital unificadas que no sólo aborden los problemas actuales, sino que también prevean y disminuyan las amenazas potenciales.

Analizar y contrastar las tácticas empleadas por otros países con gran experiencia en este ámbito, como España y México, es crucial para desarrollar unas medidas más eficaces en seguridad digital de Colombia. Estos países han desarrollado políticas adaptadas a sus circunstancias particulares, que van desde la salvaguarda de infraestructuras vitales hasta la educación e información de los funcionarios públicos. Con el fin de determinar las mejores tácticas que se pueden utilizar en el contexto colombiano, teniendo en cuenta la singularidad institucional y social de la nación, se busca evaluar las medidas de seguridad en línea en el sector gubernamental colombiano, con un enfoque particular en la aplicación del CONPES 3995 y una comparación con los métodos utilizados en España y México. Para lograrlo se examinarán los elementos técnicos y legales junto a los relacionados al funcionamiento de las organizaciones que influyen en la habilidad del gobierno colombiano para salvaguardar su infraestructura digital y proteger la información de manera efectiva. Las experiencias de otros países exitosos, aportarán insumos claves para mejorar las acciones y establecer políticas más eficientes y perdurables, garantizando así el progreso de Colombia hacia un entorno digital seguro y resistente.

CAPÍTULO I.

1. Tema de investigación

Evaluación de la política digital en Colombia 2020–2024: Desafíos y oportunidades para el fortalecimiento de la seguridad digital a partir de experiencias internacionales.

2. Línea de investigación

Capacidad Institucional en Administración Pública. Sublínea: Capacidad estatal y destinatarios de las políticas públicas

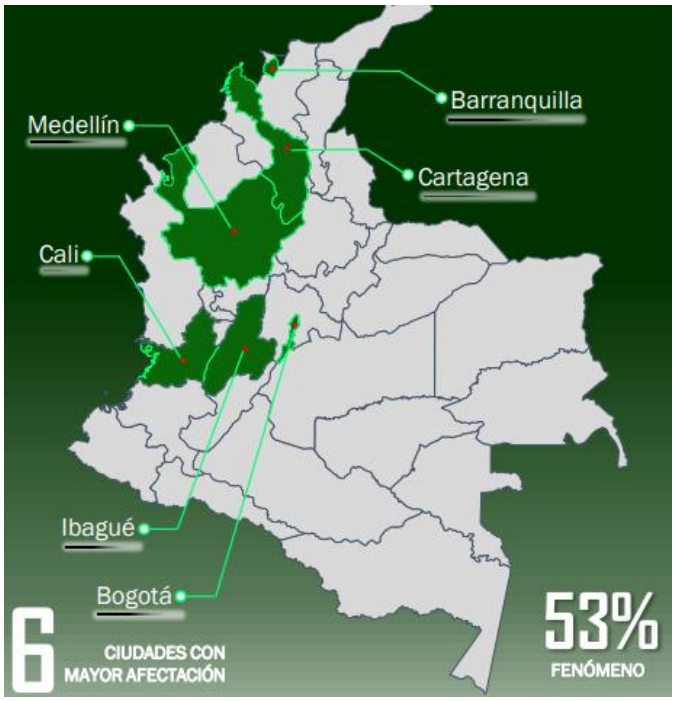
3. Planteamiento y Problema de investigación

En esta era, se está experimentando un mundo donde todos están más interconectados y dependientes de los servicios digitales. Especialmente para los gobiernos encargados de gestionar datos sensibles y prestar servicios necesarios, la seguridad de la información y el respaldo de que la asistencia sea siempre accesible ha adquirido prioridad. Es necesario desarrollar medidas sólidas de ciberseguridad para salvaguardar la estabilidad institucional y la confianza de los ciudadanos frente a ciberamenazas persistentes y cada vez más complejas.

Los gobiernos deben verificar que realmente se cumplan sus políticas de seguridad digital sean estratégicas y pertinentes en este sentido. Para tener éxito, las iniciativas en este ámbito dependen sobre todo de la capacidad de adecuarse a un ambiente de riesgo dinámico y en crecimiento incesante. Dado que los riesgos cambian con tanta rapidez, las soluciones que se elijan deben ser flexibles, escalables y tecnológicamente conscientes. Para responder eficazmente a estos ataques y, en consecuencia, predecir y gestionar mejor los peligros del entorno digital, también son cruciales la cooperación y la coordinación entre muchas entidades. Lamentablemente, no todos los países logran el mismo nivel de eficiencia en materia de protección digital. Por ejemplo, Colombia, los ciberdelitos han tenido un incremento preocupante en los últimos años, lo que hace notable la premura de robustecer la ciberseguridad en todas las áreas. Según la Cámara Colombiana de Informática y Telecomunicaciones (2023), las amenazas informáticas denunciadas crecieron un 20,5% en 2022 Esto implica que en el país se reporta un nuevo incidente cada 8 minutos. Las diferentes modalidades de delitos habituales incluyen la sustracción por plataformas digitales y la no autorización de entradas a sistemas. En 2024, cibercrimen en Colombia alcanzó

niveles alarmantes de acuerdo al Ministerio de Defensa (2024), se denunciaron 69.349 casos, un 19,9% más que los 57.838 casos que se denunciaron en 2023.

Figura 1.
Ciudades con mayor afectación por delitos informáticos en Colombia (2024)



Nota. Adaptado de *Balance Anual CECIP 2024*.

Los diferentes delitos que se presentan en el entorno digital, el número de robos de sitios web registrados pasó de 18.950 en 2021 a 25.413 en 2023, un 34% más. Ese mismo año se registraron 13.318 sucesos de entradas indebidas a sistemas informáticos y 12.775 incidencias de violación de datos personales, lo que supone el incremento del 3% respecto a 2022. Por su parte, se produjo un aumento del 4% en la usurpación de páginas web vinculada a tácticas incluidas las spear phishing, phishing y pharming (Centro Cibernético Policial, 2024).

El número total de delitos informáticos aumentó un 23% de 2023 a 2024, alcanzando los 69.349 casos. El hurto informático (31.095 denuncias), el acceso abusivo a sistemas (11.406), la información personal violentada (10.155) y la usurpación de sitios web (4.716) fueron las acciones más comunes. Con el 53% de los casos a nivel nacional, las ciudades que más han sido amenazadas fueron Bogotá, Medellín, Cali, Barranquilla, Ibagué y Cartagena. Además, surgieron nuevos

peligros como deepfakes, deep voice y robo de cuentas de WhatsApp, lo que refleja la sofisticación y el alcance del cibercrimen en su evolución (Centro Cibernético Policial, 2024).

Estos datos muestran una correlación directa entre la densidad poblacional, el uso de tecnologías en las principales ciudades del país. También el informe periódico de ciberseguridad de la Cámara Colombiana de Informática y Telecomunicaciones, (2023), plantea algunos elementos diferenciadores que ayudan a que las cifras hayan aumentado. Por ejemplo, la incidencia de factores geopolíticos, donde conjuntos de afectaciones avanzadas, como el APT C36[1], han intensificado sus actividades en Colombia. También el aumento de servicios de comercio electrónico y banca digital, con el sector Fintech han tenido un crecimiento del 27% anual en el uso de billeteras virtuales, lo que hace que la exposición incremente y el apetito de los ciberatacantes.

Por otra parte, se encuentra que no existe una sensibilización y concienciación sobre la prevención en cuanto a el descubrimiento anticipado de ataques en fases iniciales y su prevención. El cuantioso pago en la ejecución de empresas colombianas, los sistemas obsoletos, la fuga de talento humano capacitado son las percepciones que se tienen sobre la ciberseguridad como factores que han debilitado la infraestructura de defensa y la competencia de respuesta ante ataques cibernéticos.

Si vemos los sectores más vulnerables, el sector industrial, el gobierno, la educación y la salud concentran el 67% de las denuncias. Esto evidencia una falta de madurez en las estrategias de ciberseguridad de las organizaciones en dichos sectores, las cuales se encuentran rezagadas en términos de detección y respuesta ante ciberamenazas. Las medianas y pequeñas empresas (PYME) son singularmente débiles a raíz de las frágiles estrategias de ciberseguridad, lo que lleva a que solo el 7% de las PYME afectadas por un ciberataque subsistan tras el incidente, mientras que la mayoría enfrenta pérdidas irreparables que comprometen su continuidad.

En cuanto a las entidades públicas en Colombia, al aumentar persistentemente los ciberataques contra entidades del Estado colombiano, esto ha evidenciado fallas sistémicas en la defensa de la infraestructura en línea del gobierno. Estos incidentes han puesto en riesgo la

[1] Grupo de espionaje en América del Sur, activo desde 2018, que ataca principalmente a entidades gubernamentales y grandes empresas en Colombia, incluyendo sectores financiero, petrolero y manufacturero.

disponibilidad de asistencia, la reserva de la información institucional y la confianza pública en las capacidades del gobierno en el periodo 2020-2024.

En 2021 se presentaron 12.146 denuncias por ciberdelincuencia, un 32% más que en 2020, y se denunciaron 247 ataques contra instituciones públicas. Según la Policía Nacional de Colombia (2022), la mayoría de estos incidentes estuvieron relacionados con fraude electrónico (63%), vulneración de información personal (18%) y entrada ilegal a sistemas informáticos (10%). De los 1.342 eventos críticos reportados en el 2022, el 41% fueron resultado de fallas en la actualización de software (CSIRT, 2023).

De acuerdo a los reportes de la Contraloría General de la República (2023), sólo el 18% de las entidades públicas cuenta con equipos dedicados a la ciberseguridad, y el 72% de ellas no cumple las normas mínimas de defensa a la información personal. A pesar del gasto aproximadamente de 98 mil millones de pesos colombianos, los ciberataques ese mismo año causaron pérdidas estimadas en 120 mil millones de pesos colombianos (Cámara Colombiana de Informática y Telecomunicaciones [CCIT], 2023).

Aunque hasta julio 2024 no se han publicado informes exhaustivos, los primeros datos indican que el fenómeno se está intensificando. El ransomware fue la principal preocupación, sobre todo en departamentos de educación y salud, según el CSIRT Gobierno, que informó de un aumento del 20% en los ciberacontecimientos el periodo de enero a junio del 2024, si se relaciona con los datos de estos meses en el año 2023, (CSIRT Gobierno, 2024). Las brechas en los sistemas digitales informados por algunos medios de información, de al menos 15 municipios, el 80% de las cuales fueron causadas por software obsoleto, el Ministerio de Defensa anunció que se destinarían 150.000 millones de pesos para reforzar la ciberseguridad pública (Ministerio de Defensa Nacional, 2024).

Además, según una encuesta realizada entre 1.200 funcionarios públicos, el 62% de ellos cree que sus organizaciones no están preparadas para ataques significativos, siendo el phishing y la suplantación de identidad en sitios web las tácticas más populares (CCIT, 2024). Se estima que en el primer semestre de 2024 se perdieron más de 80.000 millones de pesos como consecuencia de la ciberdelincuencia en el sector público (BPO Economic Forum, 2024).

Este panorama demuestra una desconexión significativa entre las capacidades de respuesta institucional y las amenazas digitales, lo que subraya que es menester evaluar la eficacia de las

regulaciones existentes como el CONPES 3995 y desarrollar planes para reanimar la seguridad del Estado en un plano intrincado.

Colombia ha establecido una estrategia y un marco jurídico para poder reanimar la defensa de la seguridad en el área pública de 2021 a 2024 en respuesta a la creciente susceptibilidad del Estado a los ciberataques. Un primer paso importante fue la adopción del CONPES 3995 de 2020, que ofrecía una forma de fomentar la seguridad digital y la confianza a través de la articulación interseccional, la administración adecuada e integral del riesgo y las mejoras en las capacidades institucionales. Adicionalmente, se fortaleció el Modelo de Seguridad y Privacidad de la Información (MSPI), basado en modelos extranjeros como ISO/IEC 27001 y creado como herramienta para estandarizar las prácticas de protección de la información en las entidades públicas. Su adopción fue promovida por otros actos administrativos, como las Resoluciones 746 de 2022 y 2239 de 2024, que lo hicieron vital como facilitador de la Política de Gobierno Digital.

Simultáneamente, el gobierno aprobó legislación como el Decreto 338 de 2022, que codificó el establecimiento de organismos técnicos de coordinación por parte de las instituciones estatales y creó un marco orientado al control y coordinación de riesgos digitales. De forma paralela, se reformuló los criterios establecidos en la Política de Gobierno Digital, (el Decreto 767, 2022), agregando componentes específicos de ciberseguridad a la transformación digital del Estado. Esta línea estratégica fue reforzada por el Plan Nacional de Desarrollo 2022-2026 (Ley 2294 de 2023), que reconoce la transformación digital como motor del desarrollo territorial y establece metas específicas para la infraestructura, el capital humano y la seguridad de los datos en las entidades públicas. Así, estos cambios normativos marcan avances significativos en la innovación de una política pública convincente para la seguridad digital. Sin embargo, la existencia de lagunas operativas, fragmentación institucional y falta de competencias técnicas en muchas instituciones subnacionales, indica que aún existen grandes obstáculos en el recorrido alrededor hacia una ejecución exitosa y duradera en todo el aparato estatal.

4. Formulación o enunciado del problema

En este sentido, se propone la pregunta de investigación a continuación: ¿Cómo responde la Política Nacional de Confianza y Seguridad Digital en Colombia, a los desafíos y demandas de la seguridad digital en el periodo 2020 - 2024, y cómo las experiencias de México y España pueden contribuir al fortalecimiento de buenas prácticas en Colombia?

5. Justificación de la investigación

Dadas las crecientes ciberamenazas globales que ponen en riesgo la estabilidad institucional, este estudio es pertinente para la evaluación de la política de seguridad digital del Estado colombiano. Con el objetivo de dar una mejor visión de la infraestructura digital, se realiza un análisis comparativo utilizando los casos de México y España, los cuales fueron seleccionados debido a sus enfoques dispares en materia de ciberseguridad pública, historia normativa y valor referencial.

Un excelente ejemplo de política pública competente en el área de seguridad digital es España. Su estructura reguladora se ajusta a la normativa de la UE y fue establecida por organizaciones especializadas como el Instituto Nacional de Ciberseguridad (INCIBE). Esto permite observar prácticas óptimas sobre la protección de las infraestructuras digitales vitales, gobernanza multinivel y articulación normativa. En contraste, México es una norma regional cuyas realidades institucionales son más parecidas a las de Colombia. Desde 2017 desarrolla planes nacionales de ciberseguridad e integra componentes técnicos y organizacionales a su política digital. Su historia permite comparar los avances, dificultades y puntos en común de América Latina.

Esta comparación ayudará a la evaluación crítica del marco actual y permitirá el descubrimiento de lecciones relevantes para la situación colombiana. Al enfatizar el análisis institucional y estratégico y ampliar la discusión sobre políticas públicas en entornos digitales, el estudio contribuye al avance teórico de la administración pública. En términos prácticos, busca generar recomendaciones que mejoren la capacidad del Estado para manejar las ciberamenazas, avanzar en una administración pública más sólida y eficaz a través de la toma de decisiones.

6. Objetivos de la investigación

6.1. Objetivo General

Evaluar la respuesta de la Política Nacional de Confianza y Seguridad Digital de Colombia, frente a los desafíos y requerimientos de la seguridad digital entre 2020 y 2024, y determinar cómo las experiencias de México y España pueden contribuir al fortalecimiento de las prácticas de confianza y seguridad digital en el contexto colombiano.

6.2.Objetivos Específicos

- Analizar la implementación del CONPES 3995 en relación con el estado actual de la confianza y seguridad digital en Colombia, identificando los avances logrados y las brechas existentes en el periodo 2020-2024.
- Comparar los modelos y políticas de seguridad digital implementados en Colombia, México y España, identificando las mejores prácticas y estrategias efectivas en estos países y su posible aplicabilidad en el contexto colombiano.
- Proponer sugerencias para mejorar las prácticas efectivas en el manejo de la confianza y seguridad digital en Colombia, buscando fortalecer su capacidad de recuperación y alineación a estándares internacionales reconocidos.

CAPÍTULO II: MARCO DE REFERENCIA

2.1.ESTADO DEL ARTE

El estado actual combina numerosas investigaciones académicos que abordan problemas sobre la tecnología digital, incluidas sus consecuencias, aplicaciones y dificultades en diversos entornos. Con el fin de orientar y promover el avance de esta investigación, la revisión contiene estudios nacionales y extranjeros que permiten identificar enfoques teóricos, hallazgos pertinentes y lagunas en la literatura.

En primer lugar, el objetivo de la transición digital del sector público es maximizar la eficacia de los servicios públicos mediante el uso de tecnología punta, según los autores Ospina y Zambrano (2022). Los autores analizaron el funcionamiento del gobierno digital en la administración pública colombiana, la necesidad de impulsar la digitalización del Estado, mejorar la conexión en todo el país y educar a la población en ciencia y ciencia. Se hizo hincapié en lo crucial que es mejorar la administración pública y abordar los problemas sociales en campos como la discusión en oposición utilizando tecnologías como la administración electrónica, los datos abiertos, la gobernanza digital, la interoperabilidad, la ciberseguridad y la inteligencia artificial para luchar contra la corrupción, el medio ambiente, la seguridad, la salud y la formación.

Se observaron avances en las políticas de Gobierno Digital y Seguridad del Estado colombiano y en la interoperabilidad y renovación digital de entidades y servicios para los

ciudadanos de manera digitalizada. Aunque se han logrado esos avances mencionados anteriormente en tecnología digital en Colombia¸ aún es urgente mejorar la conectividad en las distintas regiones para impulsar una inclusión digital más amplia.

Se refuerza el compromiso del país con el uso responsable de tecnologías emergentes e incluye lineamientos sobre confianza digital y protección de datos, complementando las acciones previas en materia de seguridad digital en este contexto, con la definición de la Política Nacional de Inteligencia Artificial, en el CONPES 4144 de 2025.

Además, Toro García y colaboradores (2020) investigan cómo las políticas digitales que impulsan la apertura e implicación de los ciudadanos tienen un efecto en el análisis exhaustivo del impacto de las TIC. Martínez- Coral, (2017), investigó cómo la confianza en la política afecta el acogimiento de la digital tecnología. Se enfatizó la necesidad de promover un cambio cultural que impulse un cambio hacia un gobierno electrónico más inclusivo y eficiente, ya que la desconfianza en las instituciones públicas puede impedir el avance de las iniciativas de gobierno en línea.

Esta perspectiva apoya el trabajo de Tabardino Muñoz (2022), que examina cómo se regulan los servicios públicos de comunicación y cómo se modifican para la esfera digital con el fin de crear un marco jurídico que fomente acceso equitativo al material en línea.

En referencia al segundo tema, el reciente estudio realizado por Ramírez Camargo y Rincón Pinzón (2022) analizó considerar mantener la garantía de los datos en el medio público colombiano a la luz de los riesgos potenciales de uso indebido o exposición de los datos. Conservar la privacidad de la información es esencial para evitar posibles violaciones que puedan poner en peligro a los ciudadanos y a los funcionarios públicos que se relacionan con los organismos gubernamentales (Ospina y Zambrano, 2022). Como ya se ha dicho, la inteligencia artificial no solo agiliza los procesos existentes, sino que también plantea problemas de ciberseguridad que exigen la adopción de normativas estrictas y normas morales para evitar la manipulación y el uso indebido de los datos. Según Campos Ramírez (2017), los usuarios de las plataformas digitales en la sociedad actual están cada vez más preocupados por la seguridad en línea, lo que subraya el interés de aplicar una táctica integral que abarque medidas preventivas y correctivas con el fin de gestionar eficazmente las posibles situaciones relacionadas con la ciberseguridad.

Según un estudio de García Alonso et al. (2020) sobre el proyecto Vive Digital I (2010-2014), si bien este programa ha mejorado la conectividad y la infraestructura en las zonas urbanas, aún existen retos importantes en las zonas rurales. Se señala que aumentar la inversión en

educación podría ayudar a estas zonas a utilizar y comprender las TIC, haciendo énfasis en la inclusión digital desde una perspectiva global y unificadora.

Frey (2005) examina cómo las políticas de inclusión en Brasil y Europa podrían ayudar a las personas empobrecidas a acceder a la tecnología. Eliminar los obstáculos financieros y tecnológicos a la participación ciudadana debería ser el principal objetivo de la inclusión digital, según Frey, que también subraya que el acceso equitativo a las TIC puede ser esencial para promover la cohesión social y reducir la desigualdad. Finalmente, de acuerdo a Moreno (2021), la digitalización no sólo aumenta la eficacia administrativa, sino también la accesibilidad y la apertura, lo que fomenta una relación de participación entre el público y el gobierno.

2.2.MARCO TEÓRICO

Teoría de Fortalecimiento Institucional en Seguridad Digital

Esta teoría, desarrollada por Díaz Acevedo y Cremades Guisado (2024), postula que las políticas públicas para ser efectivas en el ámbito digital dependen críticamente del desarrollo de capacidades técnicas especializadas y de una coordinación interinstitucional fluida. Su enfoque se centra en cómo las instituciones deben evolucionar para enfrentar amenazas cibernéticas a través de la producción de equipos multidisciplinarios, el acogimiento de tecnologías avanzadas y la implementación de protocolos estandarizados. Dadas las continuas dificultades en la gobernanza digital en Colombia, incluyendo la división de funciones entre agencias gubernamentales y la omisión de uniformidad en las disposiciones de seguridad, esta teoría se vuelve pertinente. La reacción a los ciberataques contra infraestructuras clave sirve como ilustración específica de las vulnerabilidades institucionales, como se observa en la falta de cooperación entre el Departamento Nacional de Planeación (DNP) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Según la hipótesis, las medidas de seguridad digital seguirían siendo reactivas en lugar de preventivas en ausencia de un crecimiento de la capacidad tecnológica y de una cooperación eficiente de los actores.

Teoría de la Capacidad Estatal Digital

La teoría de la capacidad del Estado digital, que complementa a la anterior, examina la estructura interna del Estado y su potencial para adoptar y mantener los avances tecnológicos (Cárdenas, 2010; Galindo, 2020). Cejudo y Michel (2017) y Margetts y Dunleavy (2013) afirman

que la colaboración interinstitucional, los marcos regulatorios adaptables y los recursos tecnológicos son los tres pilares interdependientes que sustentan esta capacidad. Además de la infraestructura tecnológica, como las redes de fibra óptica o los centros de datos seguros, los recursos técnicos también implican el desarrollo de la experiencia humana en campos vitales como la inteligencia sobre amenazas y la criptografía. Por el contrario, el marco normativo necesita regulaciones dinámicas que aborden nuevos problemas. Por ejemplo, la Ley 1581 de 2012 de Colombia, que regula el manejo de datos personales, se ve desafiada por la aparición de nuevos tipos de ciberdelincuencia. Por último, la colaboración interinstitucional enfatiza la necesidad de redes de cooperación entre organizaciones internacionales, el sector comercial y las instituciones públicas para intercambiar inteligencia contra amenazas transnacionales como el ciberespionaje y el hacktivismo.

Teoría de la Gobernanza Digital

Desarrollada por autores como Janowski (2015) y Luna-Reyes y Gil-García (2014), la noción de gobernanza digital se centra en el cambio de las instituciones de gestión y toma de decisiones del Estado más que en la mera implementación de nuevas tecnologías. Según este punto de vista, la horizontalización de los procedimientos, la promoción de colaboración pública a través de plataformas inclusivas y el refuerzo de las capacidades institucionales para manejar tecnología sofisticada son necesarios para un gobierno eficiente en la era digital. Esta teoría permite el análisis de herramientas como el CONPES 3995 de Colombia, que pretende describir los múltiples actores (gobierno, industria y académicos) implicados en la creación de normativas de seguridad digital. La forma en que la gobernanza digital resuelve los conflictos entre centralización y descentralización es un componente crucial, especialmente en una nación con importantes divisiones geográficas. Por ejemplo, aunque Bogotá avanza a pasos agigantados en los servicios digitales integrados, zonas como Chocó luchan con problemas de red que dificultan la aplicación de normas coherentes.

Teoría de la Gestión del Riesgo Público

Esta teoría, de Hood, Rothstein y Baldwin (2001) y modificada para la esfera digital por organizaciones como ENISA (2020) y NIST (2022), considera el riesgo cibernético como un

problema polifacético que requiere medidas preventivas y predictivas. Para aumentar la resiliencia, sugiere que los gobiernos desarrollen la capacidad de reconocer los riesgos sistémicos (como los ataques a las infraestructuras energéticas), distribuyan estratégicamente los recursos y extraigan lecciones de sucesos anteriores. Su uso puede verse en Colombia en la investigación de los peligros de la firma digital, donde se evaluaron elementos sociales, incluida la desconfianza pública en los instrumentos electrónicos, además de las vulnerabilidades tecnológicas (Rodríguez, 2021). La teoría también destaca las repercusiones políticas de los fallos en la seguridad digital, como el efecto en la confianza pública tras un hackeo exitoso, que obliga a los responsables políticos a encontrar un equilibrio entre las soluciones tecnológicas y el diálogo abierto con el público.

Teoría de la Confianza Institucional en Entornos Digitales

Formulada por Bélanger y Carter (2008) y ampliada por Carter, Thatcher y Wright (2016), esta teoría sostiene que la adopción de servicios digitales públicos depende de la percepción ciudadana sobre tres factores: seguridad técnica, protección de datos y competencia institucional. La confianza no se restringe a la eficacia de los instrumentos tecnológicos, sino que funciona como un símbolo de legitimidad estatal. En Colombia, esta teoría explica fenómenos como la reticencia a usar plataformas electorales digitales tras fallas en procesos de autenticación biométrica en 2023, que erosionaron la credibilidad de la Registraduría Nacional. Además, resalta cómo las políticas de ciberseguridad cumplen un rol simbólico: al invertir en certificaciones ISO/IEC 27001 o comunicar protocolos de cifrado, el Estado envía señales de seriedad que refuerzan la confianza, incluso si los ciudadanos no comprenden los detalles técnicos.

