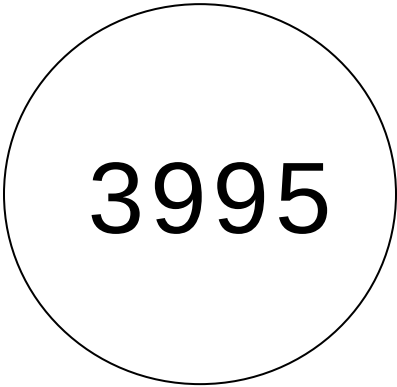


Documento CONPES

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL
REPÚBLICA DE COLOMBIA
DEPARTAMENTO NACIONAL DE PLANEACIÓN



3995

POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL

Departamento Nacional de Planeación
Ministerio de Tecnologías de la Información y las Comunicaciones
Departamento Administrativo de la Presidencia de la República

Versión aprobada

Bogotá, D.C., 01 de julio de 2020

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL CONPES

Iván Duque Márquez
Presidente de la República

Marta Lucía Ramirez Blanco
Vicepresidenta de la República

Alicia Victoria Arango Olmos
Ministra del Interior

Claudia Blum de Barberi
Ministra de Relaciones Exteriores

Alberto Carrasquilla Barrera
Ministro de Hacienda y Crédito Público

Margarita Leonor Cabello Blanco
Ministra de Justicia y del Derecho

Carlos Holmes Trujillo García
Ministro de Defensa Nacional

Rodolfo Enrique Zea Navarro
Ministro de Agricultura y Desarrollo Rural

Fernando Ruíz Gómez
Ministro de Salud y Protección Social

Ángel Custodio Cabrera Báez
Ministro de Trabajo

Carolina Rojas Hayes
Ministra de Minas y Energía (E)

José Manuel Restrepo Abondano
Ministro de Comercio, Industria y Turismo

María Victoria Angulo González
Ministra de Educación Nacional

Ricardo José Lozano Picón¹
Ministro de Ambiente y Desarrollo Sostenible

Jonathan Tybalt Malagón González
Ministro de Vivienda, Ciudad y Territorio

Karen Abudinen Abuchaibe
Ministra de Tecnologías de la Información y las Comunicaciones

Ángela María Orozco Gómez
Ministra de Transporte

Carmen Inés Vásquez Camacho
Ministra de Cultura

Ernesto Lucena Barrero
Ministro del Deporte

Mabel Gisela Torres Torres
Ministra de Ciencia, Tecnología e Innovación

Luis Alberto Rodríguez Ospino
Director General del Departamento Nacional de Planeación

Daniel Gómez Gaviria
Subdirector General Sectorial

Amparo García Montaña
Subdirectora General Territorial

¹ Estos miembros del CONPES no participaron en la sesión de aprobación del presente documento CONPES.

Resumen ejecutivo

La creciente participación de ciudadanos en el entorno digital², la alta dependencia de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) traen consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital, lo cual exige que el país cuente con suficientes capacidades para su gestión adecuada y oportuna. Las amenazas, los ataques e incidentes de seguridad digital cada día son más sofisticados y complejos e implican graves consecuencias de tipo económico o social. Por ejemplo, según estimaciones de Accenture, el costo para los negocios derivado del impacto de los ciberdelitos ha incrementado en un 72 % entre 2014 y 2019 (Accenture, 2019). Esto conlleva al deterioro de la confianza digital y la desaceleración del desarrollo de los países en el futuro digital³. Debido a lo anterior, los gobiernos alrededor del mundo han venido atendiendo los nuevos retos para la detección y manejo de amenazas, ataques e incidentes cibernéticos mediante la formulación y actualización de estrategias o políticas relacionadas con la seguridad digital.

Lo anterior exige acciones de política para que las múltiples partes interesadas⁴ en Colombia puedan adelantar sus actividades socioeconómicas en dicho entorno de manera segura y confiable.

Así las cosas, el presente documento CONPES formula una política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital. Para alcanzar este objetivo, en primer lugar, se fortalecerán las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; en segundo lugar, se actualizará el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

² En el mundo, más del 50 % de la población está en línea y cerca de 1 millón de personas cada día comienzan a usar internet. En Colombia el número total de personas de 5 años o más que usan Internet aumentó un 29 % entre 2014 y 2018.

³ Según el FEM el futuro digital debe ser inclusivo, siendo la confianza la base de todas y cada una de las interacciones en dicho futuro. Se necesita un mundo digital sostenible, en términos sociales, económicos y medioambientales (Foro Económico Mundial - FEM, 2018).

⁴ Según el Documento CONPES 3854 *Política Nacional de Seguridad Digital* aprobado en 2016, las múltiples partes interesadas son: "el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades".

Teniendo en cuenta que el tema abordado es de carácter transversal a todos los sectores del país, se requerirá de la participación de diferentes entidades e instancias tales como la Consejería Presidencial para Asuntos Económicos y Transformación Digital, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional y el Departamento Nacional de Planeación, entre otras. El logro de las condiciones descritas se dará en el período comprendido entre 2020 y 2022, con una inversión total aproximada de 8.342 millones de pesos.