Teoría de la Gestión del Riesgo Digital Sistémico

Aunque no mencionada explícitamente en los textos base, esta teoría emerge de la integración de los enfoques anteriores. Propone que los riesgos digitales (p. ej., disrupciones en servicios financieros por ataques ransomware) deben gestionarse como amenazas sistémicas que afectan múltiples sectores simultáneamente. Agencias como el NIST (2022) enfatizan la necesidad de marcos de evaluación de riesgos que consideren interdependencias tecnológicas, como cómo un ataque a proveedores de servicios en la nube podría paralizar múltiples entidades públicas. En Colombia, esta perspectiva es crucial para entender los efectos en cascada de incidentes como el ataque a la red eléctrica en 2022, que evidenció vulnerabilidades compartidas entre infraestructura física y sistemas de control digital.

La aplicación del CONPES 3995 está estrechamente ligada a las nociones mencionadas. Mientras que la teoría de la capacidad estatal examina si las entidades territoriales disponen de los medios para aplicar sus directivas, la idea de fortalecimiento institucional explica la creación del Comité de Seguridad Digital. La gestión pública de los riesgos evalúa si los protocolos prevén peligros complejos, mientras que la gobernanza digital se interroga sobre la inclusión de actores no estatales en este comité. Por último, que los ciudadanos crean que estos esfuerzos son suficientes para adoptar servicios como el voto electrónico o la facturación electrónica depende de la confianza institucional.

Cuando se combinan, estas teorías muestran que en Colombia, la seguridad digital es un tema complejo que requiere cooperación interinstitucional, marcos legislativos flexibles, inversión consistente en capacidades y una buena comunicación para fomentar la confianza. Las contradicciones teóricas no resueltas entre la centralización y la adaptación al contexto se reflejan en la persistencia de brechas, como la existente entre las políticas nacionales y las capacidades locales.

a. MARCO CONCEPTUAL

Ciberresiliencia

La ciberresiliencia es una estrategia global para gestionar los riesgos digitales que va más allá de los métodos convencionales que se centran únicamente en la seguridad. Describe la competencia en un sistema, estructura o Estado que prevee, frustrar, acomodarse y reparar acontecimientos perturbadores como ciberataques o fallos técnicos sin poner en peligro la capacidad de seguir desempeñando sus funciones esenciales. La base de esta capacidad es la detección proactiva de vulnerabilidades, para lo que se necesitan procedimientos metódicos de monitorización y evaluación que permitan prever posibles situaciones de riesgo (Guijarro-Rodríguez et al., 2018).

Además, la resiliencia cibernética incluye elementos adaptativos que permiten la reconfiguración dinámica de las estructuras de seguridad basándose en las lecciones aprendidas durante las crisis. En este sentido, Díaz Acevedo y Cremades Guisado (2024) destacan la importancia de los mecanismos de aprendizaje organizativo como base para el desarrollo continuo de protocolos defensivos. Este constructo tiene en cuenta cuatro elementos clave: la resiliencia operativa reforzada por redundancias cruciales, la recuperación adaptativa que incorpora las

lecciones aprendidas, la capacidad predictiva mediante análisis futuros y la transformación evolutiva del sistema de seguridad.

Defensa en Profundidad

Una táctica de ciberseguridad conocida como «defensa en profundidad» implica poner en marcha muchos niveles de defensa para frustrar posibles ataques a recursos vitales. Esta filosofía, según Vega Briceño (2021), es un enfoque multicapa que articula controles administrativos (modelos de acceso de Confianza Cero), técnicos (criptografía cuántica) y físicos (barreras biométricas), creando una arquitectura redundante que refuerza la idoneidad de contención respecto a los ataques cibernéticos. Además de la prevención, este paradigma hace hincapié en la identificación rápida y la contestación eficaz a los incidentes.

La Organización Internacional de Normalización también ha especificado las normas mínimas para una aplicación satisfactoria de capas de seguridad en sistemas críticos a través de ISO/IEC 27001 y sus ampliaciones (ISO/IEC, 2016). Por lo tanto, lograr una postura de defensa sólida y duradera requiere la integración armoniosa de componentes tecnológicos, humanos y organizativos. Esta estrategia es cada vez más aplicable en sistemas institucionales complejos como el colombiano, debido a la ascendente interdependencia de las infraestructuras vitales y la fragilidad ante amenazas híbridas. Por lo tanto, la defensa en profundidad permite la implementación de niveles de defensas que, incluso en la situación en la que falla un nivel de seguridad, prohíben el acceso no deseado.

Tríada CIA

Modelo de confidencialidad, integridad y disponibilidad (CIA) simboliza el marco fundamental de la seguridad de la información. Este trío garantiza que los datos son precisos y completos, están disponibles cuando se necesitan y sólo pueden acceder a ellos quienes están autorizados (Sánchez Vera et al., 2022). La confidencialidad se salvaguarda mediante técnicas como el cifrado asimétrico (por ejemplo, RSA-4096), que previene accesos no autorizados, mientras que la integridad se asegura utilizando funciones hash como SHA-3, que admiten cotejar que la información no haya sido alterada de forma maliciosa o accidental. Sin embargo, para mantener la disponibilidad se utilizan sistemas distribuidos como blockchain, que ofrecen una gran resistencia a las interrupciones del servicio. Candau (2021) amplía esta idea añadiendo ideas como el no repudio, garantizado por documentos temporales verificados, y la autenticidad, respaldada

por firmas digitales. Estas directrices permiten establecer planes de seguridad fiables en plataformas que manejan datos sensibles, como los sistemas de contratación pública o los historiales médicos electrónicos, en el entorno de la administración pública. El estricto cumplimiento de estos tres pilares fomenta la confianza de los usuarios finales al tiempo que refuerza la seguridad tecnológica.

Confianza Institucional Digital

Un componente crucial para que los ciudadanos acepten con éxito los servicios electrónicos es la confianza institucional digital. Navarrete Yáñez et al. (2022) abordan este constructo desde dos ejes básicos: la ética institucional, que se traduce en un compromiso con la translucidez algorítmica y el acatamiento a los derechos digitales, y la competencia técnica, entendida como la capacidad de las instituciones para implementar estándares sólidos como los definidos por el NIST. El deseo de los usuarios de comprometerse con las plataformas digitales gubernamentales está condicionado en gran medida por su impresión sobre la validez y eficacia del procedimiento de los datos personales.

En esta línea, Suárez Vásquez (2022) presenta la idea de «accountability tecnológica», que evalúa la responsabilidad en el manejo de datos sensibles mediante indicadores de control y supervisión externa. Rodríguez (2021) demuestra cómo estos factores afectan la decisión de las personas de utilizar servicios como el acceso remoto a procesos notariales o la inscripción digital en el registro civil. El alcance de las estrategias de los cambios digitales en Colombia se ve seriamente limitado por la falta de confianza en organizaciones como la Registraduría Nacional del Estado Civil. En consecuencia, para mejorar esta confianza se requiere una estrategia integral que incorpore la integridad institucional, la seguridad técnica y una comunicación clara.

Confianza Digital

La convicción razonable de que los actores, sistemas o plataformas en línea se comportarán de forma segura, moral y predecible en contextos digitales se conoce como confianza digital. Este elemento es crucial para promover la innovación en el uso de los servicios digitados y para facilitar el canje de datos, la colaboración y el comercio electrónico (Suárez Vásquez, 2022). La seguridad técnica (por ejemplo, utilizando protocolos TLS 1.3), la transparencia operativa (por ejemplo, a través de registros inmutables) y el cumplimiento normativo (por ejemplo, GDPR o su equivalente en América Latina) son los tres pilares en los que se basa esta confianza, según Bélanger y Carter

(2018). Además, la CEPAL (2021) sugiere ampliar esta visión añadiendo elementos de sostenibilidad mediante la idea de una huella digital ecológica y la interoperabilidad a través de API estandarizadas. Adicionalmente, la percepción de los ciudadanos respecto a la defensa de sus datos individuales y la suficiencia de soluciones de las plataformas digitales ante problemas de seguridad son indicadores de confianza digital. Producir confianza y promover el uso de tecnologías digitales seguras, se requiere implementar medidas educativas y regulatorias en lugares como Colombia, donde la percepción de riesgo está influenciada por información falsa y falta de alfabetización digital.

Gobernanza Digital

El grupo de normas, marcos y técnicas que facilitan la obtención de soluciones, creación de medidas y la vigilancia del entorno digital se conoce como gobernanza digital. En esta cooperación multinivel participan gobiernos, empresas de TI, organizaciones internacionales y la sociedad civil (OCDE, 2020). En este sentido, la ONU ha subrayado la necesidad de crear marcos jurídicos adaptables pero estrictos que respalden el ejercicio de los derechos digitales sin ahogar la creatividad (UN E-Government Survey, 2022). Temas importantes como el trámite de información, la integración de sistemas, además de regulación de tecnologías punteras, entre ellas la inteligencia artificial también forman parte de la gobernanza digital. A nivel latinoamericano, la CEPAL (2021) ha señalado que los Estados enfrentan el reto de equilibrar la soberanía digital con la ejecución de estándares internacionales de seguridad y privacidad. Iniciativas como el Marco de Referencia de Arquitectura Empresarial (MRAE) del Ministerio de TIC, que fomenta la integración de la tecnología en las instituciones públicas al tiempo que se adhiere a las normas de eficiencia y seguridad, son ejemplos de cómo Colombia demuestra este equilibrio. Sin embargo, existen disparidades en la aplicación de estas normas, lo que socava los procedimientos de gobernanza y crea asimetrías en la provisión de la oferta digital. Establecer procedimientos de evaluación continua y reforzar las capacidades institucionales son esenciales en este sentido para implementar una gobernanza digital eficiente, legal y flexible.

Transformación Digital

Las organizaciones, en particular las del sector público reorganizar sus procesos empresariales, optimizar a la atención pública y emerger la cualidad de la producción y la misión, utilizando la tecnología digital y añadir valor para la población en general a través de un proceso

estructural y estratégico conocido como «transformación digital» (OCDE, 2020). Este cambio incluye un cambio cultural, organizativo y normativo procura concentrar los proyectos públicos en torno al ciudadano. El CONPES 3975 de 2019 y la estrategia de Gobierno electrónico, que sugieren una arquitectura estatal construida sobre datos, interoperabilidad y servicios centrados en el ciudadano, han apoyado esta estrategia en Colombia (DNP, 2019). Sin embargo, hay una serie de obstáculos que impiden la realización de esta transformación, como la falta de competencias humanas especializadas, la fragmentación tecnológica y la escasa madurez digital institucional (MinTIC, 2022). El Índice de Gobierno Digital (IGD) indica que varias organizaciones presentan deficiencias en áreas críticas como la gestión del cambio y la seguridad digital. En este sentido, la transformación digital requiere una fuerte articulación con otros aspectos del ecosistema digital, incluyendo la gobernanza de datos, la ciberseguridad y la alfabetización electrónica. La consolidación de un entorno electrónico inclusivo, resistente y centrado en el valor público solo puede lograrse de esta manera.

Seguridad de la Información

La seguridad de los datos es un conglomerado de normas, prácticas y controles destinados a salvaguardar salvaguardar los activos informáticos contra los riesgos externos e internos, manteniendo la probidad, confidencialidad y reservas de la información. Incluye la gestión de peligros, la formación de los empleados y el establecimiento de funciones y responsabilidades diferenciadas dentro de las empresas, junto con componentes tecnológicos como la autenticación multifactor y el cifrado. En concreto, el ciclo PHVA (Planificar-Hacer-Verificar-Actuar), que facilita desarrollar continuamente en contextos técnicos intrincados, constituye la base del paradigma mecanismo de dirección de la información más segura.

Nota. Los criterios de selección de países se basaron en su desempeño en los índices globales de ciberseguridad (IMD, ONU e ITU) entre 2019-2024.

Los casos multinacionales examinados, demuestran que para el éxito de la ciberseguridad es necesaria una variedad de tácticas adaptadas a situaciones concretas, en lugar de depender únicamente de una táctica. La primera es la aparición de la colaboración multisectorial como eje transversal: Israel amplió su ecosistema de startups gracias a las sinergias entre su Unidad 8200 y el sector privado, mientras que Estonia logró consolidar su administración electrónica mediante asociaciones entre instituciones públicas y empresas tecnológicas. Similar a la Teoría de la Triple

Hélice, este modelo subraya la importancia de cooperación entre gobiernos, empresas y universidades.

Tabla 1.

Casos Internacionales - Éxito en Ciberseguridad

País	Estrategias Clave	Resultados Destacados	Contexto
Estonia	**1. Sistema X-Road**: Plataforma de intercambio seguro de datos entre instituciones públicas (salud, educación, justicia) con cifrado de extremo a extremo. **2. Modelo Zero Trust**: Autenticación multifactorial obligatoria para servicios críticos (ej. votación electrónica). **3. Residencia Digital**: Permite a extranjeros acceder a servicios estatales mediante blockchain y verificación biométrica.	- **Fraude electoral**: Menos del 0.25% en elecciones desde 2005. - **Reconocimiento**: 1° en Índice de Gobierno Electrónico de la ONU (2022).	Estonia sufrió ciberataques masivos en 2007, lo que impulsó su transformación en referente global. Es sede del Centro de Excelencia en Ciberdefensa de la OTAN.
Singapur	**1. Marco CCOP**: Código de Prácticas de Ciberseguridad que obliga a empresas de sectores críticos (banca, energía) a adoptar estándares como el NIST. **2. Programa Safer Cyberspace**: Capacitación ciudadana en phishing y ransomware mediante simulacros. **3. AI.SG**: Uso de inteligencia artificial para predecir amenazas en tiempo real en el sector financiero.	- **Ranking global**: 1° en Índice Global de Ciberseguridad (IMD, 2023). - **Reducción de incidentes**: 40% menos en fraudes financieros (2020-2022).	Singapur prioriza la colaboración público-privada. Su Agencia de Ciberseguridad (CSA) lidera iniciativas con empresas como Singtel y DBS Bank.
Corea del Sur	**1. Ley de Auditorías Anuales**: Empresas críticas deben someterse a evaluaciones obligatorias; multas de hasta el 3% de sus ingresos por brechas. **2. KR-CERT**: Sistema de respuesta a incidentes que bloqueó 2.3 millones de ataques en 2022. **3. Centro de IA**: Detecta amenazas en redes 5G usando machine learning.	- **Velocidad de respuesta**: Contención de ataques en menos de 12 horas (vs. 21 días promedio global). - **Preparación**: 1° en Índice de Preparación Cibernética (Microsoft, 2023).	Corea del Sur invierte el 5% de su PIB en I+D tecnológico. Su enfoque combina regulación estricta e innovación en IA y 5G.
Israel	**1. Unidad 8200**: Cuerpo de inteligencia militar que forma expertos en ciberseguridad, luego contratados por empresas como Check Point. **2. DIN SPEC 91476**: Estándar para proteger vehículos autónomos de ciberataques, adoptado por la UE en 2023. **3. CyberSpark**: Hub tecnológico que integra empresas, universidades y gobierno para compartir inteligencia.	- **Exportaciones**: USD 8,800 millones en ventas de tecnología de ciberseguridad (2022). - **Detección**: 95% de ataques a infraestructuras críticas neutralizados antes de su ejecución.	Israel dedica el 8% de su presupuesto de defensa a ciberseguridad. Es llamado "Nación Startup" por su ecosistema de innovación.
Finlandia	**1. Educación Obligatoria**: Cursos de ciberseguridad en escuelas y universidades, con énfasis en ética digital. **2. Herramienta TRAUMA**: Simulador de crisis para empresas, desarrollado por el Centro Nacional de Ciberseguridad (NCSC-FI). **3. Alianzas Tecnológicas**: Nokia y F-Secure colaboran en proteger redes 6G y energías limpias.	- **Concienciación ciudadana**: 87% de la población identifica correos phishing. - **Ranking UE**: Top 3 en Índice de Ciberseguridad de la UE (2023).	Finlandia combina educación y tecnología. Su enfoque en energías renovables incluye protección de redes inteligentes contra ataques.

Pero la financiación de tecnología innovadora está resultando clave. Entre los ejemplos de cómo la aplicación de tecnologías como blockchain, IA y confianza cero no sólo reduce los riesgos, sino que también impulsa la confianza pública se incluyen, cabe citar el uso por Singapur de sistemas de IA para predecir amenazas financieras y la aplicación por Corea del Sur del aprendizaje automático en las redes 5G. Además, la educación obligatoria en ciberseguridad de Finlandia pone un fuerte énfasis en un enfoque proactivo que da a los usuarios finales la capacidad de disminuir las debilidades humanas como el phishing. Por último, la capacidad de responder a un panorama de peligro en continuo cambio es posible gracias a una adaptación flexible de la normativa. Los marcos normativos actuales son esenciales para salvaguardar las infraestructuras vitales, como demuestran la norma israelí DIN SPEC 91476 para vehículos autónomos y la Ley de Auditoría Anual de Corea del Sur, que impone sanciones por infracciones de seguridad relacionado con las ganancias de las empresas. Estos casos, junto con el papel pionero de Estonia en normas internacionales como la Declaración de Tallin, demuestran que la normativa debe ser tan flexible como las ciberamenazas.

b. Contexto internacional comparado España y México

En la presente investigación, se consideran los países de España y México como referencias comparativas, ya que sus políticas públicas de gobernanza digital, ciberseguridad estatal y protección de infraestructuras críticas siguen caminos distintos pero complementarios. México representa un ejemplo intermedio, con avances legislativos significativos en proceso y problemas en curso en términos de articulación institucional, mientras que España ha cimentado un marco sólido con respaldo operativo y normativo. España fue seleccionada por su pertenencia a la Unión Europea, su arquitectura institucional especializada altamente eficaz y su marco reglamentado de defensa electrónica, que está en alineada con legislación de alto nivel de la UE (como la Directiva NIS2). Por su tamaño, peso político en el área y creciente interés en instituir normas de ciberseguridad en respuesta a los nuevos peligros del mundo digital, México es un gran caso de estudio para comparar con Colombia y sirve como referencia relevante para América Latina.

Modelo de España

España introdujo importantes mejoras en su marco institucional y normativo para la seguridad digital entre 2020 y 2024. La protección del ciberespacio nacional, la resiliencia de las

infraestructuras vitales, la respuesta coordinada ante incidentes y una cultura de ciberseguridad implementada son los principales objetivos de la política de seguridad Nacional electrónica, 2022. Este plan tiene coherencia internacional y fuerza vinculante al estar alineado con el marco europeo establecido por la Directiva NIS2 (Directiva (UE) 2022/2555).

A nivel normativo destaca el Real Decreto 210/2024 por el que se reorganiza el Ministerio para la Transformación Digital y la Función Pública y se crea Dirección General en Datos, encargada la seguridad y gestión estratégica de la información estatal (BOE, 2024). Además, en 2023, la nación propuso un nuevo anteproyecto de Ley Orgánica de Ciberseguridad, que pretende reforzar la coordinación entre diferentes actores Públicos frente a las amenazas digitales (Consejo de Ministros, 2023). El Esquema Nacional de Seguridad (ENS), que establece las normas mínimas de seguridad para proteger la información estatal, fue revisado en 2022, se incluyen normas actualizadas para la gestión de riesgos, la autenticación y la trazabilidad (Centro Criptológico Nacional, 2022). A través de soluciones seguras, interoperables y orientadas al ciudadano, el Plan de Digitalización de las Administraciones Públicas 2021-2025 refuerza la apuesta del Estado por la modernización institucional (Gobierno de España, 2021).

El Instituto Nacional de Ciberseguridad (INCIBE), organismo adscrito al Ministerio de Economía y Transformación Digital, complementó esta política con su Plan Estratégico 2021-2025. Este plan esbozaba la respuesta institucional del Estado a las amenazas digitales a través de iniciativas para construir el ecosistema de innovación, cultivar el talento y aumentar la concienciación pública. Al encabezar programas como Incibe Emprende, Ciberinnova, Talento Hacker y Confía, cuyo objetivo es crear capacidades en los sectores público y privado, se ha hecho un nombre como la principal organización del ecosistema español de ciberseguridad.

Modelo de México

En comparación con España, México muestra un desarrollo más fragmentado. Su legitimidad y relevancia han sido cuestionadas porque, aunque se cuenta con la Estrategia Nacional de Ciberseguridad desde 2017, no ha sido actualizada ni ejecutada a fondo en los últimos años (Gobierno de México, 2017; Observatorio Nacional de Ciberseguridad, 2022).

Para llenar esta laguna, se han defendido varias ideas legislativas en el periodo 2020-2024. Destaca la iniciativa de Ley Federal de Ciberseguridad 2023, presentado al Congreso de la Unión, que sugiere establecer un Registro Nacional de Ciberincidentes y una Agencia Nacional de Ciberseguridad para crear una estrategia federal completa (Senado de la República, 2023).

Además de establecer principios rectores como la defensa de los derechos digitales, la autonomía tecnológica y la rendición de cuentas, esta iniciativa sugiere métodos de coordinación interinstitucional. Simultáneamente, la ciberseguridad se incorpora como prioridad transversal en el Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024, enfatizando la necesidad de dotar a las instituciones de capacidades técnicas para responder a amenazas complejas, especialmente en los sectores energético, sanitario y financiero (Secretaría de Seguridad y Protección Ciudadana, 2020). No obstante, siguen existiendo fallas estructurales, como el abandono de un sistema judicial cohesionado y el bajo relacionamiento entre las partes públicas y privadas.

2.3.MARCO NORMATIVO

La normativa sobre seguridad y confianza en el entorno digital se organiza tanto a nivel nacional como internacionalmente. Cada nación ha establecido sus propias regulaciones y políticas adaptadas a sus circunstancias y necesidades particulares. Al mismo tiempo que las amenazas digitales siguen expandiendo su alcance global, se han fomentado acuerdos y tratados internacionales para promover la colaboración y la estandarización de medidas de seguridad informática. Estos convenios permiten una acción conjunta y efectiva contra delitos cibernéticos y otras amenazas que trascienden fronteras nacionales.

Tabla 2.

Convenios y tratados internacionales que Impactan a Colombia

Convenios y Tratados Internacionales que Impactan a Colombia			
Convenio/Tratado	**Tipo**	**Año de Adopción**	**Descripción/Objetivo**
Convención de Budapest sobre Ciberdelito	Tratado Internacional	2001	Colombia es parte de este tratado, que establece un marco de cooperación para combatir el cibercrimen a través de medidas legales y cooperación judicial internacional.
Convenio 108 del Consejo de Europa (y Protocolo Adicional 108+ sobre Protección de Datos)	Convenio Internacional	1981 (Protocolo 2018)	Colombia se adhirió a este convenio, que establece estándares para la protección de datos personales y la privacidad, y que fomenta la cooperación internacional en la transferencia de datos.
Guías de Seguridad Cibernética de la OCDE	Directrices Internacionales	2015	La OCDE promueve directrices que Colombia sigue para la gestión de riesgos cibernéticos y la cooperación público-privada, fortaleciendo la resiliencia en la seguridad digital.
ISO/IEC 27001 e ISO/IEC 27002	Estándares Internacionales	Adoptados en Colombia	Estándares internacionales sobre gestión de seguridad de la información, implementados en entidades que manejan información crítica en Colombia para asegurar la confidencialidad, integridad y disponibilidad de datos.
Reglamento General de Protección de Datos (GDPR)	Reglamento Internacional	2018	Aunque pertenece a la UE, Colombia adapta algunos lineamientos del GDPR en la Ley 1581 de Protección de Datos, para asegurar la transferencia internacional segura de datos personales.

Tabla 3.
Leyes y Normativas Colombia

Normograma Seguridad Digital Colombia			
Norma/Estándar	**Tipo**	**Año**	**Descripción/Objetivo**
CONPES 3701	Política Pública	2011	Define los lineamientos de ciberseguridad y ciberdefensa en Colombia para fortalecer la capacidad de protección ante amenazas cibernéticas.
Ley 1581 de 2012 (Ley de Protección de Datos Personales)	Ley	2012	Regula el tratamiento de datos personales en el sector público y privado, estableciendo principios de seguridad, legalidad y libertad.
Decreto 1377 de 2013	Decreto	2013	Complementa la Ley 1581, especificando obligaciones para las empresas en cuanto a la protección de datos personales.
Ley 1273 de 2009 (Ley de Delitos Informáticos)	Ley	2009	Tipifica los delitos informáticos y establece sanciones para actividades como acceso abusivo, sabotaje y manipulación de sistemas informáticos.
CONPES 3854 (Política Nacional de Seguridad Digital)	Política Pública	2016	Fortalece la capacidad de respuesta a amenazas cibernéticas, promoviendo el uso seguro de las TIC y la protección de infraestructuras críticas.
Política de Gobierno Digital	Política Pública	2018	Incluye la seguridad digital como un pilar para la eficiencia en la gestión pública, impulsando la transformación digital segura en el sector estatal.
Plan Nacional de Desarrollo	Plan Estratégico	2019	Incluye la seguridad y confianza digital como principios clave para el desarrollo económico y social en el contexto de la transformación digital en Colombia.
CONPES 3995 (Política Nacional de Confianza y Seguridad Digital)	Política Pública	2020	Desarrolla una estrategia para fortalecer la confianza y seguridad en el uso de tecnologías digitales, protegiendo los derechos de los ciudadanos en el entorno digital.
Ley 2017 de 2020	Ley	2020	Establece la protección de infraestructuras críticas de información, orientada a garantizar la continuidad y seguridad de los servicios esenciales.
Resolución 2926 de 2021 (MinTIC)	Resolución	2021	Define directrices para fortalecer la ciberseguridad en entidades públicas y promueve la formación especializada en ciberseguridad en el sector estatal.

La siguiente tabla, que compara las leyes, decretos, políticas e instituciones que se aprobaron en México, España y Colombia entre 2020 y 2024, destaca las distinciones y similitudes

Tabla 4. *Comparación de políticas, normativas e instituciones en seguridad digital, ciberseguridad y gobierno digital (2020–2024)*

Categoría	Colombia	España	México
Políticas	Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020)	Estrategia Nacional de Ciberseguridad 2019–2025Estrategia Digital 2021–2025	Estrategia Nacional de Ciberseguridad 2021Política Nacional de Gobierno Digital (2022)
Leyes	Ley 1581 de 2012 (Protección de datos personales)Ley 1266 de 2008Ley 1273 de 2009	Ley Orgánica 3/2018 (Protección de Datos)Ley 11/2022 (Ley General de Telecomunicaciones)	Ley Federal de Protección de Datos Personales en Posesión de Particulares (2010)Ley de Firma Electrónica
Decretos y estrategias	Decreto 620 de 2020Decreto 767 de 2022	Real Decreto 311/2022 (Esquema Nacional de Seguridad)Real Decreto-ley 14/2019 (Ciberseguridad 5G)	Estrategia de Ciberseguridad para Infraestructura Crítica 2022
Instituciones clave	MinTIC ColCERT Superintendencia de Industria y Comercio	INCIBE (Instituto Nacional de Ciberseguridad)CCN (Centro Criptológico Nacional)Agencia Digital Española	Secretaría de Seguridad y Protección Ciudadana Policía Cibernética Coordinación de Estrategia Digital

clave en la evolución institucional y regulatoria de la seguridad digital, la ciberseguridad y el gobierno digital. De acuerdo al Normograma anterior, tanto México como España han logrado consolidar marcos institucionales y legislativos fuertes en seguridad digital y ciberseguridad, así como estrategias integrales que logren un equilibrio entre la protección de los derechos humanos y el avance tecnológico. A pesar de los avances de Colombia en el desarrollo de políticas, el CONPES 3995, el país aún enfrenta dificultades de implementación, articulación interinstitucional y modernización normativa. Esto resalta la importancia del estudio comparativo para fortalecer la gobernanza digital nacional.

Nota. Elaboración propia -documentos oficiales y estratégicos de Colombia, España y México (2020–2024).

CAPITULO III. MARCO METODOLÓGICO

3.1.Enfoque epistemológico

La perspectiva post-positivista, que reconoce que el conocimiento sobre la realidad social es contextual, aproximativo y verificable por varias evidencias empíricas, es donde se sitúa el presente estudio (Phillips & Burbules, 2000). Esta estrategia se alinea con la finalidad de la investigación de evaluar la política pública en ciberseguridad colombiana, utilizando datos sistemáticos documentados y procedimientos reproducibles para compararla con las experiencias de México y España. Con el fin de preservar la trazabilidad de los procedimientos analíticos y al mismo tiempo mantener una visión crítica sobre los límites del conocimiento derivado de fuentes documentales, el post-positivismo permite combinar técnicas cuantitativas (minería de textos, frecuencias, patrones) y cualitativas (análisis de contenido, interpretación contextual) con estándares.

3.2.Tipo de investigación

Para describir las políticas públicas de ciberseguridad y comparar sus elementos estructurales, normativos y programáticos entre Colombia, México y España, este estudio es de carácter descriptivo-comparativo. Pretende caracterizar, evaluar y contrastar los componentes clave de estas políticas más que interferir o modificar factores (Hernández Sampieri et al., 2014). El alcance del estudio es proactivo y analítico; además de señalar similitudes y contrastes, sugiere formas de mejorar la política colombiana con base en las mejores prácticas que se han visto.

3.3.Diseño de la investigación

Se utiliza un diseño mixto, transversal no experimental, con un punto de vista comparativo y documental. Entre las opciones metodológicas se encuentran las siguientes:

- Recopilación y evaluación de los datos ya existentes sin ninguna modificación directa.
- Combinación de enfoques cualitativos (análisis de contenido, categorización de temas, comparación normativa) y cuantitativos (minería de textos, frecuencias, coocurrencias, modelización de temas).
- Análisis a partir de diversas fuentes verificadas, restringido a los años 2020-2024.

Al permitir evaluar desde un punto de vista crítico y metódico la coherencia de las políticas públicas, el alineamiento institucional, los procedimientos de seguimiento y los marcos estratégicos, este diseño resulta apropiado para su estudio.

3.4.Método

Se emplea un método mixto secuencial (Creswell & Plano Clark, 2018), organizado en cuatro fases:

Figura 2.
Fases método de la investigación

Nota. Basado en (Creswell & Plano Clark, 2018)

3.5.Población y Muestra

Población: El corpus informacional se conforma por documentos técnicos y normativos referentes a ciberseguridad, transformación digital y gestión de riesgos tecnológicos que fueron

publicados por los gobiernos de México, España y Colombia entre 2020 y 2024. Se tomarán en cuenta leyes, políticas públicas, estudios técnicos, diagnósticos y otros documentos pertinentes publicados por organizaciones gubernamentales y académicas.

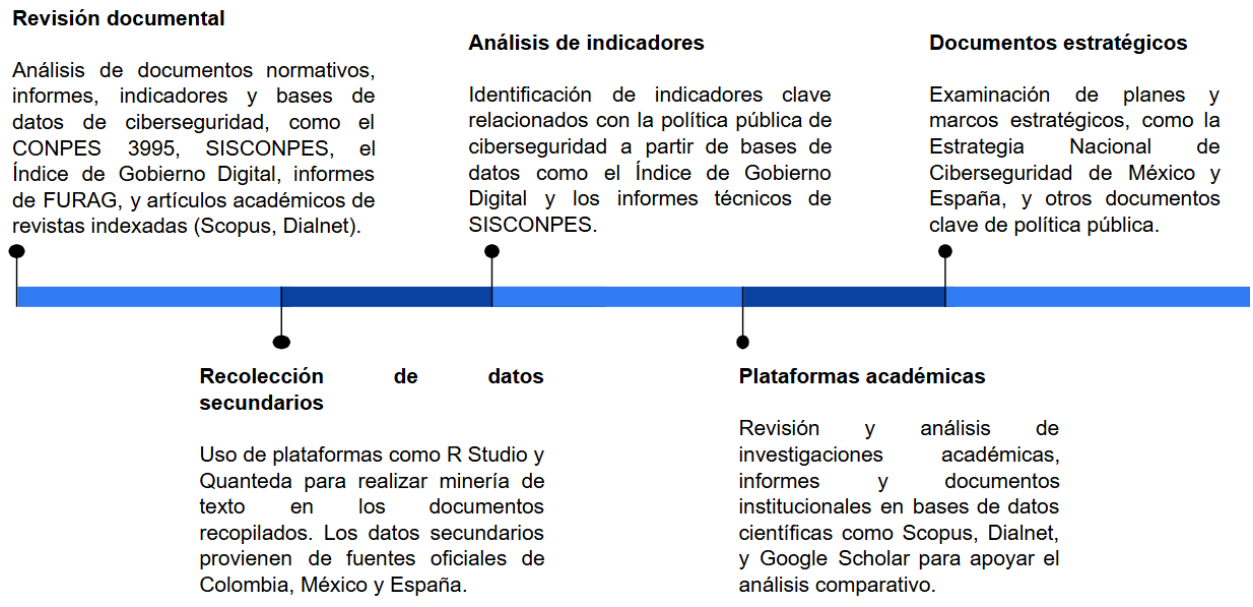
Muestra: Se seleccionarán 40 documentos de forma intencional y teórica (Patton, 2015), con el objetivo de asegurar la relevancia y representatividad de los mismos. Esta selección incluirá:

- 20 documentos de Colombia, incluyendo CONPES 3995, leyes nacionales, planes estratégicos, informes de SISCONPES, y otros documentos clave.
- 10 documentos de México, incluyendo la Política Nacional de Ciberseguridad, marcos regulatorios, y diagnósticos sobre ciberseguridad.
- 10 documentos de España, entre ellos la Estrategia Nacional de Ciberseguridad, reportes de órganos oficiales.

3.6.Técnicas e Instrumentos de Recolección de Datos

Figura 3.

Técnicas e instrumentos de recolección de datos



Nota. Las fuentes consultadas fueron seleccionadas por su relevancia institucional y académica.

3.7.Validación de Instrumentos

Para asegurar que los instrumentos sean confiables y válidos se tiene en cuenta lo siguiente:

- Se utilizarán fuentes oficiales y verificables para asegurar la precisión y relevancia de los datos.
- Se triangularán los datos de documentos de diferentes niveles (normativos, técnicos, estratégicos) para aumentar la robustez del análisis.
- Se documentará el proceso de limpieza textual (eliminación de stopwords, tokenización, lematización) y los parámetros de análisis utilizados, garantizando la transparencia y replicabilidad del proceso.

3.8.Técnicas de Análisis

Tabla 5.
Técnicas de análisis de datos

Técnica	Descripción
Minería de texto	Aplicación de técnicas de minería de texto utilizando Quanteda en R Studio para analizar grandes volúmenes de datos textuales. Se identifican patrones, términos clave y temas latentes a partir de los documentos seleccionados.
Análisis de frecuencia y co-ocurrencia	Se realiza un análisis de frecuencia de términos y co-ocurrencia para identificar las relaciones entre palabras clave en los textos analizados. Esto permite detectar temas recurrentes y áreas de énfasis dentro de las políticas de ciberseguridad.
Modelado de tópicos (Topic Modeling)	Utilización de técnicas estadísticas para agrupar contenido similar en temas o tópicos. Este análisis ayuda a identificar patrones discursivos y a determinar cómo se estructuran los temas clave en los documentos de ciberseguridad.
Análisis léxico (Dispersión léxica)	Se emplea el análisis de dispersión léxica para examinar cómo las palabras clave se distribuyen a lo largo de los documentos, visualizando la aparición de términos a través del texto y ayudando a identificar patrones de relevancia a lo largo de las políticas analizadas.
Análisis cualitativo-comparado	Se realiza un análisis comparativo entre las políticas de ciberseguridad de Colombia, México y España. Este análisis se apoya en las herramientas de minería de texto y en una evaluación cualitativa para interpretar las similitudes y diferencias en los marcos normativos y los enfoques estratégicos de los tres países.
Análisis temático	Análisis temático con enfoque deductivo-inductivo para identificar categorías relevantes relacionadas con los principios rectores de la ciberseguridad, los mecanismos de gobernanza y la alineación con estándares internacionales (OCDE, OEA, UE).
Matrices de comparación	Elaboración de matrices comparativas para contrastar los componentes estructurales, normativos y estratégicos de las políticas de ciberseguridad de Colombia, México y España. Este análisis ayuda a identificar vacíos y áreas de oportunidad en la política pública colombiana.

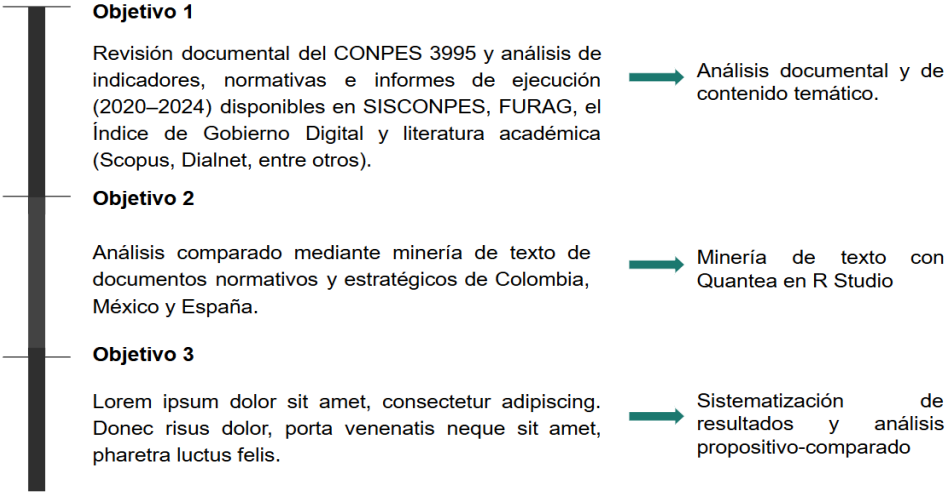
3.9.Consideraciones Éticas y Limitaciones

Ética: Todos los documentos relacionados con el estudio serán de acceso público. Se respetarán estrictamente las normas APA (7ª edición) en materia de citación responsable e integridad académica.

Limitaciones: Dado que no toda la información relacionada con la ciberseguridad está disponible o publicada, puede existir un sesgo documental. Dado que el marco temporal del estudio se limita a 2020-2024, no se evaluarán las políticas que se aplicaron antes o que aún están en proceso. El estudio no evalúa cómo se aplican realmente las políticas, sino que se centra en el análisis normativo y estratégico.

Figura 4.

Objetivos de la investigación y técnicas asociadas



Nota. Los objetivos fueron clasificados según su nivel. Las técnicas empleadas se asignaron conforme a la fase metodológica correspondiente del diseño mixto secuencia

CAPÍTULO VI. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

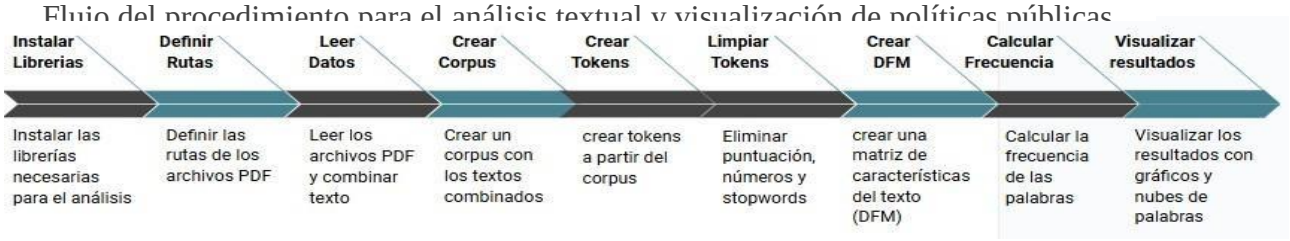
Para este estudio se utilizó el software Quanteda en R Studio para hacer análisis de textos. Este conjunto herramientas ofrece funciones y recursos para gestionar de forma eficiente y efectiva grandes cantidades de texto. Se utilizaron nubes de palabras para representar gráficamente los términos más comunes en los textos examinados, destacando su importancia dentro del corpus mediante cambios de tamaño y color. Este método facilita la búsqueda de temas y patrones importantes (Viegas & Wattenberg, 2008). La frecuencia relativa, que permite comparar la importancia de las palabras en textos de distinta extensión, sirvió de base para la visualización

(Alaminos, 2023). El procedimiento incluyó: (1) carga y consolidación de documentos PDF; (2) creación del corpus con *Quanteda* en R Studio, categorizando los textos por año o tipo; (3) procesamiento textual (tokenización, limpieza, normalización y lematización); (4) análisis de frecuencia para identificar términos dominantes; y (5) generación de nubes de palabras y gráficos de frecuencia para facilitar la comparación entre documentos.

Para encontrar patrones temáticos y evolución conceptual en los trabajos examinados, también se utilizó la técnica de dispersión léxica, que permite visualizar la distribución de términos importantes a lo largo de los textos.

Figura 5.

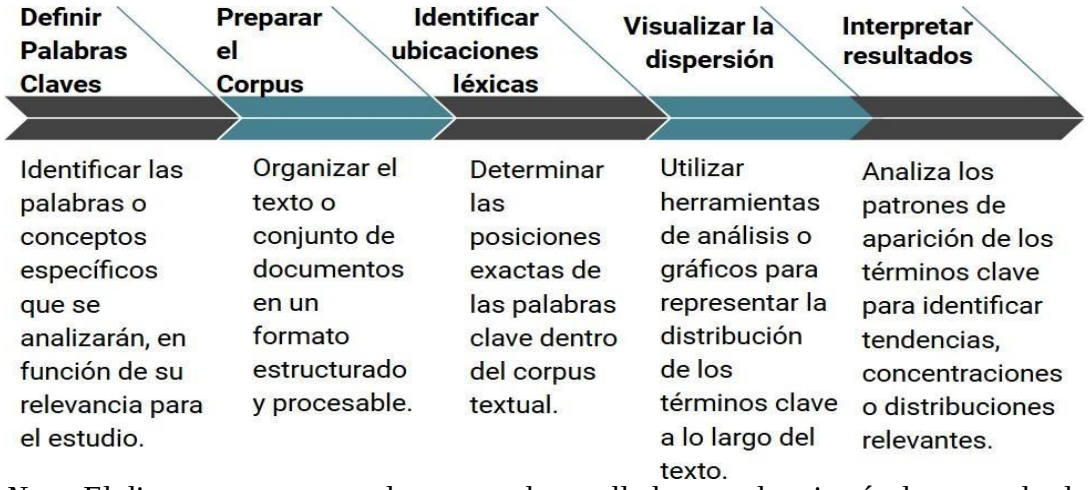
Flujo del procedimiento para el análisis textual y visualización de políticas públicas



Nota. El diagrama representa las etapas desarrolladas para la minería de texto: desde la recopilación documental hasta la visualización de nubes de palabras.

Figura 6.

Flujo del procedimiento-dispersión léxica- para el análisis textual y visualización de políticas públicas



Nota. El diagrama representa las etapas desarrolladas para la minería de texto: desde la recopilación documental hasta la visualización de la tabla de dispersión léxica.

Este estudio expone hallazgos derivados de la aplicación de la estrategia nacional contenida en el CONPES 3995 la cual aborda aspectos clave de la protección digital y la construcción de confianza institucional en Colombia en los años 2020-2024.

I. ESTRATEGIAS Y RETOS DE LA ADMINISTRACIÓN DE LA SEGURIDAD DIGITAL ESTATAL: SEGUIMIENTO AL CONPES 3995 (2020-2024)

El documento CONPES 3995 es un referente estratégico. Sin embargo, es importante examinar los impactos, vacíos y conflictos latentes de las políticas públicas además de sus contenidos formales. Partiendo de este supuesto, se exponen los hallazgos obtenidos tras evaluar cómo se ha aplicado la política de gobierno digital en Colombia. La evaluación se fundamenta en la información recopilada del Formulario Único de Reporte de Avances de la Gestión (FURAG) correspondiente a los años 2020-2023, complementado con la consolidación de los reportes elaborados por las entidades mediante el aplicativo web SisCONPES 2.0. Dichos reportes están alineados con las acciones establecidas en los Planes de Acción y Seguimiento (PAS) aprobados en las sesiones del CONPES para el periodo 2020-2024. La información obtenida se utiliza para evaluar el avance de las políticas y la ejecución de las estrategias acordadas en dichos planes, permitiendo realizar un diagnóstico detallado del estado de la política de seguridad digital en el país.

1. Análisis de los resultados sobre la medición del desempeño de la Política de Gobierno Digital 2020-2023

El análisis de los resultados del FURAG para los años 2020-2023 revela un complicado cambio desde la creación de normativas hasta el cumplimiento real de la política de ciberseguridad digital. Este proceso muestra patrones de avance, retroceso y recuperación que permiten evaluar a profundidad la madurez institucional en materia de ciberseguridad y transformación digital. Se ve impactado por varios motivos como la pandemia del COVID-19, el cambio normativo del Decreto 767 de 2022 y la adopción del nuevo Manual de Gobierno Digital.

Desempeño general

Las puntuaciones globales del Índice de Gobierno Digital muestran una curva de desarrollo característica de las políticas en fase de implementación: un fuerte descenso en 2022, una recuperación parcial en 2023 y un aumento temprano en 2020-2021. Más que una verdadera reducción de la capacidad, este comportamiento es más indicativo de un ajuste metodológico. La aplicación del manual revisado, que aumentó considerablemente los requisitos de trazabilidad y pruebas documentales, coincidió con un descenso de entre 13 y 23 puntos en todos los componentes. En consecuencia, aunque la media general disminuyó de 85,7 en 2021 a 72,2 en 2022, este descenso debe considerarse un «reinicio estadístico» que señaló el cambio de una fase de verificación declarativa a una operativa. Aunque de forma desigual, el repunte hasta 74,9 en 2023 indica que algunas empresas están empezando a adaptarse a estas nuevas normas.

Tabla 6. *Análisis comparado de indicadores de Gobierno digital (FURAG 2020-2023)*

1. Evolución del puntaje promedio anual (sobre 100)

Componente	2020	2021	2022*	2023
Seguridad y Privacidad de la Información	79.3	81.8	68.0	72.8
Arquitectura (TI y empresarial)	84.1	88.1	65.5	68.8
Servicios y Procesos Inteligentes	65.3	65.3	46.6	47.2
Decisiones basadas en Datos	74.7	77.5	62.4	68.0
Servicios Ciudadanos Digitales	77.0	78.1	15.6	15.6
Estado Abierto	73.8	76.3	86.4	**87.7**
Índice de Gobierno Digital (global)	81.4	**85.7**	72.2	74.9

Nota. El fuerte descenso 2022 coincide con la puesta en marcha del Manual de Gobierno Digital expedido con el Decreto 767 de 2022).

Diferenciación por componente

Con una media de 87,7 en 2023 y un aumento de +14 puntos con respecto a 2020, el componente de Estado abierto muestra una tendencia al alza constante. Con puntuaciones cercanas a 100, organizaciones como el DNP y la Contraloría General cuentan con un sólido marco institucional para la rendición de cuentas. Los Servicios Ciudadanos Digitales, por su parte, muestran una importante debilidad estructural. La discrepancia entre la dotación institucional y el

diseño normativo queda demostrada por el estancamiento en 15,6 puntos en 2022 y 2023. La mayoría de las empresas no logran superar la barrera tecnológica que representa la exigencia de integrar la autenticación digital, la Carpeta Ciudadana y la Pasarela de Pagos. El hecho de que Medicina Legal haya sido la única empresa que ha obtenido la mejor nota pone de manifiesto la urgencia de invertir en infraestructuras de interoperabilidad y talento digital.

Tras fuertes caídas en 2022, componentes como Arquitectura de TI (68,8) y Seguridad y Privacidad de la Información (72,8) muestran modestas recuperaciones en 2023. Estos hallazgos implican que las organizaciones están empezando a adaptar sus procedimientos a las nuevas normas, especialmente las que se encuentran en el Decreto 1263 de 2022 y el CONPES 3995 de 2020. Sin embargo, existe un problema importante de coherencia estructural, ya que algunos organismos, como la Contaduría General de la Nación y la CAR Cundinamarca, alcanzan 100 puntos, mientras que otras, como la Universidad Pedagógica y Cormagdalena, registran 0 puntos.

Tabla 7.

Componentes con mayor desempeño (2023)

Estado Abierto (87,7)
Mejores entidades: Contraloría General, Consejo de Estado y DNP (≥ 98).
Explica la consolidación de portales de datos abiertos y mecanismos de transparencia activa.
Seguridad y Privacidad (72,8)
100 ptos: Contaduría General, Consejo Superior de la Judicatura y CAR Cundinamarca.
Refleja la implementación de la *Política Nacional de Confianza y Seguridad Digital – CONPES 3995*.

Brechas regionales y sectoriales: la brecha centro-periferia persiste

La conclusión más preocupante del análisis FURAG es que sigue existiendo una brecha digital geográfica. Mientras que los hospitales rurales y las universidades, particularmente en Chocó, Amazonia y el Caribe, registran desempeños críticos, las organizaciones con sede en Bogotá (superintendencias, ministerios) concentran los puntajes más altos. La ausencia de competencias técnicas y financieras más allá del núcleo administrativo queda demostrada por la Universidad del Pacífico, que presenta numerosos ceros en áreas cruciales como Datos y Procesos

Inteligentes. Esta discrepancia cuestiona las ideas de inclusión y acceso universal a los servicios digitales desde el punto de vista de la equidad geográfica en las políticas públicas. La distribución de las competencias para la transformación digital es increíblemente desigual, lo que exige medidas correctoras específicas en materia de infraestructuras, formación y asistencia técnica específica.

Tabla 8.

Componentes con desafíos persistentes

Servicios Ciudadanos Digitales (15,6)
El estándar 2022 exige evidencia de integración con Autenticación, Carpeta y Pasarela de Pagos; la mayoría de entidades no la presenta.
Solo el Instituto de Medicina Legal (100 pts) alcanza madurez completa.
Servicios y Procesos Inteligentes (47,2)
Brecha de −18 pts respecto a 2020; destaca la Escuela Tecnológica ITC (100 pts) pero universidades regionales como Pacífico (0 pts) y Tecnológica del Chocó (0 pts) evidencian rezagos en automatización.
Arquitectura (68,8)
Caída neta de −15 pts frente a 2020; mejora leve 2023 tras la expedición del Decreto 1263 de 2022 que fija estándares de transformación digital.

Disparidades entre entidades (2023)

El análisis de las puntuaciones por entidad revela una notable disparidad en la aplicación de las políticas digitales.

Las organizaciones con mejor desempeño: La CAR de Cundinamarca, el Consejo Superior de la Judicatura y la Contraloría General de la República obtuvieron calificaciones impecables en seguridad y privacidad. Con puntuaciones de 100, organizaciones como el Ministerio de Salud, COTECMAR y la CAR Boyacá destacaron en el campo de la arquitectura.

Organizaciones que obtuvieron resultados deficientes: Por el contrario, organizaciones como la CAR Quindío, la Universidad Pedagógica y Cormagdalena recibieron puntuaciones bajas o nulas en varios componentes, lo que indica una falta de recursos o capacidad para implementar con éxito la política digital.

Tabla 9.
Disparidades entre entidades (2023)

Componente	Entidades mejor puntuadas	Entidades con menor puntaje
Seguridad y Privacidad	Contaduría G., Consejo Sup. Judicatura, CAR C/marca (100)	CAR Quindío, Universidad Pedagógica, Cormagdalena (0)
Arquitectura	CAR Boyacá, COTECMAR, MinSalud (100)	CAR Quindío (14 pts.), CDA Amazonia (14 pts.)
Procesos Inteligentes	ITC Central (100)	Fondo Nacional de Ahorro, Univ. del Pacífico (0)
Datos	RTVC, Positiva, MinEducación (100)	FPS Ferrocarriles, Senado, Univ. del Pacífico (0)
Servicios Ciudadanos	Medicina Legal (100)	Sanatorio de Contratación, Banco Agrario (0)

Nota. La tabla presenta un contraste entre entidades con alto y bajo desempeño en la implementación de componentes clave de gobierno digital y ciberseguridad en 2023.

Tendencias clave (2020-2023)

Tabla 10.
Tendencias clave 2020-2023

Efecto COVID-19 (2020-2021)
Aceleró canales digitales y elevó puntajes globales, sobre todo en seguridad y arquitectura.
Reinicio estadístico (2022)
La nueva métrica eleva el umbral de evidencia; se traducen en descensos de 13-23 pts en casi todos los dominios
Recuperación selectiva (2023)
Se observan rebotes moderados en seguridad (+4,8 pts) y datos (+5,6 pts); servicios ciudadanos se estanca.
Estado Abierto sobresale
+14 pts desde 2020, impulsado por la obligatoriedad de datos abiertos y la cultura de transparencia.
Brecha centro-periferia
Entidades nacionales con sede en Bogotá concentran los puntajes >90; universidades y hospitales regionales registran varios ceros, señal de limitaciones de capacidad.

Componente Datos

Tras descender de 77,5 en 2021 a 62,4 en 2022, el componente Decisiones basadas en datos apenas mejora en 2023 (68,0), lo que sugiere una lenta adopción de la cultura de la evidencia y la analítica institucional. Esta recuperación podría considerarse un indicio de que el mercado está preparado para adoptar nuevas tecnologías como la inteligencia artificial, cuyas directrices estratégicas se anticipan en 2025. Sin embargo, aún quedan importantes obstáculos por superar para que los datos dejen de ser una promesa y se conviertan en una aportación transversal útil para el gran público. Entre estos obstáculos se encuentran la calidad de los datos, la compatibilidad de las plataformas y los estándares de los informes.

Componente Servicios y Procesos Inteligentes

La automatización y robotización de los procesos institucionales sigue siendo una limitación estructural, como demuestra la reducción neta de 18 puntos en este componente de 2020 a 2023 (de 65,3 a 47,2). El Fondo Nacional del Ahorro y varias instituciones regionales registran cero puntos, mientras que otras organizaciones, como el ITC Central, alcanzan los 100 puntos. Así, la falta de capacidades de automatización de procesos se convierte en un problema que limita el desarrollo de un Estado inteligente, flexible y centrado en sus ciudadanos.

Lecciones y perspectivas

El análisis integral permite identificar al menos tres lecciones clave para consolidar una madurez sostenible en la política de ciberseguridad digital:

Tabla 11.

Perspectivas índices gobierno digital 2020-2024

De la norma al desempeño operativo	Política diferenciada y territorializada	Ciberseguridad como eje habilitador
El desafío ya no es la ausencia de política, sino la capacidad para evidenciar su cumplimiento real. La nueva métrica del FURAG impone un estándar que exige trazabilidad, sostenibilidad y resultados verificables.	No se puede aplicar una política uniforme en un ecosistema institucional tan desigual. Es necesario implementar enfoques multinivel y sectoriales que reconozcan las capacidades diferenciales y prioricen el cierre de brechas regionales.	La seguridad digital no puede verse como un apéndice técnico, sino como el cimiento de la confianza institucional en entornos digitales. Para 2025, Colombia debe consolidar CSIRTs sectoriales, universalizar Servicios Ciudadanos Digitales base y mantener seguimiento riguroso a entidades con bajos puntajes.

El desarrollo del FURAG entre 2020 y 2023 muestra un cambio significativo en las prioridades de la política pública colombiana en materia de ciberseguridad digital. Aunque la formulación normativa era el foco principal en fases anteriores, los últimos años han demostrado que el verdadero problema está en la aplicación eficiente y a largo plazo de las políticas y los marcos normativos.

En este sentido, más que un verdadero declive, la reciente adopción de herramientas normativas como el Decreto 767 de 2022, el Decreto 1263 de 2022 y el CONPES 3995 de 2020, que establecen requisitos más estrictos para los procesos técnicos y de documentación para la seguridad digital, ha demostrado una transición. Una evaluación más rigurosa del desempeño institucional, que produce una estimación más precisa y confiable de la madurez de las instituciones públicas, es lo que causó el declive metodológico observado en 2022 y no un declive en la capacidad del Estado (Gil-García, 2007).

El concepto de gobernanza digital, propuesto por autores como Luna-Reyes y Gil-García (2014) y Janowski (2015), es esencial para comprender esta cuestión. La gobernanza digital no se limita al desarrollo de marcos legales, sino que implica un cambio fundamental en las capacidades institucionales, horizontalizando la toma de decisiones y garantizando la ejecución efectiva de las políticas públicas. El hecho de que solo unas pocas empresas hayan alcanzado una puntuación perfecta en áreas cruciales como la seguridad y la arquitectura de TI indica una brecha significativa en las capacidades de las entidades colombianas en este sentido. El 42% de las entidades que obtienen una puntuación inferior a 60 puntos muestra una madurez claramente fragmentada, lo que sugiere que, a pesar de los avances normativos, las capacidades operativas, humanas y tecnológicas necesarias para una implementación exitosa siguen siendo deficientes (Margetts & Dunleavy, 2013; Cejudo & Michel, 2017).

Sin embargo, los retrasos encontrados en los Procesos Inteligentes y los Servicios Ciudadanos Digitales muestran que la infraestructura regulatoria es insuficiente por sí sola para garantizar una transición fluida hacia una gobernanza digital avanzada. Para analizar esta situación puede utilizarse la Teoría de la Capacidad del Estado Digital, que enfatiza que la adopción de políticas digitales depende de la presencia de capacidades humanas especializadas, infraestructura tecnológica suficiente y marcos regulatorios flexibles, en lugar de solo marcos regulatorios (Cejudo & Michel, 2017).

Las insuficiencias encontradas en estas facetas cruciales de la administración pública ponen de manifiesto que el éxito del modelo de ciberseguridad por el que ha optado la nación se ve limitado por la falta de inversión en mano de obra y tecnología, así como por el rediseño de los procedimientos administrativos. Sin embargo, la recuperación del componente de datos para 2023 muestra avances en la preparación para nuevas tecnologías en desarrollo como la analítica y la inteligencia artificial, que son esenciales para la gestión de la ciberseguridad de Colombia en el futuro (Pérez & Hernández, 2020). Sin embargo, será necesario cerrar brechas en interoperabilidad, calidad de datos y cultura de la evidencia para que la nación se beneficie de estos avances. En este contexto, la idea de ciberresiliencia, que es la capacidad de una organización para recuperarse rápidamente de los ciberataques es crucial. Las organizaciones públicas deben mejorar continuamente sus medidas de seguridad aprendiendo de los incidentes, además de defenderse de los ataques (Ramírez, 2019).

De cara a 2024-2025, los recursos planteados en la nueva estrategia nacional de inteligencia artificial y la «Caja de Transformación Institucional» del Manual de Gobierno Digital podrían ayudar a Colombia a pasar de una fase de adopción normativa a una de gobernanza digital madura. En este sentido, la Teoría de la Gobernanza Digital se ofrece una vez más como un marco analítico crucial para comprender los procedimientos que Colombia necesita mejorar para perfeccionar sus capacidades institucionales y la gestión del riesgo. Esta teoría plantea que para llegar a una madurez operativa sostenible se deben consolidar los CSIRT sectoriales, universalizar los Servicios Ciudadanos Digitales fundacionales y monitorear de manera diferente a las organizaciones con puntajes críticos (Gil-García, 2007).

Por último, asegurar evidencias operativas verificables y duraderas en todos los niveles del Estado colombiano es la dificultad actual de la política de ciberseguridad, al no contar con un estándar. De acuerdo con Luna-Reyes y Gil-García (2014), este reto hace parte de una evolución que exige tanto el cambio estructural como la adhesión a marcos normativos para que las entidades públicas cuenten con la capacidad operativa necesaria para responder a las exigencias de la seguridad digital en el siglo XXI.

1. **Análisis de las acciones concertadas con las entidades en los Planes de Acción y Seguimiento (PAS) aprobados en sesión CONPES (SisCONPES)**

A continuación, se presenta un desglose completo de los avances, desafíos y tendencias del sector TIC en cada corte semestral, desde 2020 hasta 2024:

Tabla 12.
Evolución de las acciones concertadas en los Planes de Acción y Seguimiento (PAS) aprobados en sesión CONPES (2020-2021)

Corte 2020-1	**Avance anual:** 81.7% (Puesto 15/28 sectores). **Acciones:** 159 totales | 67 habilitadas | 75 finalizadas | 17 no iniciadas. **Desempeño destacado:** Inteligencia y Org. Electoral con 100% de avance. TIC mostró debilidad en acciones "Al día" (49.3%). Retos: Alta proporción de acciones no iniciadas (17) y sin reporte (9%).	**Corte 2020-2**	**Avance anual:** 92.7% (Puesto 7/29 sectores). **Acciones:** 161 totales | 73 habilitadas | 79 finalizadas | 9 no iniciadas. **Mejoras:** Reducción de acciones no iniciadas (de 17 a 9). Mayor eficiencia en cierre de proyectos (75 → 79 finalizadas). Debilidades: Persistencia de acciones en alerta (ej. Educación: 68.2%).	**Corte 2021-1**	**Avance anual:** 83.8% (Puesto 9/30 sectores). **Acciones:** 173 totales | 76 habilitadas | 92 finalizadas | 5 no iniciadas. **Tendencias:** Aumento del 23% en acciones totales vs. 2020-2. MinTIC lideró el 55% de acciones "Al día". **Problemas:** Ambiente y Ciencia con avances <70%. Primeras señales de sobrecarga operativa.	**Corte 2021-2**	**Avance anual:** 95.7% (Puesto 2/30 sectores). **Acciones:** 182 totales | 80 habilitadas | 95 finalizadas | 7 no iniciadas. **Logros:** Máximo histórico en avance anual (95.7%). 74% de acciones del TIC "Al día". **Factores clave:** Mayor coordinación con sectores como Trabajo (96.3%) y Cultura (92.7%).
Corte 2022-1	**Avance anual:** 78.9% (Puesto 5/30 sectores). **Acciones:** 199 totales | 83 habilitadas | 112 finalizadas | 4 no iniciadas. **Cambios críticos:** Caída del 17% en avance vs. 2021-2 por retrasos en proyectos de infraestructura. Territorial (31.7%) y Org. control (52.2%) como cuellos de botella.	**Corte 2022-2**	**Avance anual:** 84.1% (Puesto 7/30 sectores). **Acciones:** 205 totales | 81 habilitadas | 118 finalizadas | 6 no iniciadas. **Recuperación parcial:** TIC mejoró su posición (de 14° a 7°). Salud y Educación mostraron avances >75%. **Advertencias:** Sin aprobación aumentó al 10% por trámites burocráticos.	**Corte 2023-1**	**Avance anual:** 77.3% (Puesto 14/30 sectores). **Acciones:** 206 totales | 63 habilitadas | 140 finalizadas | 3 no iniciadas. **Crisis operativa:** Solo 37% de acciones "Al día" (mínimo histórico). Ciencia y Org. control con avances <50%. **Causas:** Recortes presupuestarios y falta de personal especializado.	**Corte 2023-2**	**Avance anual:** 87.8% (Puesto 6/30 sectores). **Acciones:** 206 totales | 62 habilitadas | 142 finalizadas | 2 no iniciadas. **Recuperación estratégica:** MinTIC priorizó proyectos de ciberseguridad y conectividad rural. Igualdad y Equidad emergió como nuevo sector con 81.1% de avance.
Corte 2024-1		**Avance anual:** 80.9% (Puesto 11/30 sectores). **Acciones:** 210 totales | 59 habilitadas | 149 finalizadas | 2 no iniciadas.	**Tendencias finales:** Estancamiento en eficiencia, Solo 44% de acciones "Al día". Verdad y justicia (39.5%) y Territorial (33.0%) siguen rezagados				

Nota: Elaboración propia con base en los informes del Sistema de Seguimiento CONPES 2020-2024 (SisCONPES).

De acuerdo a lo anterior, se muestran notables avances en la capacidad del ecosistema digital del Estado colombiano para cerrar proyectos. En este sentido, se evidencia la necesidad de aumentar la eficacia y la cooperación institucional y medidas estratégicas que aborden algunas cuestiones estructurales. La optimización del uso de los recursos públicos es una de las principales preocupaciones, y esto se logra reservando fondos especiales para proyectos importantes como el despliegue de la infraestructura 5G, cuya ejecución requiere una planificación intersectorial a largo plazo.

Las inconsistencias en la gobernanza digital colombiana se evidencian en el avance anual de la industria TIC, que fluctúa entre 77,3% en el primer semestre de 2023 y 95,7% en el segundo semestre de 2021. Estas variaciones reflejan deficiencias estructurales en la implementación de políticas, pese a marcos como el CONPES 3995. Janowski (2015, p. 45) advierte que la gobernanza digital exige no solo diseño normativo, sino capacidad operativa para coordinar actores y recursos, un desafío persistente en Colombia. Dicha variación implica que el Estado colombiano aún enfrenta grandes dificultades operativas a pesar de las iniciativas legislativas y el marco institucional vigente. De hecho, los recortes presupuestarios y la falta de personal especializado, factores que Margetts y Dunleavy (2013, p. 112) vinculan a la desconexión entre prioridades estratégicas y asignación de recursos, son los principales responsables de la caída de 2023-1, lo que pone de manifiesto las escasas capacidades del Estado en el ámbito digital.

Además de lo anterior, la creciente discrepancia entre las tareas asignadas y la capacidad operativa real se refleja en la disminución del número de acciones permitidas para informar, que pasó de 67 en 2020-1 a 59 en 2024-1. Este fenómeno contradice las nociones de adaptación normativa y desarrollo de competencias técnicas, que deberían ser cruciales para mejorar la administración pública y la gobernanza, afirman Cejudo y Michel (2017, p. 89). Es evidente la falta de un plan preventivo de gestión de riesgos en la industria de las TIC, como demuestra la evolución incoherente del número de actividades finalizadas, que pasó de 75 en 2020-1 a 149 en 2024-1. Con un retraso del 32,5% en 2024-1, sectores como el Territorial, en particular, siguen mostrando un retraso notable. Esto demuestra una propensión a la gestión reactiva en lugar de proactiva, que según Hood et al. (2001, p. 23) debería ser el principal énfasis de la gestión pública de riesgos.

En este sentido, el CONPES 3995, pese a ser un documento importante, no incorpora plenamente las amenazas digitales, dando prioridad a las métricas de cumplimiento por encima de la defensa frente a posibles ataques. Un elemento importante que obstaculiza la capacidad de la nación para prever los peligros y disminuir así sus efectos adversos es la ausencia de un enfoque proactivo. La confianza institucional es un factor clave que influye en la capacidad del Estado para funcionar eficazmente. El descenso al 37% de los porcentajes de «Al día» en 2023-1 indica una grave crisis de confianza, sobre todo a la luz de la percepción pública de que la eficacia y la transparencia de las instituciones están amenazadas. Zamorín y González (2018, p. 15) subrayan que la legitimidad gubernamental depende de transparencia y eficacia, mientras que Berríos y Gómez (2017, p. 102) atribuyen parte del declive a vulnerabilidades en protección de datos personales, un factor crítico en la era digital.

Esta carencia es evidente en el pobre desempeño de Colombia en áreas importantes como ciencia (50% en 2024-1) y medio ambiente (66,5% en 2023-1) y plantea interrogantes sobre la capacidad del gobierno para manejar adecuadamente los datos y salvaguardar la información. Las acciones de «No aprobación» (10% en 2022-2), que son el resultado de procesos manuales que no se han digitalizado lo suficiente, demuestran cómo esta situación empeora por la ausencia de estrategias sólidas de confianza cero, que incluyan medidas como la segmentación de la red y la autenticación multifactor (Cabrera y Mendoza, 2021, p. 12).

Las pruebas actuales también cuestionan el concepto de ciberresiliencia, que sugiere la capacidad de recuperarse rápidamente de los eventos digitales (Ramírez, 2019, p. 88). Una parte significativa del 28% de las acciones TIC que estaban «atrasadas» en 2023-1 estaban relacionadas con iniciativas de infraestructura digital que aún no habían cumplido los requisitos exigidos. Aunque se priorizan los firewalls (Castro, 2017, p. 78), no se están implementando otras medidas básicas como la segmentación de la red o la autenticación multifactor, necesarias para garantizar una arquitectura de confianza cero (Garza & Silva, 2020, p. 34). Este rezago es indicativo de una inadecuada estructura de defensa en profundidad (Sánchez & Moreno, 2018, p. 56). Estas fallas sistémicas demuestran que las defensas de ciberseguridad de la nación contra amenazas sofisticadas aún son deficientes, lo que tiene un impacto directo en su resiliencia digital.

Por último, es importante resaltar que la ciberseguridad colombiana enfrenta un problema debido a su falta de coherencia con las normas mundiales. Colombia aún presenta deficiencias en la coordinación interinstitucional, con sectores como el Organismo de Control con una mejora de

tan solo 46,1% en 2024-1, a pesar de que la Unión Europea ha incrementado la cooperación transfronteriza para salvaguardar infraestructuras vitales (Comisión Europea, 2019, p. 9). López y Martínez (2016, p. 67) señalan que la capacidad de la nación para salvaguardar adecuadamente sus infraestructuras digitales se ve obstaculizada por esta falta de coordinación. Además, la ausencia de aplicación de marcos como el NIST (2022) demuestra un distanciamiento de las mejores prácticas mundiales, lo que indica que la voluntad política es más importante para el avance de la tecnología de la información que la capacidad técnica nacional.

En conclusión, Colombia enfrenta una paradoja de modernización: avances cuantitativos en proyectos TIC (de 75 a 149 acciones completadas, 2020-2024) coexisten con brechas cualitativas en gobernanza. La ausencia de una estrategia integral que integre recursos intangibles (confianza, coordinación, adaptabilidad) con desarrollos tecnológicos explica la volatilidad en métricas. Como propone Janowski (2015, p. 51), superar esto requiere no solo fondos para 5G, sino institucionalizar procesos de aprendizaje organizacional que prioricen la ciberresiliencia y la construcción de capital social digital.

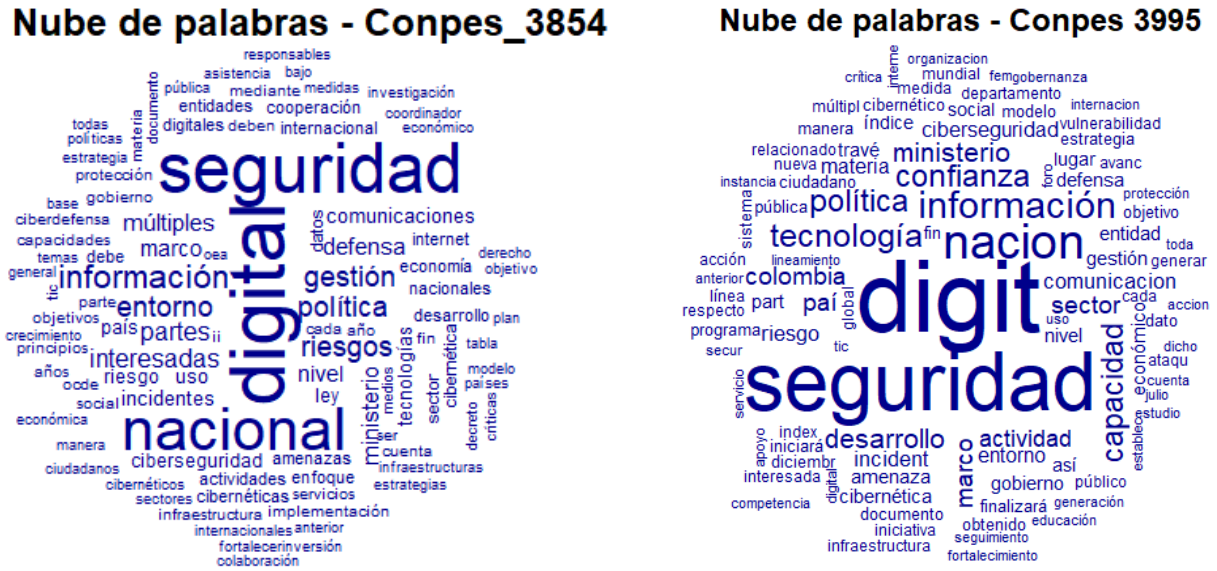
2. Análisis Nubes de Palabras y Frecuencias Políticas de confianza y seguridad digital en Colombia

Antes de analizar el diseño e implementación de la política pública de seguridad digital en Colombia, resulta pertinente identificar cómo ha evolucionado el discurso institucional frente al fenómeno del cibercrimen en los últimos años. Para ello, se toman como referencia los informes anuales emitidos por el Centro Cibernético Policial (CECIP), los cuales permiten observar qué conceptos han sido priorizados, visibilizados u omitidos en la narrativa oficial. Los términos que aparecen con más frecuencia en los informes de 2021, 2022 y 2023 se hallan utilizando tecnologías de minería de textos, en particular nubes de palabras. Esto permite inferir patrones de enfoque gubernamental y predecir conflictos entre la acción pública y el discurso. A partir de este análisis se evaluará la coherencia, énfasis y omisiones de la política nacional en materia de confianza y seguridad digital.

La nube de palabras 2021 se estructura en torno a palabras como “seguridad”, “información”, “empresa”, “acceso” y “usuario”, lo que denota un enfoque tecnocrático centrado en la protección de activos informáticos y redes privadas. Esta terminología institucional

demuestra una visión limitada de la ciberseguridad como una cuestión tecnológica, coherente con lo que Schneier (2010) denomina «seguridad basada en el control», que presupone que la pérdida de control sobre los sistemas es la preocupación. A pesar de ser esencial, esta visión omite aspectos importantes como el desarrollo de la confianza institucional, el derecho a la privacidad y la participación ciudadana en entornos digitales.

Figura 7.
Nubes de palabras Políticas de seguridad digital



El debate se desplaza hacia 2022; palabras como “virtual”, “interpol”, “captura”, “fiscalía” y “violencia sexual” ganan presencia. Este cambio expone una judicialización de la narrativa: la ciberdelincuencia es ahora un delito con rostro criminal y una víctima específica, en lugar de una mera amenaza sistémica. Esta metodología adopta un enfoque punitivo, reactivo y fragmentado de la ciberseguridad. Este tipo de enfoque institucional, como advierten Díaz y Sánchez (2019), reacciona menos a un plan estructural y más a demandas de legitimidad y control político. Así, fortalece una gobernanza digital centrada en el castigo, que obstaculiza el crecimiento de las capacidades preventivas y socava el enfoque de derechos. La historia se reordena una vez más en 2023, ya que aparecen palabras como “captura”, “resultado”, “red”, “estratégico”, “visita virtual” y “prevención” coexisten con una presencia fuerte de “ciberseguridad”. Esta simultaneidad refleja una doble narrativa: por un lado, el énfasis en «policía», «TI» y «delincuencia» refuerza la naturaleza policial y operativa del discurso; por otro, surge un propósito institucional de demostrar una reacción bien articulada y estratégica. Pero como señala Gómez (2020), las medidas

operativas o los resultados medibles por sí solos no pueden establecer la confianza digital. La legitimidad, la apertura y la corresponsabilidad institucional, todas ellas mencionadas de pasada en el vocabulario institucional estudiado, son necesarias para la confianza.

En la narrativa institucional para el año 2024 se observa un aumento sustancial de la complejidad y tecnificación del fenómeno delictivo. Los documentos, a diferencia de años anteriores, se centran en nuevas modalidades como el uso de la IA para esquemas transnacionales de «delincuencia como servicio», el fraude de criptoactivos y la usurpación de identidad (deepfake y deepvoice). Tanto la nube de palabras como la redacción del informe demuestran esta sofisticación delictiva, que pone a prueba la capacidad de respuesta del Estado, sobre todo en términos de anticipación a los avances tecnológicos y ajuste de la normativa. Los ataques basados en IA y blockchain requieren un cambio de un enfoque basado en la contención a uno de resiliencia cibernética proactiva, como advierte Ramírez (2019). Una gobernanza digital que antepone los resultados a corto plazo a los procedimientos institucionales a largo plazo se ve reforzada por la concentración operativa del documento en capturas, incautaciones y denuncias.

Como sugieren Criado (2021) y Díaz Acevedo & Cremades Guisado (2024), esta contradicción entre la complejidad de la actividad delictiva y la respuesta institucional reactiva pone de manifiesto la necesidad de políticas públicas que incorporen capacidades técnicas, inteligencia preventiva y una visión sistémica del riesgo digital. De este modo, el balance de 2024 muestra la evolución de los fenómenos, así como los límites actuales del modelo de gestión pública en materia de confianza y seguridad digital. Por otra parte, los documentos CONPES 3854 de 2016 y 3995 de 2020 ofrecen una ventana a la evolución del enfoque de la política pública colombiana en materia de seguridad digital y confianza. Mediante el análisis de nubes de palabras y frecuencias se pueden encontrar los énfasis conceptuales de cada documento, así como los cambios en el lenguaje institucional que significan el paso de una visión técnica y reactiva a un modelo más estratégico, preventivo y orientado a la gobernanza digital. Gracias a esta comparación se puede trazar una línea de continuidad y cambio en la comprensión y gestión de los riesgos asociados al entorno digital por parte del Estado colombiano en los últimos años.

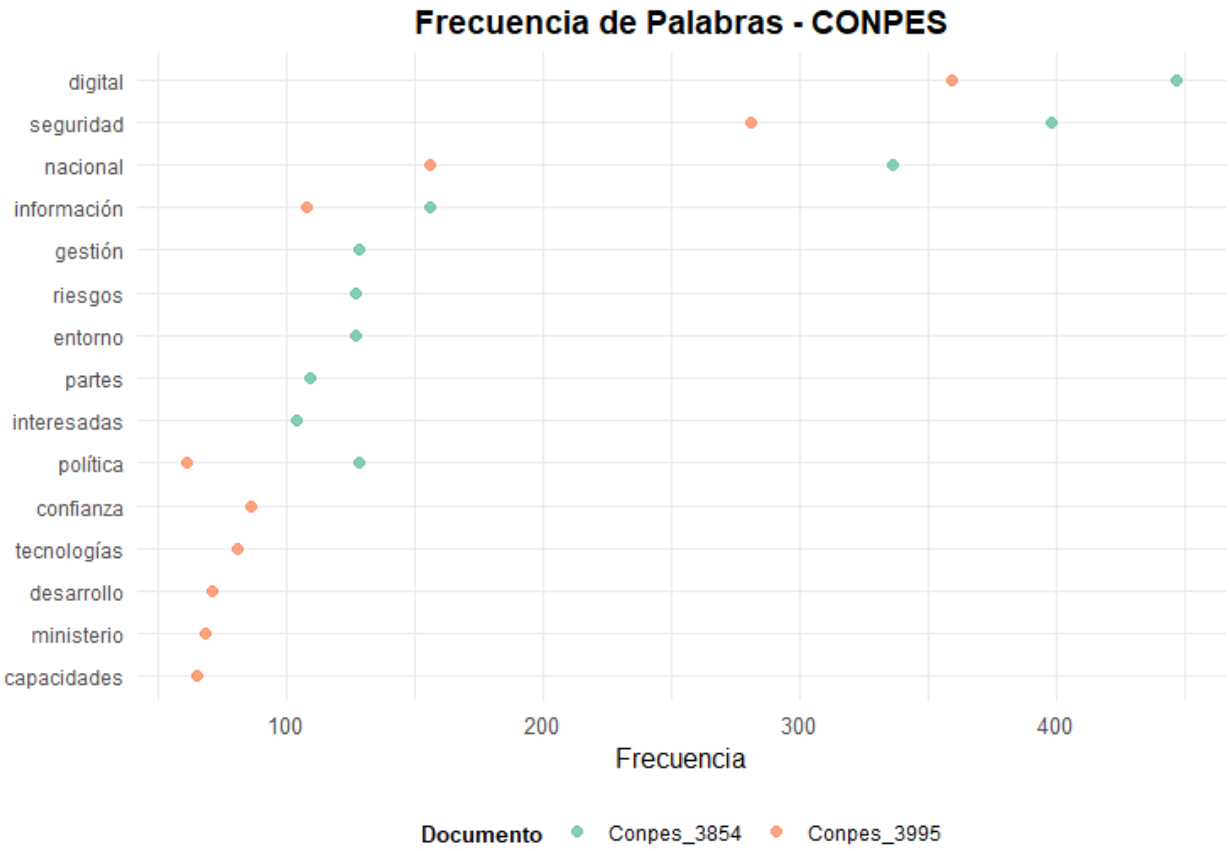
En el CONPES 3854 predominan términos como *"amenazas"*, *"incidentes"*, *"infraestructura"* y *"riesgos"*, lo que indica una aproximación más técnica y reactiva. Este

documento refleja una etapa inicial en la agenda digital del país, donde la preocupación principal era consolidar capacidades básicas frente a un entorno crecientemente hostil. La presencia de palabras como *"colaboración"*, *"entidades internacionales"* y *"marco legal"* introduce, sin embargo, una semilla de lo que posteriormente sería una apuesta por la cooperación multinivel y la estandarización, en sintonía con marcos internacionales como ISO/IEC 27001 o la OECD (2015).

En contraste, el CONPES 3995 revela una transformación discursiva más estratégica. Términos como *"gobernanza mundial"*, *"política pública"*, *"modelo"* o *"competencia"* sugieren un cambio de escala y profundidad: la seguridad digital ya no se concibe únicamente como una respuesta ante amenazas, sino como un componente estructural de la administración pública, directamente ligado a la confianza institucional. La aparición de expresiones como *"índice de ciberseguridad"* y *"nueva materia"* refuerza esta mirada adaptativa y proactiva frente a amenazas emergentes, como el ransomware, y plantea un Estado que busca posicionarse frente a estándares internacionales (ISO/IEC 27002) y métricas de desempeño.

La comparación de los dos CONPES revela un cambio en el lenguaje institucional, indicando que la seguridad digital en Colombia es ahora un asunto de gobernabilidad y legitimidad pública más que sólo tecnológico. Términos como transparencia, confianza y cooperación sobresalen en el CONPES 3995, indicando un cambio hacia lo social, lo estratégico y lo internacional, mientras que el CONPES 3854 se refiere principalmente a infraestructuras, sucesos y marcos legales.

Tabla 13.
Tabla de frecuencias de Políticas de seguridad digital



Hay una razón para esta progresión. Reacciona a una maduración de la estrategia estatal, que pasa de la formulación diagnóstica y normativa al uso de sistemas cada vez más intrincados de evaluación y coordinación. Dicho de otro modo, pasa de definir el qué y el cómo a plantear cuestiones sobre quién participa, cómo se describe a los actores y qué métricas se aplican para medir los avances. Este cambio significa un cambio político además de una continuidad tecnológica. Además, la mayor atención prestada a la confianza indica que el Gobierno ha empezado a darse cuenta de que las relaciones con los ciudadanos son tan importantes para la protección digital como los protocolos. Cuando se habla de datos protegidos, transparencia o derechos digitales, es necesario reconocer que la sensación de seguridad y la legitimidad de las instituciones actúan como mediadores en la adopción de nuevas tecnologías. De este modo, las políticas públicas crean propósitos además de prevenir peligros.

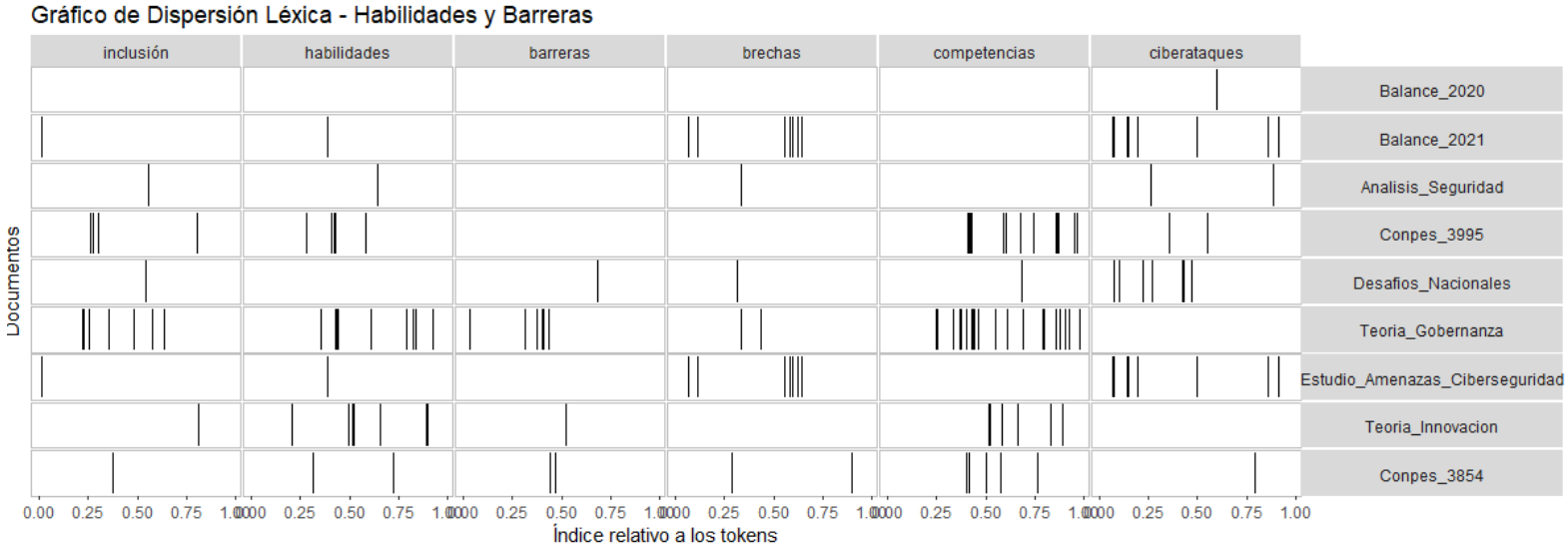
De acuerdo al siguiente diagrama de dispersión léxica de las habilidades y barreras identificadas en el análisis, revela una dinámica compleja en la interacción de conceptos

fundamentales como "habilidades", "competencias", "barreras", "brechas", "inclusión" y "ciberataques" en documentos clave. El abanico de competencias encontrado en documentos como el CONPES 3995 y Desafíos Nacionales demuestra un interés normativo por mejorar las capacidades estratégicas para afrontar eficazmente los riesgos y amenazas, así como una preocupación general por mejorar las competencias técnicas y profesionales en el entorno digital. Pero, "obstáculos' y “dificultades", frases de uso común en estudios como el de Amenazas a la Ciberseguridad ponen de relieve problemas sistémicos y disparidades persistentes en el acceso a recursos, conocimientos técnicos y políticas inclusivas que dificultan la inclusión justa de las personas en la adopción de la tecnología digital.

Además, la importancia de los «ciberataques» en publicaciones como Security and Cybersecurity Analysis Colombia llama la atención sobre un problema operativo acuciante que pone a prueba las capacidades de las instituciones y expone la insuficiencia de las medidas establecidas para hacer frente a una amenaza en constante evolución. Este análisis sugiere una desconexión entre la identificación normativa de competencias ideales y las barreras estructurales y sociales que limitan su implementación efectiva. En este sentido, la construcción de capacidades debe ir acompañada de un enfoque integral que contemple no solo el desarrollo de habilidades técnicas, sino también la reducción de brechas a través de políticas públicas inclusivas y adaptativas, que permitan una respuesta efectiva y sostenible ante los desafíos de la seguridad digital en un contexto de creciente vulnerabilidad cibernética.

Figura 8.

Gráfico de dispersión léxica-Habilidades y barreras en las políticas de confianza y seguridad digital en Colombia



En este sentido, de acuerdo al Tictac, (2021). "*El gobierno es un actor activo al tener como mandato constitucional la protección de la vida, la integridad de las personas y la protección de la privacidad*" Por esto, se han definido algunas estrategias nacionales digitales de Colombia, 2023- 2026 (Mintic, 2023), donde se proponen la eliminación de barreras por parte de las entidades territoriales en áreas de la tecnología, así como robustecer las condiciones institucionales para impulsar la innovación pública y remover barreras para la innovación, sin embargo, las amenazas a la seguridad nacional y los retos a enfrentar en el ciberespacio, avanzan más rápido que la capacidad de acción de los gobiernos. Es así como, la resiliencia, es decir, la capacidad de una organización para adaptarse en este contexto es fundamental, ya que le permite anticipar y hacer frente a situaciones difíciles como crisis y cambios inesperados. En el ámbito de la ciberseguridad empresarial, es esencial salvaguardar los activos digitales y gestionar con éxito incidentes de seguridad como ciberataques o violaciones de datos. Pero, para mejorar la resiliencia y las capacidades preventivas, es crucial establecer asociaciones estratégicas entre organizaciones públicas y comerciales que fomenten el progreso del conocimiento.

II. POLÍTICAS DE SEGURIDAD DIGITAL EN COLOMBIA, MÉXICO Y ESPAÑA: UN ANÁLISIS COMPARATIVO

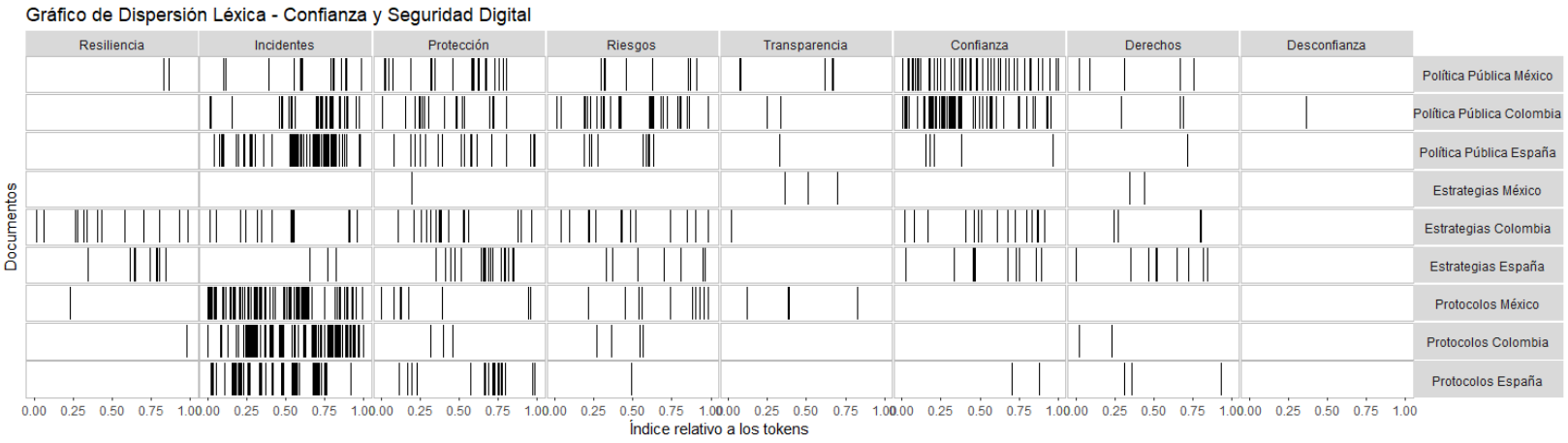
1. Seguridad y confianza digital

Las políticas públicas relativas a la seguridad digital no sólo abordan los peligros tecnológicos, sino que también establecen el marco para fomentar la confianza de los ciudadanos en los entornos digitales en un contexto global caracterizado por una creciente interdependencia digital. Como plantea Schneier (2010), las decisiones sobre seguridad están influenciadas por modelos culturales y científicos que cambian con el tiempo, por lo que la percepción de confianza digital también puede ser moldeada por la información y las experiencias de los usuarios. Este apartado compara los discursos institucionales de Colombia, México y España a partir del análisis léxico de documentos normativos, estratégicos y técnicos, con el fin de identificar prioridades semánticas, vacíos discursivos y patrones narrativos en torno a la seguridad y la confianza digital.

El siguiente gráfico permite identificar patrones clave en la distribución de términos relacionados con confianza y seguridad digital en los documentos analizados. Estos documentos se clasifican en tres categorías —políticas públicas, estrategias y protocolos— correspondientes a México, Colombia y España.

Figura 9.

Dispersión léxica de conceptos clave en políticas de seguridad y confianza digital (Colombia, México y España)



Nota. Elaboración propia mediante minería de texto con R studio de los documentos Estrategia Digital Nacional México (2021-2024), Estrategia Nacional Digital Colombia (2023-2024), Estrategia Nacional de Ciberseguridad España (2019). Políticas de ciberseguridad en México (2023), Política Nacional de Confianza y Seguridad Digita Colombia, CONPES 3995 (2020), Ley 12/2018, de Seguridad de las redes y sistemas de información España (2018).

El gráfico de dispersión léxica revela una estructura semántica marcada por la alta frecuencia del término “confianza” en los tres países analizados, con una distribución especialmente densa y homogénea en los textos estratégicos de Colombia y México. Esta reiteración sugiere que la confianza se posiciona como eje discursivo central, vinculado con la legitimidad institucional y la credibilidad de las autoridades digitales. Sin embargo, llama la atención que esta visibilidad no se acompañe de una presencia significativa de conceptos como “transparencia” o “derechos”, lo cual indica una narrativa más orientada al control que a la apertura o la garantía de derechos digitales.

El análisis del gráfico de dispersión léxica permite evidenciar cómo las políticas públicas, estrategias y protocolos sobre seguridad digital en Colombia, México y España articulan, de forma desigual, las nociones de confianza, riesgo, protección y transparencia. Estos conceptos no solo

reflejan la orientación técnica o legal de las políticas, sino que revelan los marcos cognitivos desde los cuales cada país concibe la construcción de seguridad digital como bien público.

Uno de los hallazgos más visibles es la centralidad del término "confianza", el cual aparece con alta frecuencia y dispersión en todos los países, pero con especial densidad en los textos colombianos. Esto sugiere que en el discurso institucional de Colombia existe una intención explícita por legitimar la acción pública en ciberseguridad a través del fortalecimiento de la confianza ciudadana. Sin embargo, esta reiteración no necesariamente indica profundidad conceptual o consistencia normativa: la confianza es tratada más como objetivo deseable que como resultado de procesos tangibles como la rendición de cuentas, la participación o la protección efectiva de derechos digitales.

El contraste con términos ausentes o marginales como "desconfianza" o "transparencia" refuerza esta hipótesis. La escasa aparición de estas palabras, especialmente en Colombia y México, sugiere un tratamiento retórico de la confianza, sin reconocimiento explícito de los factores que la deterioran. Esta es una ausencia crucial en el ciclo de formulación y evaluación desde la perspectiva de la teoría de las políticas públicas, ya que dificulta el desarrollo de mecanismos de retroalimentación institucional que revelen brechas y fomenten el aprendizaje (Miller & Whicker, 1999). La confianza digital, según Schneier (2010), es una variable que se ve impactada por las percepciones de seguridad de los usuarios, las cuales se ven influenciadas por la destreza tecnológica del Estado, así como por su apertura, coherencia y transparencia. El corpus colombiano apenas contiene la frase «resiliencia», y sólo aparece esporádicamente en México y España. Dada la oleada de amenazas digitales, esta baja frecuencia es preocupante porque un componente clave de cualquier estrategia contemporánea de ciberseguridad es la resiliencia institucional, que se define como la capacidad de prever, frustrar, adaptarse y recuperarse de los desastres cibernéticos. La ausencia discursiva del concepto puede indicar que la política pública colombiana en esta materia sigue anclada en modelos reactivos o de solo defensa, sin incorporar marcos adaptativos o de gestión de la incertidumbre que son esenciales para el paradigma de la administración pública 4.0 (Criado, 2021).

España tiene una narrativa más sólida en torno a los «riesgos», con apariciones esporádicas pero constantes en los textos, según la investigación comparativa. Esto demuestra una estrategia más exhaustiva y proactiva que considera la seguridad digital como un componente de una arquitectura institucional de gestión de riesgos, así como una reacción a los sucesos. Esta tendencia

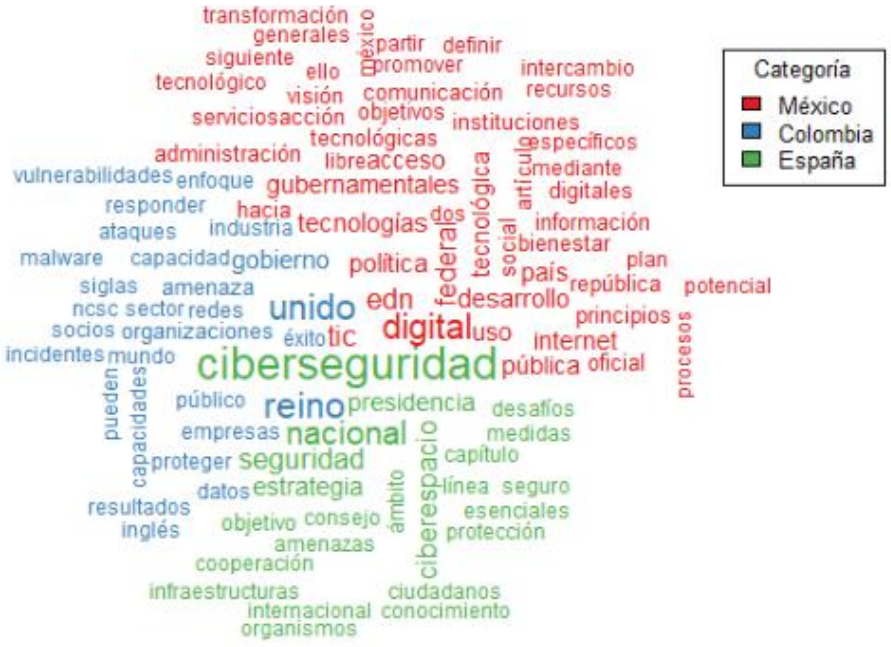
es compartida en cierta medida por México, pero la palabra es menos común en Colombia debido a la falta de sistematización en el diagnóstico de amenazas, lo que restringe la capacidad de crear intervenciones basadas en la evidencia y evaluadas prospectivamente.

Sin embargo, la falta de un enfoque de derechos digitales y de gobierno abierto en la formulación y evaluación de las políticas públicas de seguridad se evidencia en el bajísimo uso de términos como «derechos» y «participación» en las tres naciones, pero particularmente en Colombia. Para legitimar la actividad pública en el ámbito digital es necesario incorporar la transparencia, la co-creación y la corresponsabilidad ciudadana en un enfoque transversal, según las propuestas actuales de gobierno abierto (Criado, 2021). Según este punto de vista, la confianza es un resultado acumulativo de conexiones institucionales democráticas y abiertas, más que un insumo que hay que salvaguardar. Por último, la ausencia de palabras como «evaluación» o «aprendizaje» en los documentos examinados apunta a un fallo en la forma en que las normas de seguridad digital institucionalizan los procedimientos de supervisión y retroalimentación. Cuando la complejidad de las amenazas cambia rápidamente, la falta de estos mecanismos pone en peligro la legitimidad y la eficacia de las políticas públicas al dificultar su adaptación a circunstancias y demandas cambiantes.

Por lo tanto, a pesar de que Colombia ha incorporado sustancialmente el lenguaje de la confianza digital, el análisis semántico comparativo muestra que su narrativa institucional tiene notables lagunas en términos de transparencia, resiliencia y enfoque basado en derechos. Estas disparidades contrastan con los avances logrados en México y España, donde la semántica institucional está más en línea con los marcos modernos de gobernanza digital abierta y flexible. Este hallazgo subraya la necesidad urgente de alinear el discurso normativo colombiano con principios de administración pública innovadora y con un enfoque genuinamente democrático de la seguridad digital.

En el caso de la nube de palabras y la tabla de frecuencia, permiten observar con claridad los énfasis léxicos predominantes en los marcos estratégicos de seguridad digital en Colombia, México y España. Aunque en los tres países el término “ciberseguridad” ocupa un lugar central, la composición discursiva restante revela diferencias significativas en el modelo de gobernanza digital adoptado por cada uno.

Figura 10.
Nube de palabras: estrategias de seguridad digital en Colombia



Nota. Visualización de los términos más frecuentes en la estrategia nacional de seguridad digital de Colombia. Elaboración propia con base en documentos institucionales (2020–2024).

Colombia presenta una concentración semántica alrededor de términos como “sistema”, “nacional”, “infraestructura”, “ciberespacio” y “entidades”, lo que denota una estrategia centrada en la institucionalidad estatal y en el resguardo del aparato público ante amenazas externas. Este patrón discursivo es consistente con políticas que priorizan la estabilidad institucional por encima de la apertura o la transparencia. Sin embargo, su densidad no garantiza sostenibilidad política en el tiempo. Como advierten Patashnik y Zelizer (2009), las políticas mal diseñadas o carentes de soportes institucionales robustos pueden generar retroalimentaciones débiles, incapaces de reformar las dinámicas de gobernanza de forma duradera. En el caso colombiano, la ausencia de

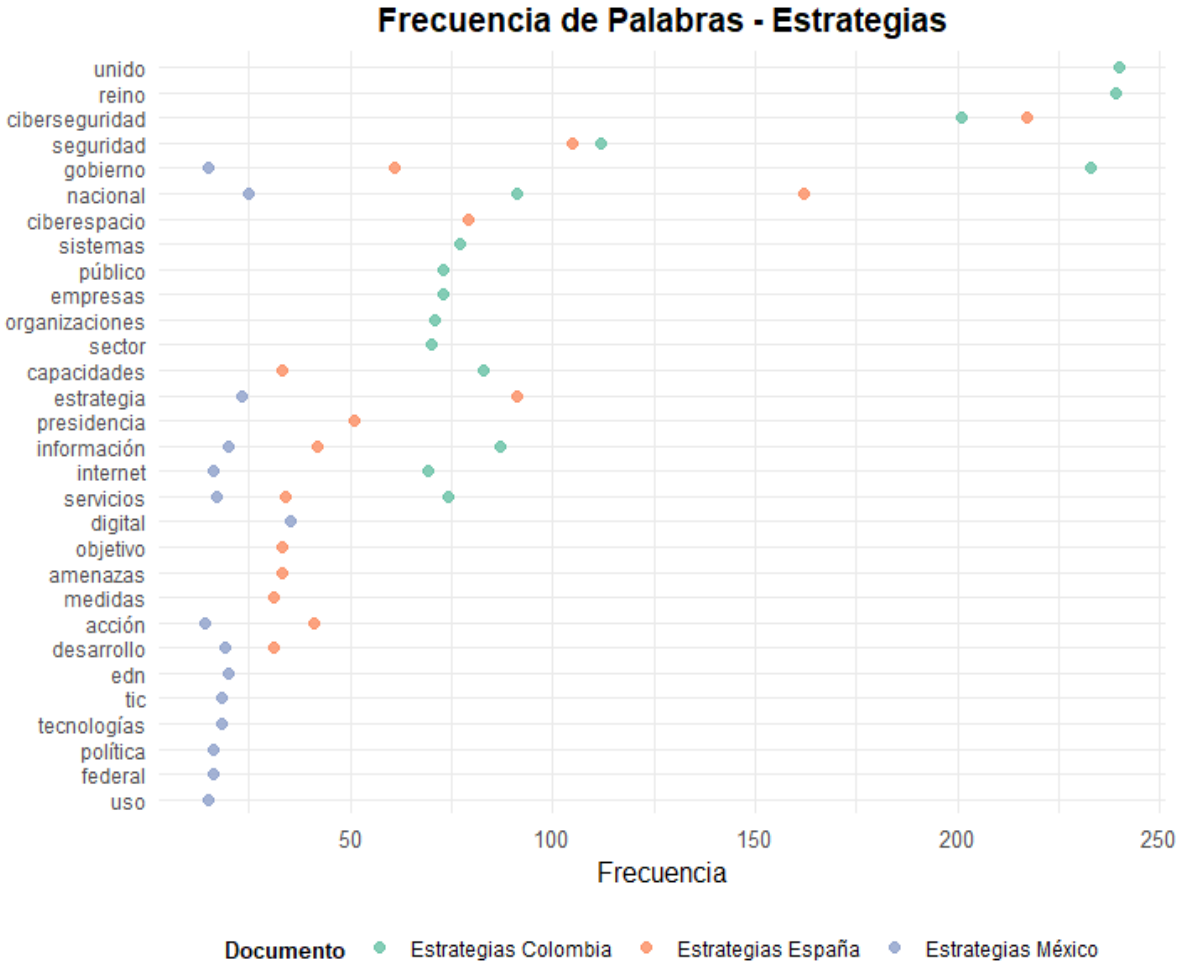
términos como “participación”, “evaluación” o “aprendizaje” sugiere precisamente esa falta de mecanismos de refuerzo que permitan sostener una política adaptativa y legitimada socialmente.

Nota. Representación de la distribución y frecuencia relativa de términos estratégicos en documentos oficiales de seguridad digital. Elaboración propia con minería de texto (2020–2024).

México, aunque también enfatiza el aparato institucional (con palabras como “política”, “federal”, “instrumentos”, “acciones”), introduce mayor diversidad semántica en torno al “uso”, “desarrollo” y “tecnologías”, lo que indica una narrativa más orientada a la innovación digital. Sin

Tabla 14.

Tabla de frecuencia de conceptos clave en las estrategias de seguridad y confianza digital (Colombia, México y España)



embargo, se observa una débil articulación con componentes evaluativos, lo que representa una limitación importante desde el enfoque de políticas públicas efectivas. Tal como plantean Miller y Whicker (1999), la evaluación sistemática y la generación de evidencia son condiciones

fundamentales para la adaptación estratégica de políticas en contextos complejos. La carencia de este componente podría impedir a México consolidar procesos de retroalimentación positiva que sustenten la implementación a largo plazo.

España, en contraste, despliega un discurso más relacional e integrador. La presencia de términos como “cooperación”, “conocimiento”, “interoperabilidad” y “ciudadanos” sugiere una estrategia estructurada sobre bases colaborativas, coherente con los principios del gobierno abierto. Esta orientación no solo fortalece la legitimidad democrática, sino que habilita la cocreación de valor público mediante alianzas multinivel (Criado, 2021). A diferencia de los otros países, España parece avanzar hacia un modelo de confianza digital que no depende exclusivamente del control estatal, sino de relaciones institucionales recíprocas y legitimadas.

No obstante, un elemento transversal a los tres países es la baja frecuencia de conceptos como “riesgo sistémico”, “fractura digital” o “desconfianza”. Esta omisión discursiva impide anticipar las brechas estructurales que erosionan la legitimidad institucional. Schneier (2010) advierte que la confianza digital no se impone desde arriba, sino que es construida a partir de la experiencia del usuario, modelada por su percepción de seguridad, transparencia y respuesta institucional. Ignorar estos elementos podría contribuir a que la política pública de seguridad digital se desconecte de los factores que verdaderamente afectan la confianza ciudadana.

Desde la perspectiva del análisis comparado, puede observarse que Colombia adopta una narrativa predominantemente institucional y jerárquica; México, una normativa orientada a la infraestructura digital; y España, una lógica relacional y ciudadana. Sin embargo, sólo este último caso presenta una mayor probabilidad de generar ciclos de retroalimentación sostenibles. Según Patashnik (2009), esto se debe a que las políticas que no logran crear efectos acumulativos por diseño débil, falta de apoyo institucional o momento político inadecuado tienden a desvanecerse sin dejar legados transformadores. En este contexto, la sostenibilidad política de la estrategia de confianza digital dependerá no sólo de su diseño normativo, sino de su capacidad para activar mecanismos de aprendizaje, evaluación, apropiación social y adaptación constante.

2. Política y Gestión de Incidentes

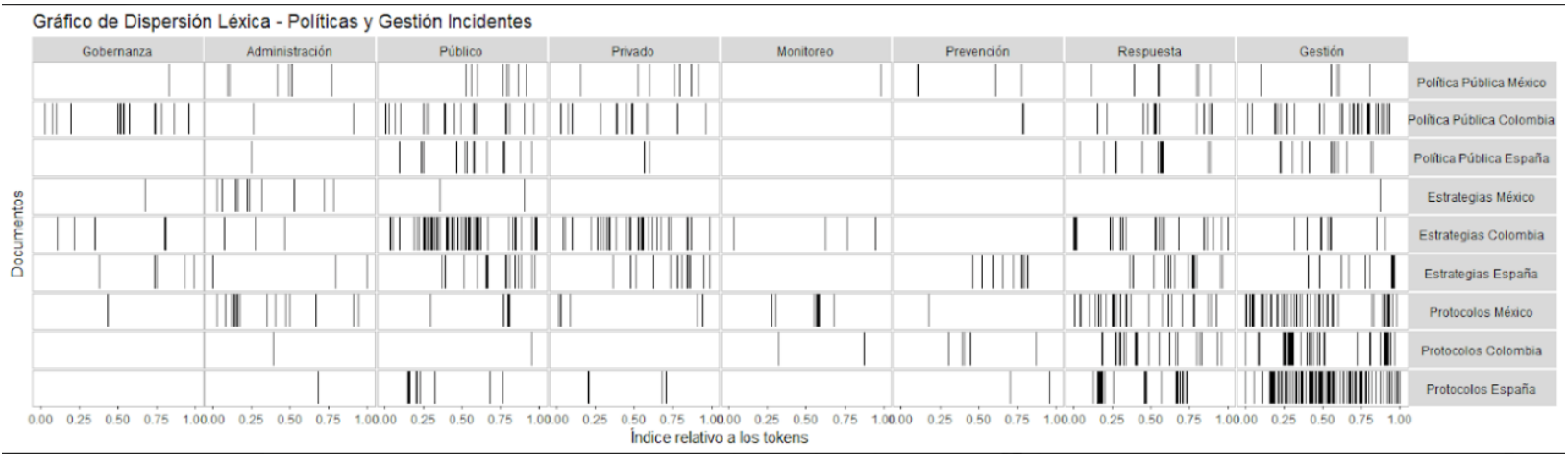
La crecientemente utilización y el avance de las TIC, la ciberseguridad se ha convertido en un elemento esencial para preservar la estabilidad internacional. La presencia constante de internet y las plataformas digitales expone a los estados y sus habitantes a una diversidad de riesgos

cibernéticos que podrían afectar gravemente infraestructuras vitales y provocar importantes pérdidas financieras. La falta de límites en el ciberespacio agrava esta situación, haciendo que la seguridad nacional sea cada vez más vulnerable (Leyva-Méndez, 2021).

En este sentido, el siguiente gráfico de dispersión léxica sobre políticas públicas y gestión de incidentes permite identificar cómo los términos clave se distribuyen en los documentos analizados de México, Colombia y España.

Figura 11.

Gráfico de dispersión léxica – Políticas y Gestión de Incidentes en documentos de México, Colombia y España.



Nota. Elaboración propia con base en análisis de minería de texto aplicada a documentos normativos, estratégicos y operativos de ciberseguridad (2020–2024).

El gráfico de dispersión léxica revela patrones diferenciados en el tratamiento discursivo de la gestión de incidentes cibernéticos en los marcos normativos, estratégicos y operativos de México, Colombia y España. Términos clave como *respuesta*, *prevención*, *monitoreo*, *administración pública* y *gestión* se distribuyen de manera irregular, lo que refleja no solo enfoques técnicos distintos, sino también capacidades institucionales disímiles y trayectorias divergentes de política pública.

En Colombia, se observa una fuerte concentración de los términos *gestión*, *respuesta*, *infraestructura* y *gobierno*. Este patrón sugiere un enfoque estatal centralizado y operativo, donde la atención está puesta en las respuestas institucionales a los incidentes, más que en la anticipación o la resiliencia. Sin embargo, como advierten Sanabria y Leyva (2023), este modelo de gobernanza es el resultado de un proceso de reformas fragmentadas, que combinaron instrumentos de la Nueva

Gestión Pública con modelos normativos sin resolver las deficiencias estructurales de coordinación, meritocracia y vigilancia. A pesar de que Colombia ha desarrollado marcos jurídicos sofisticados, todavía no se aplican de manera uniforme técnicas eficaces de gestión de incidentes, que a menudo dependen de acuerdos extraoficiales o de recursos externos.

En cambio, México tiene una distribución más equitativa de frases como «política», «seguridad», «prevención» y «privado». Aunque todavía no se ha desarrollado completamente una arquitectura de gobernanza adaptativa, esto sugiere una narrativa que reconoce la necesidad de la colaboración público-privada. Aunque la metodología de los textos mexicanos intenta combinar el asesoramiento técnico con el diseño normativo, carece de una estructura institucional sólida para supervisar la aplicación o iniciar canales de retroalimentación eficaces. México se encuentra en un punto intermedio en lo que respecta a la retroalimentación política; su estructura legal ofrece pocos incentivos para el aprendizaje institucional, pero también evita el estancamiento que conllevan las instituciones altamente burocratizadas (Patashnik y Zelizer, 2009).

España, en contraste, despliega una narrativa más integrada y estratégica. La aparición consistente de palabras como *infraestructuras*, *coordinación*, *monitoreo* y *respuesta* revela un modelo basado en la cooperación multinivel y la anticipación de riesgos, articulado con la gobernanza europea. Este enfoque refleja una capacidad institucional más madura, donde la gestión de incidentes no se limita a la reacción inmediata, sino que se inserta en un sistema de seguridad nacional con flujos permanentes de información, evaluación y respuesta. España parece alinearse con lo que Patashnik (2009) denomina un modelo de reforma institucional sostenible, donde las políticas públicas generan efectos acumulativos en capacidades estatales y transforman la relación entre ciudadanía y Estado. Desde una perspectiva comparativa, el análisis muestra que Colombia enfatiza la respuesta desde el aparato estatal, pero con baja articulación evaluativa; México adopta una posición normativa con apertura al sector privado, pero sin mecanismos robustos de seguimiento; y España institucionaliza un enfoque sistémico, apoyado en redes de gobernanza, interoperabilidad y aprendizaje organizacional. Estas diferencias no solo son sintomáticas del nivel de desarrollo institucional, sino también de cómo se concibe la relación entre política, administración pública y seguridad digital.

Así mismo, la nube de palabras (Figura 13) y la tabla de frecuencia (Figura 14) revelan los ejes semánticos que estructuran las políticas públicas de seguridad digital en México, Colombia y España. Aunque existe un núcleo común de términos como *ciberseguridad*, *digital*, *servicios* y *información*, cada país despliega una narrativa con énfasis institucional y funcional propios, reflejo tanto de sus trayectorias normativas como de sus capacidades estatales.

Figura 12.
Nube de palabras – Políticas públicas -Colombia, México y España.

Nota. Visualización de los términos más frecuentes en los documentos normativos de ciberseguridad de los tres países. Elaboración propia con técnicas de minería de texto (2020–2024).

Términos como «servicios esenciales», «operadores», «decreto-ley», «obligaciones» e «información» son bastante comunes en España, lo que indica una política gubernamental muy controlada y centrada en la defensa de las infraestructuras vitales. El marco legislativo de la Unión Europea, que considera la seguridad digital como una cuestión de interés público supranacional, articula este enfoque normativo y técnico. Este enfoque refleja una lógica de gobernanza integrada, en la cual el Estado actúa como garante de estándares comunes y como coordinador de redes público-privadas. Como señalan Sanabria y Leyva (2023), este tipo de arreglo institucional exige una burocracia robusta, capaz de traducir los mandatos normativos en mecanismos operativos y

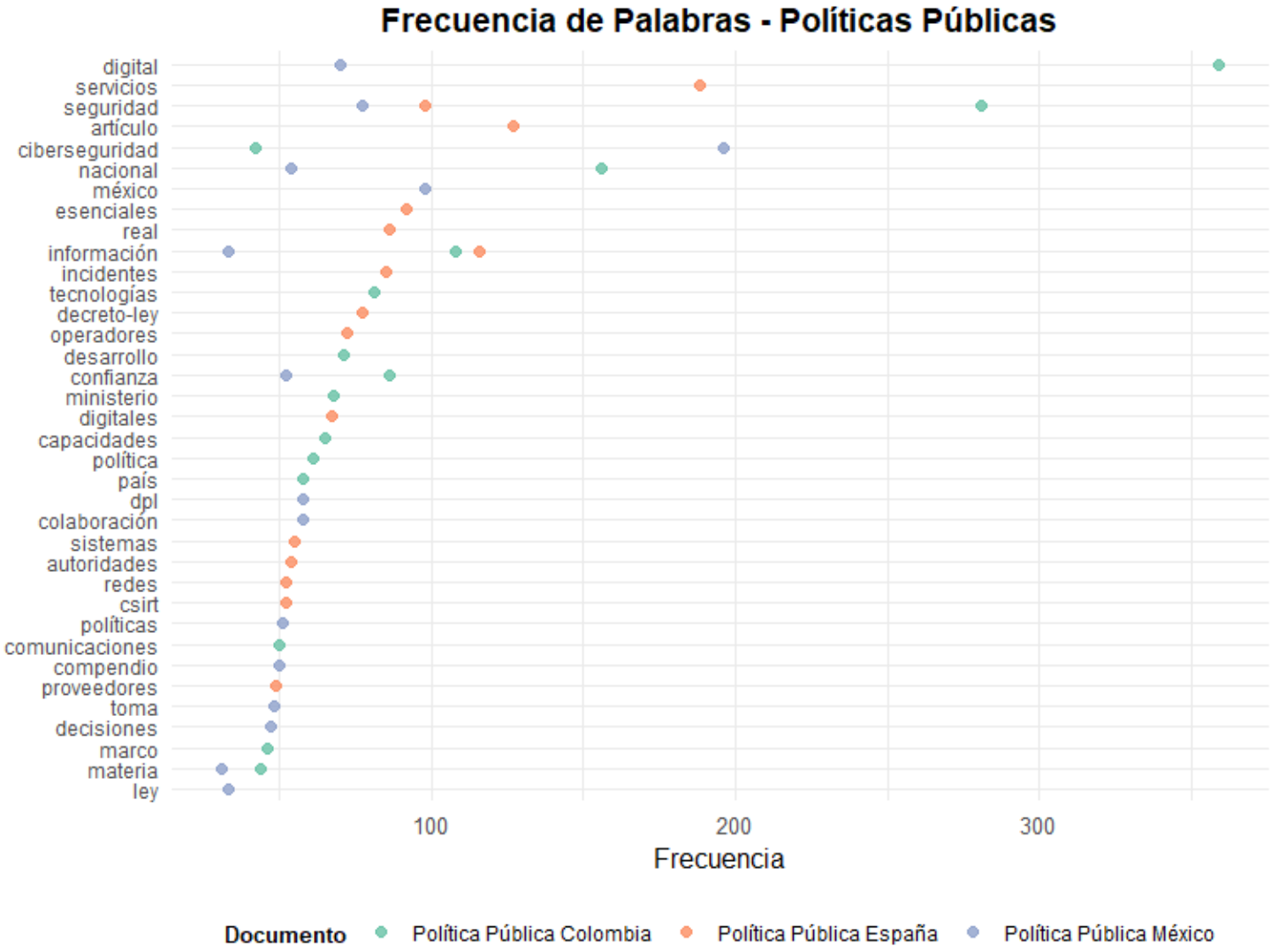
evaluativos sostenibles, algo que España ha logrado consolidar progresivamente a través de reformas basadas en capacidades.

Colombia, en cambio, muestra una frecuencia elevada en términos como *digital*, *seguridad*, *capacidades*, *desarrollo* y *autoridades*. Esta configuración sugiere una política centrada en el fortalecimiento de capacidades estatales, pero con una orientación más programática que regulatoria. Aunque el discurso se apoya en categorías propias de la transformación digital y la protección de activos informáticos, la baja presencia de términos normativos como *decreto*, *obligaciones* o *notificaciones* evidencia una débil estructura de enforcement. Como advierte Patashnik (2009), las reformas que carecen de institucionalización profunda, es decir, que no transforman reglas de operación, incentivos o actores tienden a ser reversibles o a producir impactos acotados. En el caso colombiano, la política de ciberseguridad podría estar atrapada en un diseño débil, donde las capacidades retóricas superan a las capacidades operativas.

México, por su parte, articula su política pública en torno a palabras como *política*, *colaboración*, *comisión*, *congreso*, *materia* y *federal*, lo que indica una narrativa más centrada en la dimensión política-institucional del diseño de la ciberseguridad. Esta semántica refleja el protagonismo del poder legislativo y de las agencias gubernamentales en la formulación de los marcos regulatorios, pero también sugiere una distancia respecto a la ejecución concreta de políticas públicas centradas en la ciudadanía o el aprendizaje institucional. El énfasis en términos como *compendio*, *toma de decisiones* y *referencia* refuerza la idea de una estrategia aún anclada en la formalización normativa y en la sistematización de lineamientos, más que en su implementación integral.

Como lo plantean Sanabria y Leyva (2023), este fenómeno de institucionalismo procedimental presente también en Colombia refleja una tendencia regional a concebir el diseño normativo como un fin en sí mismo, sin garantizar necesariamente la transformación del desempeño público.

Figura 13.
Frecuencia de palabras – Políticas públicas de seguridad digital



Desde una perspectiva crítica, los tres países exhiben vacíos discursivos en torno a nociones clave como *evaluación*, *rendición de cuentas* o *participación ciudadana*, lo cual revela que el diseño de las políticas de ciberseguridad se ha desarrollado principalmente desde arriba, sin mayores vínculos con los marcos de gobernanza democrática digital. Esto limita la capacidad de las políticas para generar ciclos de retroalimentación sostenibles o adaptarse a cambios en el entorno tecnológico y social. En línea con Patashnik (2009), esto sugiere que, si bien las reformas existen formalmente, aún no han logrado consolidar los efectos acumulativos necesarios para volverse irreversibles y efectivas.

3. Infraestructura

En las políticas de ciberseguridad actuales, la salvaguarda de las infraestructuras vitales se ha convertido en un componente esencial. Estas infraestructuras son los pilares esenciales del funcionamiento social, político y económico, y su perturbación podría poner en peligro la integridad institucional y la estabilidad nacional, según el Consejo Europeo (2008). El siguiente gráfico de dispersión léxica muestra la relación entre los términos proveedores y conexiones en documentos gubernamentales mexicanos, colombianos y españoles.

España es particularmente notable por la frecuencia y distribución de la palabra «proveedores» en su política pública, lo que indica una narrativa institucional destinada a controlar, coordinar y supervisar la prestación digital crucial. Modelo europeo gobernanza digital, que se define por las conexiones interdependientes entre el Estado, los operadores clave y los marcos legislativos unificados, es coherente con este nivel de intensidad del discurso. El uso frecuente del término en documentos normativos de alto nivel demuestra una perspectiva estratégica en la que el Estado consolida una estrategia estructural de ciberresiliencia actuando como articulador de capacidades dispersas.

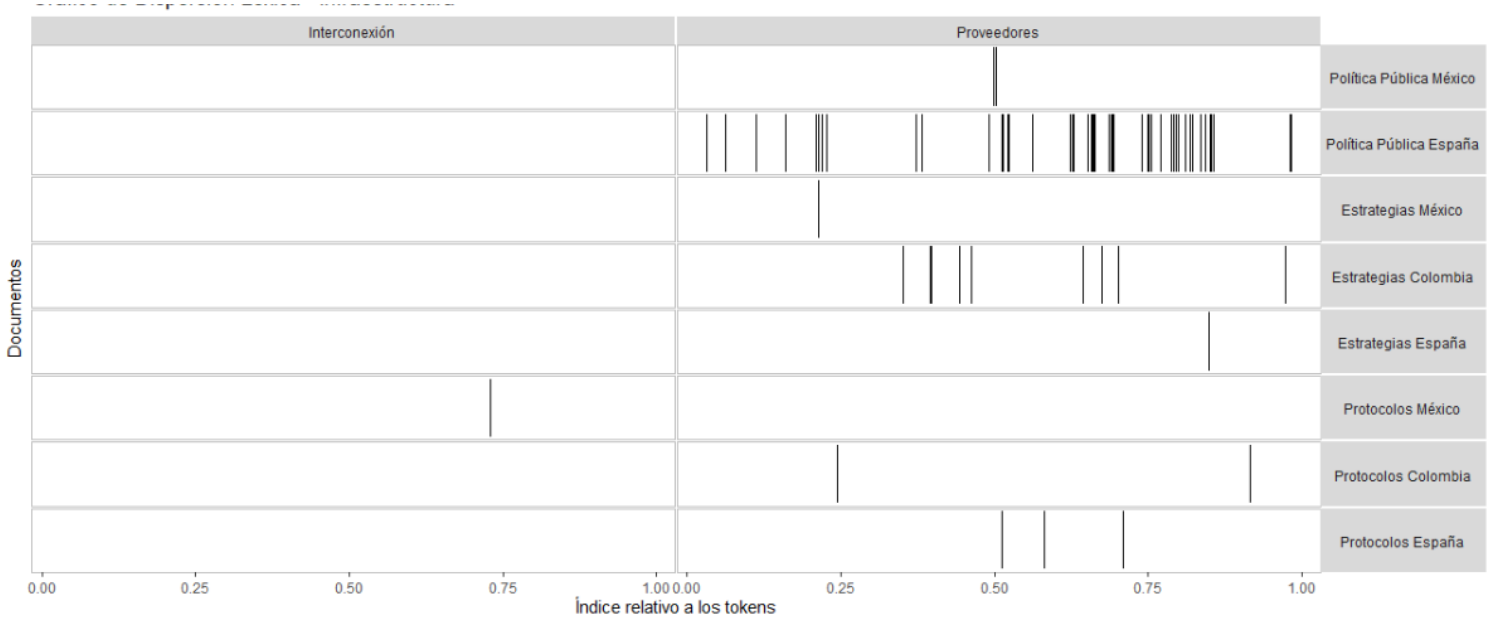
Colombia, por otro lado, tiene una presencia mínima de «interconexión» y una prevalencia mucho menor de la frase «proveedores». Este patrón apunta a una narrativa estrecha sobre la gestión sistémica de infraestructuras vitales o la colaboración con entidades comerciales. Este déficit discursivo, como advierten Sanabria y Leyva (2023), es consecuencia de un modelo de Estado híbrido que ha dado más prioridad al desarrollo normativo que a la construcción de una gobernanza colaborativa o de una capacidad pública sostenible. Una imagen fragmentada de la infraestructura digital que prioriza el control estatal por encima de la resiliencia articulada se muestra en la exclusión de estas ideas cruciales.

Por el contrario, México presenta una mínima diversidad de vocabulario en los términos «interconexión» y «proveedores», lo que indica un incipiente discurso institucional en torno a la infraestructura vital. La falta de estas ideas indica una baja prioridad discursiva del componente operativo y físico de la ciberseguridad, a pesar de que la nación ha adoptado procedimientos regulatorios y procesos de respuesta. En términos de política pública, esta omisión puede estar

limitando la capacidad del Estado mexicano para estructurar una arquitectura de colaboración efectiva con actores del ecosistema digital, condición fundamental para garantizar continuidad operativa ante incidentes complejos.

Figura 14.

Diagrama de dispersión léxica - Infraestructura



En este sentido, se observa que España lidera con un enfoque regulador e interconectado, mientras que Colombia presenta un marco discursivo débil en infraestructura, y México aún carece de una narrativa estructurada en este eje. Estas diferencias no son triviales: el reconocimiento discursivo de los proveedores como actores críticos es condición necesaria para activar mecanismos de coordinación, estándares compartidos y protocolos conjuntos de respuesta. Como argumenta Patashnik (2009), sin estructuras que institucionalicen el cambio, las reformas tienden a ser vulnerables, reversibles o de corto alcance. En ciberseguridad, esto es especialmente relevante: sin gobernanza multinivel, la infraestructura digital se convierte en un punto ciego de la política pública.

Por otra parte, la nube de palabras y la tabla de frecuencia siguientes, revelan cómo cada país organiza discursivamente sus protocolos operativos para proteger infraestructuras críticas y responder ante ciberincidentes. Aunque todos priorizan términos como *seguridad*, *incidentes* y *ciberincidentes*, la distribución semántica muestra énfasis institucionales distintos.

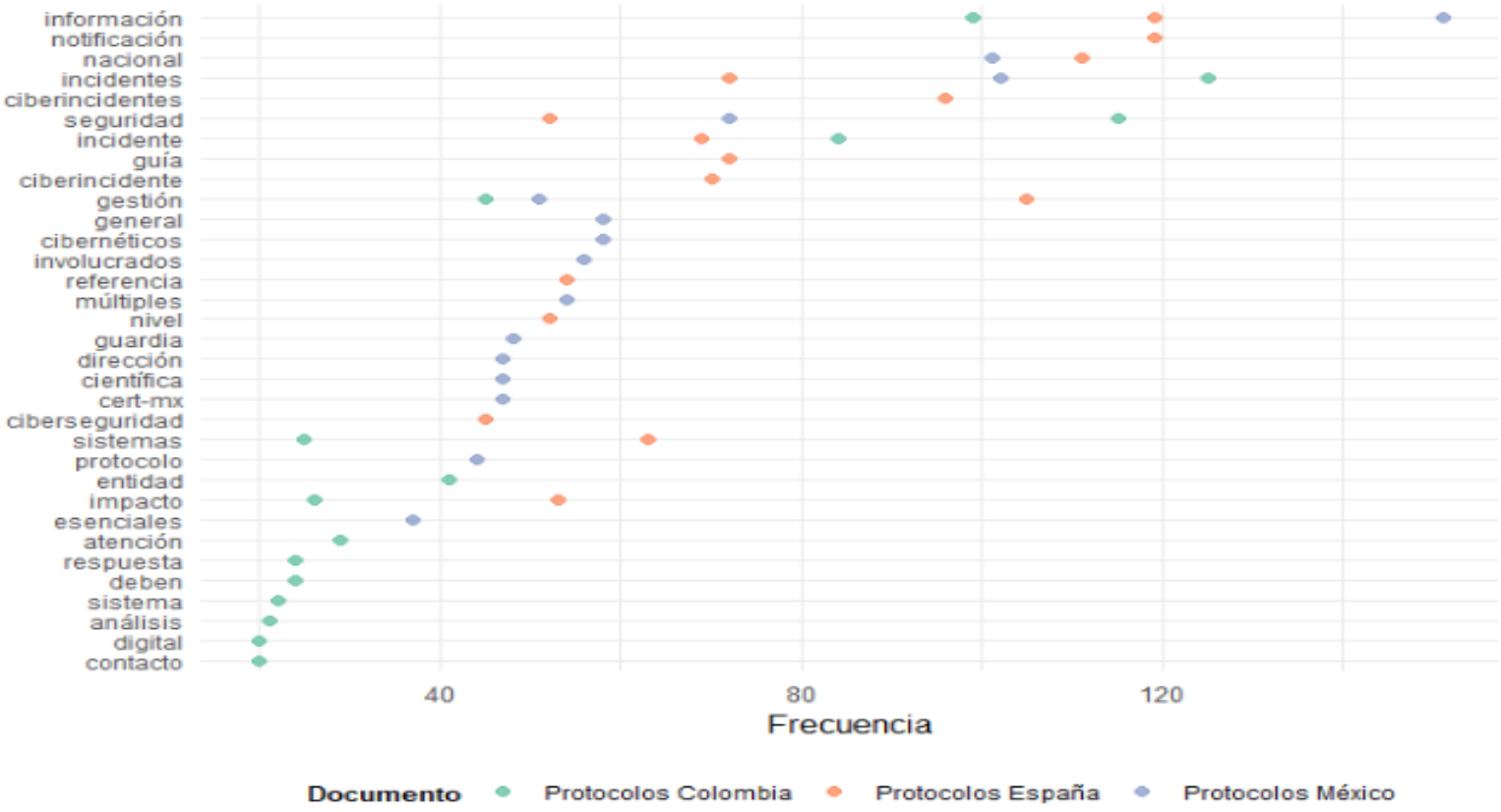
Figura 15.
Nube de palabras protocolos de cada país de estudio

México destaca por la alta frecuencia de términos como *cert-mx*, *científica*, *general*, *involucrados*, *operadores* y *guardia*, lo que refleja una fuerte orientación hacia el nivel federal y la actuación de cuerpos especializados en la gestión de incidentes. Esta narrativa revela una arquitectura protocolaria centralizada, con fuerte énfasis en la clasificación técnica y en la delimitación institucional de responsabilidades. Sin embargo, como advierten Sanabria y Leyva (2023), una institucionalidad centrada en la seguridad técnica, pero sin canales efectivos de articulación multisectorial o capacidades distribuidas, puede derivar en respuestas altamente burocratizadas, con baja adaptabilidad ante amenazas complejas.

Colombia, en cambio, articula sus protocolos en torno a términos como *notificación*, *gestión*, *entidad*, *respuesta*, *guía* y *ámbito*, lo cual sugiere una aproximación más procedimental y adaptativa, donde se intenta definir responsabilidades claras dentro del aparato público. No obstante, la baja visibilidad de términos como *proveedores* o *coordinación* indica una limitada integración de actores no estatales, lo que es problemático en contextos donde gran parte de la infraestructura digital está en manos privadas. En términos de política pública, esta ausencia discursiva compromete la capacidad para consolidar redes resilientes o generar alertas compartidas. Como plantea Patashnik (2009), las reformas que no construyen relaciones duraderas entre actores clave tienden a producir políticas inestables, vulnerables al cambio político o institucional.

Figura 16.

Protocolos España, Colombia México



En cambio, España hace hincapié en «notificación», «múltiple», «niveles», «referencias», «sistemas» e «impacto», además de una semántica más variada. Esta densidad discursiva sugiere un enfoque protocolario más complejo basado en sistemas jerárquicos y marcos interoperables. Parece que España ha creado un lenguaje operativo acorde con las directrices europeas sobre protección de infraestructuras críticas, que instan a los operadores a cooperar y fomentar una

cultura de notificación metódica. En línea con la estrategia estructural de ciberresiliencia propugnada por el Consejo Europeo (2008), esta arquitectura demuestra una lógica de gobernanza relacional y aprendizaje continuo.

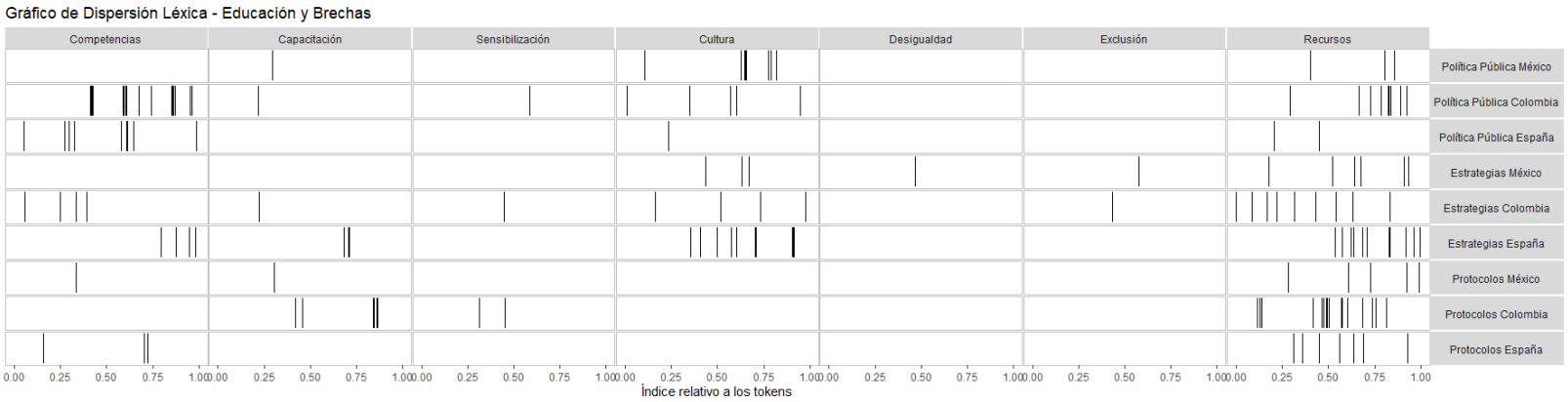
Se observa que mientras México construye un modelo fuertemente estatal y técnico, Colombia opera desde lo procedimental con escasa articulación público-privada, y España despliega un enfoque multinivel y cooperativo, con mecanismos de reporte y gestión del conocimiento institucionalizado. Estas diferencias afectan no solo la eficacia de la respuesta ante incidentes, sino también la posibilidad de prevenir fallas sistémicas y construir confianza digital a largo plazo. En entornos hiperconectados, la resiliencia no depende únicamente de los sistemas, sino de la coordinación eficaz entre sectores, niveles y actores.

4. Educación y Brechas

La capacidad de influir en las normas y comportamientos a través del diseño de tecnologías digitales es un privilegio que, hasta el momento, está concentrado en pocas manos. Algunos Estados y grandes corporaciones poseen los recursos y conocimientos necesarios para moldear estas regulaciones tecnológicas. Esta desigualdad genera una brecha digital que condiciona la capacidad de los países para tomar decisiones soberanas en el ámbito digital. Por lo tanto, es fundamental que los Estados desarrollen capacidades tecnológicas propias para garantizar una regulación democrática y respetuosa de la soberanía nacional (Vercelli, 2015).

En este sentido, se realiza el siguiente análisis del gráfico de dispersión léxica, con respecto a la aparición de términos relacionados con competencias, capacitación, sensibilización, cultura, desigualdad, exclusión y recursos en las políticas públicas, estrategias y protocolos de México, Colombia y España.

Figura 17.
Gráfico dispersión léxica – Educación y Brechas



El gráfico de dispersión léxica evidencia un patrón desigual en la forma en que los marcos normativos, estratégicos y procedimentales de México, Colombia y España incorporan conceptos como *competencias*, *capacitación*, *sensibilización*, *cultura digital*, *desigualdad*, *exclusión* y *recursos*. Estos términos, clave para comprender el vínculo entre ciberseguridad, equidad y formación ciudadana, permiten evaluar si los documentos abordan la dimensión estructural de la brecha digital como parte de su política pública.

España destaca por la aparición consistente de los términos *recursos* y *competencias* en protocolos y estrategias. Esta frecuencia sugiere un enfoque que no se limita a la infraestructura, sino que incorpora la dimensión humana y educativa de la seguridad digital. El reconocimiento explícito de la necesidad de *capacitación* y *sensibilización* indica una narrativa institucional que vincula la ciberseguridad con la construcción de ciudadanía digital, coherente con marcos de gobernanza inclusiva. Además, la presencia del término *cultura* en las políticas públicas españolas muestra que existe un intento por transversalizar la digitalización en términos sociotécnicos, no solo técnicos.

Colombia, por su parte, exhibe una mayor concentración en términos como *cultura*, *competencias* y *recursos* dentro de las estrategias y protocolos. Sin embargo, la virtual ausencia de menciones a *exclusión*, *desigualdad* y *sensibilización* sugiere una política pública que reconoce la brecha digital desde una perspectiva funcional como falta de habilidades o equipamiento, pero no desde una óptica estructural. Esto refleja lo que Vercelli (2015) denomina “asimetría tecnológica”, donde el control del entorno digital sigue en manos de élites estatales o corporativas,

sin democratizarse hacia los sectores periféricos o marginados. La omisión de estas desigualdades en el discurso institucional limita la posibilidad de diseñar políticas que enfrenten las causas profundas de la exclusión digital.

México, en contraste, presenta una baja densidad léxica general en todos los conceptos del eje, con excepciones parciales en *cultura* y *recursos* en protocolos. Este patrón muestra una narrativa débil en torno a la dimensión educativa de la ciberseguridad, lo que implica un desfase entre el enfoque técnico-normativo y las realidades sociales que atraviesan el acceso, uso y apropiación de tecnologías. Tal como han planteado estudios sobre políticas digitales en América Latina, la falta de estrategias activas de formación y empoderamiento digital reproduce desigualdades ya existentes, y obstaculiza la creación de soberanía tecnológica a nivel nacional.

En este contexto puede afirmarse que, España avanza hacia un modelo más inclusivo e integral, donde la ciberseguridad se articula con capacidades ciudadanas y políticas redistributivas. Colombia construye un enfoque parcial, centrado en competencias y recursos, pero sin afrontar plenamente las causas de la brecha digital. México, por su parte, presenta una narrativa institucional incipiente, con escasa tematización de la educación digital como herramienta de soberanía o justicia tecnológica. Esta asimetría discursiva reproduce desigualdades globales en el acceso al conocimiento, y pone en riesgo la capacidad de los países para diseñar e implementar marcos regulatorios propios frente a lógicas impuestas por actores dominantes del norte global (Vercelli, 2015).

El análisis comparativo de los documentos normativos, estratégicos y operativos de México, Colombia y España evidencia una profunda heterogeneidad en los enfoques nacionales frente a la seguridad y confianza digital. Aunque los tres países han desarrollado políticas que abordan los riesgos del entorno digital, la forma en que articulan conceptos como gestión de incidentes, infraestructura crítica, soberanía tecnológica y brechas educativas revela diferencias no solo en sus capacidades institucionales, sino en las lógicas de gobernanza que orientan sus decisiones públicas. La siguiente matriz permite visualizar de forma clara las similitudes, diferencias y vacíos entre los enfoques adoptados por cada país, tanto en lo normativo como en lo operativo.

Tabla 15.
Matriz similitudes y diferencias Colombia, España, México

LÍNEAS DE ACCIÓN	OBJETIVOS	COMPONENTES	INDICADORES DE SEGUIMIENTO
Diseño del Programa Nacional de Capacidades Digitales para la Gestión Pública	Estandarizar e institucionalizar un programa de formación y certificación en seguridad digital, enfocado en servidores públicos de los niveles nacional y territorial.	Módulos temáticos: protección de datos, análisis de riesgo, ciberresiliencia, gestión de incidentes, marcos internacionales (NIST-CSF, ISO 27001). Modalidades: formación mixta (virtual-presencial) con acreditación nacional. Alianzas: universidades públicas, SENA, MinTIC y cooperación internacional	% de servidores públicos certificados por nivel (básico/intermedio/avanzado). % de entidades con personal capacitado en normativa del CONPES 3995. Número de capacitaciones anuales ofrecidas por sector.
Fortalecimiento de infraestructura tecnológica en entidades priorizadas	Identificar, actualizar y proteger los sistemas tecnológicos de entidades que prestan servicios esenciales.	Auditoría de vulnerabilidades técnicas y obsolescencia. Adopción de esquemas de defensa en profundidad, segmentación de redes y sistemas de respaldo seguro. Priorización de inversión basada en análisis de criticidad.	% de entidades con infraestructura actualizada según estándar técnico. % de servicios esenciales con continuidad operativa garantizada ante ciberincidentes. N° de inversiones en ciberseguridad financiadas vía presupuesto nacional o cooperación.
Creación de Unidades Técnicas de Respuesta Rápida (UTRR)	Establecer equipos técnicos sectoriales que actúen como primeros respondedores ante incidentes de ciberseguridad, articulados con el CSIRT nacional.	Conformación de equipos multidisciplinarios en entidades de sectores como salud, justicia, transporte y educación. Protocolos de actuación estandarizados (detección, contención, recuperación, reporte). Simulacros anuales obligatorios por sector.	Tiempo medio de contención de incidentes (MTTC). % de sectores con equipos UTRR activos. N° de simulacros realizados y evaluados por año.
Integración de las capacidades operativas al ciclo de gestión institucional	Incluir explícitamente la ciberseguridad y la confianza digital como variables obligatorias en los instrumentos de planeación institucional (PEI, MIPG, FURAG).	Lineamientos técnicos del DNP y MinTIC para transversalizar la política digital. Inclusión en indicadores de desempeño institucional. Evaluación del avance de entidades en términos de madurez digital.	% de planes institucionales que integran objetivos de confianza digital. Puntuación media en los indicadores de gestión TI del FURAG. N° de auditorías que incluyen ciberseguridad como criterio de evaluación.

Esta matriz evidencia que, aunque los tres países reconocen la importancia de la ciberseguridad como eje estratégico, España avanza con un modelo más integral, institucionalizado y adaptativo. Colombia y México, por su parte, muestran desarrollos desiguales: mientras Colombia amplía sus marcos normativos con dificultades en la implementación, México

mantiene una narrativa legal-técnica con baja integración social. Las brechas en infraestructura crítica, participación multisectorial y capacidades ciudadanas limitan la consolidación de una política verdaderamente soberana e inclusiva en América Latina.

III. PROPUESTAS PARA EL FORTALECIMIENTO DE LA CONFIANZA Y SEGURIDAD DIGITAL EN COLOMBIA

Es necesario comenzar a ver las potencialidades que la transformación digital tiene para superar los desafíos que enfrenta Colombia en sentido social, ambiental y económico, que se dan por medio de la consolidación de sus elementos habilitadores y un impulso decidido al uso y apropiación de los datos y las tecnologías digitales por parte de las entidades públicas, los hogares, las personas y el sector productivo, aproximándose a los riesgos, daños y retos posibles que conlleva el crecimiento de la digitalización. En este sentido, y a partir de los resultados presentados en la presente investigación, se exponen las brechas y los retos de Colombia en la seguridad digital, las lecciones aprendidas respecto a las buenas prácticas de los países de México y España, para finalmente realizar una propuesta para el fortalecimiento de la confianza y seguridad digital en Colombia a partir de la Política Nacional de confianza y seguridad digital, CONPES 3995 (2020).

1. Fortalecimiento de la capacidad técnica y operativa para la implementación efectiva del CONPES 3995

Una de las principales limitaciones identificadas en la evaluación del CONPES 3995 es la débil capacidad técnica y operativa de las entidades encargadas de su implementación, lo cual impide su consolidación como una política pública transformadora. La evidencia recopilada en los objetivos 1 y 2 de esta investigación muestra que, pese al avance normativo, Colombia continúa anclada a un modelo de acción fragmentado y técnicamente débil, en el que las entidades no cuentan con el talento humano, las herramientas tecnológicas ni las condiciones estructurales para ejecutar una política integral de confianza y seguridad digital.

A diferencia de España, donde se ha consolidado una arquitectura de gobernanza digital con cuerpos técnicos especializados, y de México, que ha establecido centros de respuesta sectorial y protocolos federales de coordinación, en Colombia persiste una brecha entre el diseño de política pública y su capacidad institucional de ejecución. Por tanto, se propone una estrategia enfocada en

el fortalecimiento del talento técnico, la infraestructura digital y la capacidad de ejecución en todos los niveles del Estado, con énfasis en sectores estratégicos.

Tabla 16.
Líneas de acción fortalecimiento técnico

LÍNEAS DE ACCIÓN	OBJETIVOS	COMPONENTES	INDICADORES DE SEGUIMIENTO
Diseño del Programa Nacional de Capacidades Digitales para la Gestión Pública	Estandarizar e institucionalizar un programa de formación y certificación en seguridad digital, enfocado en servidores públicos de los niveles nacional y territorial.	Módulos temáticos: protección de datos, análisis de riesgo, ciberresiliencia, gestión de incidentes, marcos internacionales (NIST-CSF, ISO 27001). Modalidades: formación mixta (virtual-presencial) con acreditación nacional. Alianzas: universidades públicas, SENA, MinTIC y cooperación internacional	% de servidores públicos certificados por nivel (básico/intermedio/avanzado). % de entidades con personal capacitado en normativa del CONPES 3995. Número de capacitaciones anuales ofrecidas por sector.
Fortalecimiento de infraestructura tecnológica en entidades priorizadas	Identificar, actualizar y proteger los sistemas tecnológicos de entidades que prestan servicios esenciales.	Auditoría de vulnerabilidades técnicas y obsolescencia. Adopción de esquemas de defensa en profundidad, segmentación de redes y sistemas de respaldo seguro. Priorización de inversión basada en análisis de criticidad.	% de entidades con infraestructura actualizada según estándar técnico. % de servicios esenciales con continuidad operativa garantizada ante ciberincidentes. N° de inversiones en ciberseguridad financiadas vía presupuesto nacional o cooperación.
Creación de Unidades Técnicas de Respuesta Rápida (UTRR)	Establecer equipos técnicos sectoriales que actúen como primeros respondedores ante incidentes de ciberseguridad, articulados con el CSIRT nacional.	Conformación de equipos multidisciplinarios en entidades de sectores como salud, justicia, transporte y educación. Protocolos de actuación estandarizados (detección, contención, recuperación, reporte). Simulacros anuales obligatorios por sector.	Tiempo medio de contención de incidentes (MTTC). % de sectores con equipos UTRR activos. N° de simulacros realizados y evaluados por año.
Integración de las capacidades operativas al ciclo de gestión institucional	Incluir explícitamente la ciberseguridad y la confianza digital como variables obligatorias en los instrumentos de planeación institucional (PEI, MIPG, FURAG).	Lineamientos técnicos del DNP y MinTIC para transversalizar la política digital. Inclusión en indicadores de desempeño institucional. Evaluación del avance de entidades en términos de madurez digital.	% de planes institucionales que integran objetivos de confianza digital. Puntuación media en los indicadores de gestión TI del FURAG. N° de auditorías que incluyen ciberseguridad como criterio de evaluación.

Esta estrategia no se limita a reforzar habilidades técnicas en abstracto, sino que busca conectar capacidades institucionales, planificación estratégica y cultura digital. Fortalecer las

capacidades técnicas y operativas no es solo un paso necesario para la implementación del CONPES 3995: es la condición mínima para que la política de confianza y seguridad digital transite de la norma al territorio, y de la intención a la transformación institucional.

2. Evaluación y rediseño continuo de la política pública de confianza y seguridad digital

Uno de los hallazgos más significativos de esta investigación es la debilidad de los mecanismos de evaluación, seguimiento y retroalimentación institucional en la implementación del CONPES 3995. A pesar de contar con una política formalmente adoptada, el bajo nivel de cumplimiento, la dispersión de responsabilidades y la ausencia de una arquitectura evaluativa sólida han limitado su capacidad transformadora. Colombia presenta una brecha entre el diseño técnico de la política y su capacidad real de aprendizaje institucional.

A diferencia de España, donde existen sistemas integrados de evaluación periódica vinculados a indicadores de madurez digital y planes de mejora correctiva, o de México, donde se han desarrollado observatorios ciudadanos y plataformas de transparencia en ciberseguridad, en Colombia la evaluación de esta política pública ha sido superficial, poco participativa y sin mecanismos adaptativos.

Por ello, esta estrategia propone un rediseño estructural del sistema de seguimiento, evaluación y retroalimentación del CONPES 3995, con base en principios de evaluación orientada al cambio, alineación normativa, apertura institucional y control social.

Esta estrategia no solo fortalece los sistemas de evaluación existentes, sino que redefine el papel del Estado como actor que aprende, se adapta y rinde cuentas. Evaluar no es simplemente medir el cumplimiento de metas, sino abrir espacios para el rediseño constante, la corrección de desvíos y la construcción colectiva de legitimidad institucional. Implementar esta estrategia posiciona la política de seguridad digital como un instrumento dinámico de gobernanza pública, no como una normativa estática.

Tabla 17.
Estrategia evaluación y rediseño continuo

LÍNEAS DE ACCIÓN	OBJETIVOS	COMPONENTES	INDICADORES DE SEGUIMIENTO
Diseño del Sistema de Evaluación Integral de la Política de Confianza y Seguridad Digital (SEIP-CSD)	Crear un sistema permanente de evaluación que combine seguimiento técnico, análisis institucional, retroalimentación participativa y control ciudadano.	Marco de evaluación basado en teoría del cambio, metas cuantificables y ciclos de ajuste. Participación de actores públicos, privados, académicos y sociedad civil. Publicación periódica de resultados y recomendaciones.	N° de informes de evaluación publicados por año. % de acciones del CONPES 3995 ajustadas tras evaluación. Grado de cumplimiento del plan de mejora posterior a cada ciclo de evaluación.
Integración de indicadores técnicos y estratégicos en el FURAG y el SIPG	Incorporar la política de confianza y seguridad digital como un eje transversal del desempeño institucional medido por el DAFP.	Desarrollo de un set de indicadores de madurez digital y ciberresiliencia institucional. Vinculación directa de estos indicadores a planes de mejora y recursos presupuestales. Capacitación a evaluadores institucionales en enfoque de gobernanza digital.	% de entidades con indicadores digitales integrados al FURAG. Evolución del puntaje promedio nacional en gobernanza TI. N° de entidades con planes de mejora específicos en seguridad digital.
Plataforma pública de seguimiento a la política de seguridad digital	Garantizar transparencia, control social y participación mediante una herramienta pública y digital de monitoreo.	Dashboard interactivo con visualización de indicadores, alertas, metas y avances. Mecanismos de retroalimentación ciudadana (encuestas, reportes, observaciones). Espacios de diálogo entre entidades ejecutoras y ciudadanía organizada.	N° de visitas y usuarios activos de la plataforma. N° de observaciones ciudadanas incorporadas en los informes de seguimiento. Nivel de percepción ciudadana sobre confianza digital (encuesta nacional).

3. Fortalecimiento de la gobernanza y la articulación interinstitucional en seguridad digital

Una de las debilidades estructurales más visibles en la evaluación de la política de confianza y seguridad digital en Colombia es la ausencia de una arquitectura de gobernanza clara, cohesionada y operativa. Pese a la existencia de múltiples actores involucrados MinTIC, CSIRT, entidades sectoriales, operadores privados y entes territoriales no existe una instancia de coordinación efectiva que alinee esfuerzos, defina prioridades conjuntas y garantice respuestas articuladas frente a amenazas digitales complejas.

Este vacío se traduce en ineficiencia, duplicación de esfuerzos, fragmentación normativa y baja trazabilidad en la implementación del CONPES 3995. Mientras en España se han consolidado modelos de gobernanza multinivel y cooperación obligatoria entre operadores y Estado, y en México se avanza en la construcción de mecanismos federales articulados, Colombia sigue operando bajo una lógica institucional dispersa. Esta estrategia plantea, por tanto, un rediseño de la gobernanza de la política pública, centrado en la coordinación, corresponsabilidad y capacidad de respuesta conjunta.

Como se evidencia a continuación, esta estrategia apunta a cerrar la brecha más sensible de la política de confianza y seguridad digital en Colombia: su incapacidad para operar como un sistema. Sin coordinación, no hay respuesta oportuna. Sin gobernanza efectiva, las políticas se fragmentan. Consolidar estructuras formales de cooperación, articulación sectorial y mecanismos de corresponsabilidad permitirá que el CONPES 3995 se implemente con alcance real, legitimidad institucional y capacidad operativa sostenida.

Tabla 18.

Fortalecimiento de la gobernanza y la articulación interinstitucional

LÍNEAS DE ACCIÓN	OBJETIVOS	COMPONENTES	INDICADORES DE SEGUIMIENTO
Marco de cooperación público-privada para infraestructura crítica digital	Establecer mecanismos jurídicos e institucionales que obliguen a los operadores de infraestructura crítica a colaborar con el Estado en seguridad digital.	Firma de acuerdos de cooperación obligatoria y confidencialidad. Integración de los operadores en ejercicios de simulación y respuesta conjunta. Revisión periódica de los niveles de riesgo compartido.	N° de operadores críticos vinculados formalmente. N° de simulacros conjuntos público-privados realizados. Tiempo medio de respuesta ante eventos compartidos de alto impacto.
Formalización de redes sectoriales de seguridad digital	Establecer comités técnicos permanentes en sectores estratégicos (salud, justicia, energía, transporte, educación), articulados con el Comité Nacional y el CSIRT.	Elaboración de protocolos sectoriales de prevención, respuesta y recuperación. Coordinación con actores privados (EPS, operadores energéticos, universidades, etc.). Evaluación sectorial periódica de amenazas y capacidades.	N° de redes sectoriales activas y funcionales. % de sectores con protocolos sectoriales validados. Grado de madurez operativa de cada red, según matriz técnica MinTIC.
Creación del Comité Nacional de Gobernanza Digital y Ciberseguridad	Establecer un órgano técnico de alto nivel, con capacidad de decisión, que articule al nivel central, sectorial y territorial, y garantice la implementación transversal del CONPES 3995.	Participación de MinTIC, Presidencia, CSIRT, Procuraduría, operadores críticos, sector privado y entes territoriales. Funciones: diseño de estrategias, definición de alertas prioritarias, gestión de crisis y seguimiento a planes sectoriales. Reuniones periódicas y generación de informes públicos.	N° de sesiones realizadas y acuerdos operativos adoptados. % de sectores integrados con representación permanente. N° de acciones coordinadas ejecutadas en respuesta a eventos críticos.

4. Inclusión digital, alfabetización tecnológica y cultura de confianza

Uno de los pilares fundamentales de una política pública de seguridad digital eficaz es su capacidad para integrarse con los derechos ciudadanos, la justicia digital y la equidad territorial. En Colombia, la brecha digital sigue siendo una barrera estructural que impide que amplios sectores de la población accedan de forma segura, consciente y activa al entorno digital. Esta situación no solo profundiza desigualdades socioeconómicas, sino que erosiona la legitimidad de las políticas de transformación digital y limita su sostenibilidad. El diagnóstico evidenció que la Política Nacional de Confianza y Seguridad Digital (CONPES 3995) ha sido concebida desde una lógica eminentemente técnica, con baja participación ciudadana y escasa incorporación de estrategias de empoderamiento digital. La falta de programas estructurados de alfabetización tecnológica, sensibilización en protección de datos, cultura de reporte o promoción de derechos digitales representa una amenaza a largo plazo para la construcción de confianza pública.

Tabla 19.

Inclusión digital, alfabetización tecnológica y cultura de confianza

LÍNEAS DE ACCIÓN	OBJETIVOS	COMPONENTES	INDICADORES DE SEGUIMIENTO
Programa Nacional de Alfabetización Digital con enfoque diferencial	Diseñar e implementar un programa permanente de formación ciudadana en confianza y seguridad digital, con enfoques territoriales, etarios, de género y étnico.	Contenidos: navegación segura, protección de datos personales, reporte de incidentes, derechos digitales, desinformación. Modalidades: talleres presenciales, recursos virtuales, trabajo comunitario y alianzas con bibliotecas, centros educativos y JAC. Participación de entidades territoriales, universidades públicas y el sector educativo.	N° de personas beneficiarias por región y grupo poblacional. N° de municipios con cobertura activa del programa. Nivel de apropiación medido mediante encuestas antes/después.
Integración curricular de la seguridad digital en educación básica y media	Incluir la ciberseguridad, el pensamiento crítico digital y los derechos en internet como componentes del currículo escolar nacional.	Inclusión de contenidos obligatorios en áreas de tecnología, ética y ciudadanía. Capacitación docente en enfoques de educación digital segura. Evaluación de competencias digitales de los estudiantes.	% de instituciones educativas que aplican el componente curricular. % de docentes capacitados en ciudadanía digital. Evaluación de competencias en seguridad digital en pruebas Saber.
Campaña nacional de cultura de confianza digital	Promover una cultura pública de confianza, corresponsabilidad y conciencia frente a los riesgos y derechos en el entorno digital.	Campañas multicanal (TV, radio, redes, comunitarias) sobre prevención, privacidad, reporte y buenas prácticas. Enfoque positivo y preventivo: la confianza como construcción colectiva, no solo como control estatal. Participación de actores públicos, medios, sector privado y sociedad civil.	Alcance estimado de la campaña por región y medio. N° de reportes ciudadanos registrados tras las campañas. Nivel de percepción de confianza digital (encuesta nacional DANE/MinTIC).

A partir de lo anterior, se busca corregir el sesgo tecnocrático de la política actual, reconociendo que la seguridad digital no es un asunto exclusivo del Estado ni de expertos, sino una dimensión transversal del ejercicio ciudadano. Sin inclusión, no hay legitimidad. Sin ciudadanía informada, no hay confianza. Y sin confianza, ninguna arquitectura digital es sostenible.

CONCLUSIONES Y RECOMENDACIONES

El análisis del marco institucional, los documentos normativos y los sistemas de seguimiento de la política pública de confianza y seguridad digital en Colombia permitió advertir una contradicción estructural entre el avance regulatorio y la precariedad de sus condiciones de implementación. La existencia de un instrumento como el CONPES 3995 representa un paso importante hacia la consolidación de un ecosistema digital seguro, pero no garantiza, por sí solo, su efectividad en el plano operativo. La política ha sido formulada bajo principios conceptualmente adecuados como la transversalidad, la protección de derechos digitales y la corresponsabilidad multisectorial, pero se ha desplegado en un entorno caracterizado por capacidades institucionales desiguales, debilidad técnica en los niveles territoriales y escasa cultura de evaluación.

La coordinación, la trazabilidad y la consolidación de una gobernanza digital sólida se ven obstaculizadas por la notable fragmentación entre los numerosos niveles gubernamentales y sectores responsables que se puso de manifiesto al examinar los documentos de estrategia y las herramientas de supervisión del Estado.

Las entidades operan de forma discontinua, sin protocolos interoperables ni mecanismos de reporte compartidos, y con bajos niveles de formación especializada en temas que requieren abordajes altamente técnicos. Estos fallos han conducido a un enfoque reactivo de la gestión de los riesgos digitales, que obstaculiza el desarrollo de una cultura institucional de anticipación, adaptabilidad y aprendizaje -todos ellos componentes esenciales de la ciberresiliencia- y retrasa la capacidad de reacción ante las ciberamenazas.

El estudio comparativo demostró que la creación de una política de éxito en este ámbito depende de la capacidad del Estado para crear coordinación, cultivar la confianza pública y crear un clima de responsabilidad compartida, además del marco normativo. Las experiencias de España y México mostraron que cuando la seguridad digital es concebida como parte integral del aparato

público y no como un componente accesorio vinculado exclusivamente a las tecnologías es posible construir respuestas más sólidas y sostenibles. En ambos casos, la existencia de comités técnicos, redes de cooperación público-privada, mecanismos de evaluación continua y campañas ciudadanas contribuyó a fortalecer la legitimidad y el alcance de sus respectivas estrategias.

En contraste, la política colombiana aún se encuentra anclada en una lógica vertical y centrada en el cumplimiento de metas técnicas sin conexión con la ciudadanía ni con las realidades de los territorios. Términos como participación, inclusión, evaluación y confianza se utilizan poco en los documentos nacionales, según la minería de textos realizada sobre ellos. Esto indica que la política pública está más centrada en el control que en la creación de capacidades. Esta ausencia es significativa porque dificulta la comprensión de la confianza digital como un valor compartido basado en la apertura, la corresponsabilidad y la protección de derechos, así como la ciberseguridad como un beneficio público.

En consecuencia, es necesario un cambio significativo que articule la seguridad digital con un plan institucional a largo plazo y trascienda la visión tecnocrática. Hay que dotar a las políticas de capacidad de aplicación real; limitarse a dictarlas es insuficiente. Para garantizar que la política deje de ser una herramienta programática y se convierta en una herramienta de cambio institucional, es imprescindible fortalecer el capital humano del Estado, integrar la ciberseguridad en el ciclo de planificación institucional, establecer procedimientos de evaluación independientes y crear foros de comunicación entre actores públicos, privados y sociales.

Del mismo modo, sin abordar la brecha digital que sitúa a millones de personas en la periferia de las ventajas y peligros del mundo digital, ningún esfuerzo institucional puede sostenerse. Además de restringir el acceso a los servicios, la exclusión tecnológica también obstaculiza el desarrollo de una ciudadanía digital comprometida. La alfabetización tecnológica, el desarrollo de una cultura de confianza digital y el éxito de la protección de los derechos fundamentales en Internet -especialmente para las poblaciones históricamente excluidas- necesitan que el Estado asuma un compromiso ético y político.

Este artículo ofrece un punto de vista crítico sobre las deficiencias del enfoque formalista de la elaboración de políticas digitales en el contexto de la gestión pública. Las soluciones institucionales requieren circunstancias de aplicación, marcos de evaluación y procedimientos de aprendizaje en grupo, en lugar de limitarse únicamente a la formulación de políticas. Las políticas deben considerarse marcos vivos que pueden ajustarse a las circunstancias, cambiar en respuesta

a las pruebas y evolucionar en función de la participación y las pruebas, en lugar de funcionar como dispositivos cerrados. Sólo así podrá establecerse un modelo de gobernanza digital democrático, legítimo y exitoso, en el que la seguridad sea un requisito previo y no un obstáculo para el ejercicio libre, justo y respetable de la ciudadanía en la era digital.

REFERENCIAS BIBLIOGRÁFICAS

Accenture. (2019). Securing the Digital Economy. Reinventing the Internet for Trust. Obtenido de https://library.cyentia.com/report/report_002680.html

Aguilar-Antonio, J.-M. (2020). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, 25, 24-40.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., ... & Savage, S. (2012). Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy* (pp. 265-300). Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-33383-5_12.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine*, 40(8), 102-114. DOI: 10.1109/MCOM.2002.1024422

Antonio, J. M. A. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Revista de estudios en seguridad internacional*, *6*(2), 17-43.

Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios Internacionales*, *53*(198), 169–197. https://doi.org/10.5354/0719-3769.2021.57067

Ballesteros Trujillo, B. Z. (2014). Reflexión sobre la teoría de la sociedad del riesgo. *Temas Sociales*, 203.

Belmonte, A., Braunbel, M., Camerano, A., Camuña, P., Caramuto, M., Carbajal, M., ... & Stalker, G. (2009). Construyendo confianza: hacia un nuevo vínculo entre estado y sociedad civil (Vol. 2). *Fundación CIPPEC*.

Bossler, A. M., Holt, T. J., & Seigfried-Spellar, K. C. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Routledge.

Baldwin, D (1997).The concept of Security, en Review of International Studies, 23, 5- 26.

Centro Criptológico Nacional, (2020). La ciberseguridad y su relevancia en el Sector Público: El papel del Centro Criptológico Nacional. *Revista española de control externo*, *22*(64), 66-87.

Cámara Colombiana de Informática y Telecomunicaciones. (2023). *Estudio anual de ciberseguridad*. Recuperado de https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf

Consejo Europeo. (2008). *Directiva 2008/114/CE del Consejo Europeo relativa a la identificación y designación de las infraestructuras críticas europeas y a la evaluación de la necesidad de mejorar su protección*. Diario Oficial de la Unión Europea. Disponible en: https://eur-lex.europa.eu

Departamento Nacional de Planeación (DNP). (2016). POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación (DNP). (2020). CONPES 3995 de 2020: Política nacional de confianza y seguridad digital. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Departamento Nacional de Planeación (DNP). (2011). *CONPES 3701 de 2011: Política Nacional de ciberdefensa y Ciberseguridad*. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación (DNP). (2016). Política Nacional de Seguridad Digital (CONPES 3854). Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Schmitt, M. N. (Ed.). (2017). Tallin Manual 2.0 on the International Law Applicable to Cyber Operations. Newport, Rhode Island: Cambridge University Press.

Galindo Camacho, M. (2016). *Teoría de la administración pública*. Editorial Purrúa.

Hernández, Y. S., Llanes Font, M., & Suárez Benítez, M. Á. (2020). *Transformación digital en la administración pública*. Avances, 22(4), 1-9.

Guzan, B., Waever, O., & De Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.

Kello, L. (2013). The meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, 38(2), 7-40.

Leyva-Méndez, A. E. (2021). Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano. *Polo del Conocimiento*, *6*(3), 1229-1250.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2021). *Guía para la gestión y clasificación de incidentes de seguridad de la información* (Versión 4). Bogotá, Colombia.

Rentería Echeverry, F. A. (2014). *Inicio y Evolución de la Seguridad Informática en el Mundo* (Bachelor's thesis, Universidad Piloto de Colombia).

Observatorio del Sector Público**.** (2017). *Ciberseguridad en el Sector Público. Documento de conclusiones.* Informática El Corte Inglés. España. Disponible en https://www.ospi.es/export/sites/ospi/documents/informes/Informe_ciberseguridad.pdf

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2024). *Capacidades del sector público para la transformación digital*. Este capítulo evalúa las capacidades institucionales existentes para apoyar las políticas de gobierno digital en América Latina y el Caribe (LAC). https://www.oecd-ilibrary.org/docserver/509d733a-es.pdf

Sánchez Vera, F., Martínez Guirao, J. E., & Téllez Infantes, A. (2022). La seguridad en el ciberespacio desde una perspectiva sociocultural. *Methaodos. Revista de Ciencias Sociales*, 10(2), 243-258. http://dx.doi.org/10.17502/mrcs.v10i2.577

Torres Melo, J., & Santander, J. (2013). *Introducción a las políticas públicas*. Bogotá.

Vega Briceño, E. (2021). *Seguridad de la información*. Área de Innovación y Desarrollo, S.L. https://doi.org/10.17993/tics.2021.4

Von Solms, R. and Van Niekerk, J. (2013) From Information Security to Cyber Security. Computers & Security, 38, 97-102.

F. Bélanger and L. Carter, “The Effects of the Digital Divide on e-Government: An Empirical Evaluation,” Proceedings of the 39th Hawaii International Conference on System Sciences, Vol. 4, 2006, pp. 1-7.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2012). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

Ransbotham, S., Mitra, S., & Ramsey, J. (2017). "Are Markets for Vulnerabilities Effective?" *MIS Quarterly*, 41(3), 703-713. DOI: 10.25300/MISQ/2017/41.3.03.

Organisation for Economic Cooperation and Development (OECD). (2019). *The Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security*.

Schneier, B. (2010). *El espejismo de la seguridad*. Recuperado de http://www.ted.com/talks/lang/eng/bruce_schneier.html

e-Estonia. (2020). "Estonia’s Cyber Security Strategy 2019-2022." Disponible en: [e-Estonia](https://e-estonia.com/solutions/security-and-safety/cyber-security/)

European Commission. (2019). "The EU Security Union Strategy." Disponible en: [European Commission](https://commission.europa.eu/projects/cybersecurity-programme_en)

International Telecommunication Union. (2020). "Global Cybersecurity Index." Disponible en: [ITU](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx)

OECD. (2015). "Digital Security Risk Management for Economic and Social Prosperity." OECD Publishing.

Vercelli, A. H. (2015). Repensando las regulaciones de Internet: análisis de las tensiones políticas entre no-regular y re-regular la red de redes.

World Economic Forum. (2018). "The Global Risks Report." Disponible en: [World Economic Forum](https://www.weforum.org/reports/the-global-risks-report-2018)

https://www.ccit.org.co/estudios/seguimiento-a-documentos-conpes-sector-tic-julio-de-2022/
https://www.csirtasobancaria.com/

https://commission.europa.eu/projects/cybersecurity-programme_en

European Commission. (2019). "The EU Security Union Strategy". Disponible en: European Commission

World Economic Forum. (2018). "The Global Risks Report." Disponible en: [World Economic Forum](https://www.weforum.org/reports/the-global-risks-report-2018)

https://www.mindef.gob.cl/estrategia-nacional-de-ciberseguridad/

https://www.gob.pe/institucion/pcm/organismos-y-unidades/377-comite-nacional-de-ciberseguridad-conaciber

https://www.piranirisk.com/es/blog/posibles-causas-ataque-cibernetico-ifx-networks

https://www.javeriana.edu.co/pesquisa/ciberataque-ifx-networks-colombia/

Estado del Arte

Bekerman, U. (2020). Algunas medidas de ciberseguridad en Argentina, Colombia, Cuba, Egipto, Francia, Grecia, Japón, Singapur y Turquía. Diario DPI Suplemento Derecho y Tecnologías, 66, 07.08.2020.

Camilo Cetina. (2020). La aceleración digital de los gobiernos e implicaciones de política pública. Dirección de Innovación Digital del Estado de CAF.

Campos Ramírez, J. F. (2017). Seguridad de la información en el sector público colombiano. Universidad Piloto de Colombia.

Frey, K. (2005). Gobernanza electrónica urbana e inclusión digital: experiencias en ciudades europeas y brasileñas. Nueva Sociedad, 196, 109.

García Alonso, R., Caldas, J. M., Dávila, D. E., & Thoene, U. (2020). Políticas públicas de inclusión digital en Colombia: Una evaluación del Plan Vive Digital I (2010-2014). Revista de Estudios Sociales, 41(7), 13.

Instituto de Ciencias Aplicadas y Tecnología (ICAT). (2022). *Vigilancia tecnológica en ciberseguridad*. Universidad Nacional Autónoma de México (UNAM). Recuperado de https://www.icat.unam.mx/wp-content/uploads/2022/09/Vigilancia_Tecnologica_en_Ciberseguridad_Boletin.pdf

Martínez-Coral, P. (2017). "Seguro mató a confianza": Desafíos para la adopción del gobierno digital en Colombia. Revista Inclusión & Desarrollo, 5(1), 63-72.

MinTIC. (2017). La OCDE dará rutas de acción para la evolución hacia un Gobierno Digital. Ministerio de Tecnologías de la Información y las Comunicaciones.

MinTIC. (2021). Fortalecimiento y Actualización de la Política de Gobierno Digital del Estado Colombiano.

Moreno Hernández, E. C. (2021). Análisis de la implementación de la política de gobierno digital en el MADS y su contribución a la transformación digital para el acceso a la información pública (2018–2020).

OECD. (2017). Evaluación de Impacto del Gobierno Digital en Colombia: Hacia una Nueva Metodología. Éditions OCDE, París.

Ospina, J., & Zambrano, L. (2022). Gobierno digital e inteligencia artificial: Una mirada al caso colombiano. Administración & Desarrollo, 53(1), 1-34.

Ramírez Camargo, E. A., & Rincón Pinzón, M. A. (2022). La importancia de la seguridad de la información en el sector público en Colombia. Revista Ibérica de Sistemas y Tecnologías de Información, (46), 87-99.

Salvador Serna, M. (2021). Inteligencia artificial y gobernanza de datos en las administraciones públicas: Reflexiones y evidencias para su desarrollo. Gestión y Análisis de Políticas Públicas, 26, 20-32.

Tabarquino Muñoz, R. A. (2022). Consolidación legal y regulatoria del servicio público de las comunicaciones en Colombia 1847-2020. Revista Tendencias, XXIII(1), 395-411.

Toro-García, A. F., Gutiérrez-Vargas, C. C., & Correa-Ortiz, L. C. (2020). Estrategia de gobierno digital para la construcción de un Estado transparente y proactivo. Revista CEA, 12(22), 77-89.

Análisis

Alaminos Fernández, A. F. (2023). *Introducción a la minería de texto y análisis de sentimiento con R*

Policía Nacional de Colombia, Centro Cibernético Policial. (2020). *Balance Anual de Cibercrimen 2020.* Policía Nacional de Colombia.

Policía Nacional de Colombia, Centro Cibernético Policial. (2022*). Balance Anual de Cibercrimen 2022.* Policía Nacional de Colombia.

Policía Nacional de Colombia, Dirección de Investigación Criminal e Interpol. (2023). *Balance de Ciberseguridad 2023*. Centro Cibernético Policial

Cuesta Castillo, D. M. (2022). *Análisis de la Seguridad de la Información en Entidades Públicas de Colombia: 2020-2022*. Universidad Militar Nueva Granada.

Departamento Nacional de Planeación. (2020). *Política Nacional de Confianza y Seguridad Digital (CONPES 3995).* República de Colombia.

Díaz, M. R. O., & Rangel, P. E. S. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Criminalidad,* 62(2), 199-217

Quintero Agudelo, Y. (2014). *Seguridad y Ciberdefensa en Colombia. Universidad Piloto de Colombia.*

TicTac. (2021). *Evaluación, retos y amenazas a la ciberseguridad. Tanque de Análisis y Creatividad de las TIC (TicTac).* Cámara Colombiana de Informática y Telecomunicaciones (CCIT).

Viegas, F., & Wattenberg, M. (2008). *The word cloud: A new way to visualize text*. En *Proceedings of the 2008 IEEE International Conference on Information Visualization* (pp. 1-6). IEEE.

Alaminos, A. (2023). *Manual de análisis de datos textuales: Aplicaciones con R*. Universidad de Alicante.

Bardin, L. (2002). *Análisis de contenido*. Ediciones Akal.

Barros, C., Campero, C., & Cabello, J. (2016). Gobernanza digital. En CEPAL, *Gobernanza digital e interoperabilidad gubernamental*.

Berríos, D., & Gómez, F. (2017). Confianza digital y su impacto en la participación ciudadana. *Revista de Gobierno Electrónico*, 16(4), 199–212.

Cabrera, J., & Mendoza, F. (2021). La confianza cero como modelo de seguridad en el gobierno digital. *Revista de Tecnología y Política Pública*, 35(4), 214–228.

Candau, J. (2021). *Ciberseguridad. Evolución y tendencias*. Documento Marco, 11/2021.

Cámara Colombiana de Informática y Telecomunicaciones. (2023). *Impacto económico de la ciberseguridad en Colombia*. https://ccit.org.co/estudios

Cámara Colombiana de Informática y Telecomunicaciones. (2024). *Informe de percepción sobre ciberseguridad en el sector público*. https://ccit.org.co/encuesta-percepcion-2024

Cárdenas, M. (2010). Desarrollo de capacidades estatales para gobiernos locales. *Revista INNOVAR*, 20(38), 187–202.

Castro, D. (2017). La ciberseguridad en el contexto gubernamental. *Tecnología y Sociedad*, 45(2), 56–68.

CEPAL. (2021). *Gobernanza digital e interoperabilidad gubernamental*. https://www.cepal.org/es/publicaciones/47608

Centro de Respuesta a Incidentes Cibernéticos del Gobierno de Colombia (CSIRT Gobierno). (2023). *Reporte de incidentes cibernéticos 2022*. https://csirtgobierno.gov.co/estadisticas

Centro de Respuesta a Incidentes Cibernéticos del Gobierno de Colombia (CSIRT Gobierno). (2024). *Alertas tempranas primer trimestre 2024*. https://csirtgobierno.gov.co/alertas

Cienfuegos, I. (2021). Aportes de la gobernanza digital para una gestión pública local inteligente. *Dialnet*. https://dialnet.unirioja.es/servlet/articulo?codigo=7983855

Cienfuegos Spikin, I. (2012). Teoría de las decisiones y gestión del riesgo en organizaciones públicas. *Revista de Gestión Pública*, 1(1), 45–68.

Contraloría General de la República. (2023). *Informe de vigilancia a la gestión de entidades públicas en ciberseguridad*. https://www.contraloria.gov.co/resultados-investigaciones

Criado, J. I. (Coord.). (2021). *Gobierno abierto, innovación pública y colaboración ciudadana*. Instituto Nacional de Administración Pública.

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

Díaz, A., & Sánchez, P. (2019). La ciberseguridad pública en América Latina: Retos y perspectivas. Universidad de Buenos Aires.

Flick, U. (2015). *Introducción a la investigación cualitativa* (5.ª ed.). Morata.

Foro Económico BPO. (2024). *Impacto cibernético en el sector público colombiano: Primer semestre 2024*. https://forobpo.org/informe-ciberataques

Galindo, O. A. (2020). Transformación digital: una agenda de oportunidades. *Revista Perspectiva Empresarial*, 7(2), 12–25.

Garza, A., & Silva, M. (2020). Implementación de Zero Trust en las instituciones públicas. *Revista de Seguridad Cibernética*, 13(1), 78–92.

Gil-García, J. R. (2007). E-Government and public administration: A brief analysis. *Journal of Government Information*, 34(1), 17–38.

Gómez, S. (2020). *Confianza digital y privacidad en la administración pública digital*. Editorial Universidad Autónoma de Madrid.

Guijarro-Rodríguez, A. A., et al. (2018). Defensa en profundidad aplicado a un entorno empresarial. *Revista Espacios*, 39(42), 25–34.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill.

López, A., & Castro, J. (2020). *Estrategias de defensa en profundidad en el sector público*. Editorial Universidad Nacional de Colombia.

López, R., & Martínez, L. (2016). Ciberseguridad pública: Políticas y estrategias en el contexto gubernamental. *Revista de Seguridad Digital*, 22(3), 115–128.

Ministerio de Defensa Nacional. (2024). *Boletín de cifras de criminalidad 2023–2024*. https://www.mindefensa.gov.co/ir/publicaciones/estadisticas

Ministerio de Defensa Nacional. (2024). *Plan anual de inversiones en ciberseguridad 2024*. https://www.mindefensa.gov.co/ir/plan-ciberseguridad-2024

Miller, G. J., & Whicker, M. L. (Eds.). (1999). *Handbook of research methods in public administration*. Marcel Dekker.

Muñoz, M., & Ríos, L. (2018). *La administración pública en la era digital*. Editorial Universidad de Chile.

Navarrete Yáñez, B., et al. (2022). Confianza institucional y evaluación ciudadana del acceso a información. *Revista Iberoamericana de Estudios Municipales*, 13(26), 1–20.

Patashnik, E. M., & Zelizer, J. E. (2009). When policy does not remake politics: The limits of policy feedback. *SSRN*. https://ssrn.com/abstract=1449996

Pérez, L., & Hernández, C. (2020). *Fortalecimiento de la ciberresiliencia en el sector público*. Editorial Tecnológica.

Policía Nacional de Colombia. (2022). *Informe anual de cibercriminalidad 2021*. https://www.policia.gov.co/noticia/estadisticas-delitos-informaticos

Ramírez, J. (2019). Ciberresiliencia: Preparación y recuperación ante ciberataques en las instituciones públicas. *Revista de Ciberseguridad*, 25(3), 124–139.

Real Instituto Elcano. (2023). *La ciberresiliencia: Entre la ciberseguridad y la resiliencia*. https://www.realinstitutoelcano.org/informes/la-ciberresiliencia/

Rodríguez, M. P. (2021). Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano. *Revista UIS Ingenierías*, 20(3), 45–60. https://revistas.uis.edu.co/index.php/revistauisingenierias/article/view/11485

Sánchez, R., & Moreno, F. (2018). Defensa en profundidad: Estrategias de seguridad cibernética en la administración pública. *Revista de Ciberseguridad*, 24(1), 58–73.

Sanabria, P., & Leyva-Méndez, F. (2023). *El Estado del Estado en Colombia: Radiografía institucional de un modelo híbrido*. Fundación Konrad Adenauer & Universidad Externado de Colombia.

Schneier, B. (2010). *Liars and outliers: Enabling the trust that society needs to thrive*. Wiley.

Silva, D., & González, E. (2020). *Ciberseguridad: La protección de la infraestructura digital pública*. Editorial Universidad Autónoma de Madrid.

Subirats, J. (2012). *Análisis e intervención en las políticas públicas*. Ariel.

Suárez Vásquez, E. C. (2022). Los retos entorno a la confianza y la seguridad digital en Colombia. *Derecho & Negocios*. Universidad Externado de Colombia. https://dernegocios.uexternado.edu.co/...

Tovar, C. (2017). *La confianza institucional en la administración pública digital*. Editorial Universidad Nacional de Colombia.

Viegas, F. B., & Wattenberg, M. (2008). Tag clouds and the case for vernacular visualization. *Interactions*, 15(4), 49–52. https://doi.org/10.1145/1374489.1374501

Zamorín, M., & González, J. (2018). Confianza institucional y su impacto en la gestión pública. *Revista de Ciencias Sociales*, 31(2), 57–70.