Clasificación: F52, H11, H12, L86.

Palabras clave: confianza digital, seguridad digital, ciberdefensa, ciberseguridad, ciberterrorismo, ciberdelito, cibercrimen, ciberinteligencia, gestión de riesgos, entorno digital, economía digital, prosperidad económica y social, amenazas cibernéticas, capacidades, coordinación, fortalecimiento, liderazgo, infraestructuras críticas cibernéticas, nacionales, actividades y funciones críticas, ciberespacio.

TABLA DE CONTENIDO

1. INTRODUCCIÓN	8
2. ANTECEDENTES Y JUSTIFICACIÓN	10
2.1. Antecedentes.....	10
2.2. Justificación.....	14
3. MARCO CONCEPTUAL.....	15
4. DIAGNÓSTICO.....	16
4.1. Debilidades en las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado.....	18
4.2. El marco de gobernanza en materia de seguridad digital no ha alcanzado un grado de desarrollo adecuado	24
4.3. Se requiere la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital con énfasis en nuevas tecnologías	26
5. DEFINICIÓN DE LA POLÍTICA	27
5.1. Objetivo general	27
5.2. Objetivos específicos	27
5.3. Plan de acción	27
5.3.1. Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país	27
5.3.2. Actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y mejorar el avance en seguridad digital del país.....	34
5.3.3. Analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías para preparar al país a los desafíos de la 4RI	37
5.4. Seguimiento	38
5.5. Financiamiento	38
6. RECOMENDACIONES.....	40
GLOSARIO.....	42
ANEXOS	45
BIBLIOGRAFÍA	49

ÍNDICE DE GRÁFICOS

Gráfico 1. Panorama del índice de confianza digital para los países evaluados	18
Gráfico 2. Resultados del <i>Children Online Security Index 2020 para Colombia</i>	20
Gráfico 3. Resultados del <i>National Cyber Security Index 2019</i> – Porcentaje de avance por indicador.....	23

ÍNDICE DE FIGURAS

Figura 1. Implementación de políticas y estrategias desde el Gobierno nacional para brindar seguridad y defensa en el ciberespacio.....	10
---	----

ÍNDICE DE TABLAS

Tabla 1. Índice de Confianza Digital para Colombia por parámetro de evaluación.....	17
Tabla 2. Cronograma de seguimiento.....	38
Tabla 3. Financiamiento estimado indicativo de la política	39

SIGLAS Y ABREVIACIONES

4RI	Cuarta Revolución Industrial
ColCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia
CONPES	Consejo Nacional de Política Económica y Social de Colombia
COSI	Índice de Protección Infantil en Línea (en inglés, <i>Children Online Safety Index</i>)
CRC	Comisión de Regulación de Comunicaciones
CSIRT	Equipos de respuestas ante incidentes de seguridad (en inglés, <i>Computer Security Incident Response Team</i>)
CSIRT Gobierno	CSIRT del Gobierno nacional
CSIRT PONAL	CSIRT de la Policía Nacional de Colombia
FEM	Foro Económico Mundial
IoT	Internet de las Cosas (en inglés <i>Internet of Things</i>)
NICE	Iniciativa Nacional de Educación en Seguridad Cibernética
NCSI	Índice de Ciberseguridad Nacional (en inglés, <i>National Cyber Security Index</i>)
OCDE	Organización para la Cooperación y Desarrollo Económicos
PAS	Plan de Acción y Seguimiento
SENA	Servicio Nacional de Aprendizaje
SIC	Superintendencia de Industria y Comercio
TIC	Tecnologías de la Información y las Comunicaciones
UIT	Unión Internacional de Telecomunicaciones

1. INTRODUCCIÓN

El entorno digital es un escenario en el que globalmente se desarrollan cada vez más todo tipo de actividades socioeconómicas. Esto expone tanto a las personas como a las mismas organizaciones a amenazas cibernéticas por parte de delincuentes que aprovechan el creciente intercambio de información. En consecuencia, el desarrollo de una economía digital, para cualquier país, requiere la construcción de un entorno digital seguro, como elemento clave para que sea confiable, y que esté acorde con el aumento y dinamismo de las actividades digitales.

La Cuarta Revolución Industrial (4RI)⁵ está impulsando rápidamente la transformación de todos los sectores de la economía. Para 2022, se estima que digitalizará más del 60 % del PIB mundial y que el 70 % del nuevo valor creado en la economía durante la próxima década se basará en plataformas habilitadas digitalmente (Foro Económico Mundial, 2019). Por otro lado, según el estudio *Securing the Digital Economy*, el nivel de dependencia a Internet se ha incrementado de un 23 % en 2008 a un 100 % en 2018, tal como lo reporta el 68 % de los CEOs de las empresas que hicieron parte del estudio. Sin embargo, estos CEOs reconocen que el nivel de confianza en Internet está en decremento. Actualmente, para el nivel que se presenta de dependencia a Internet, el nivel de confianza en Internet se considera bastante bajo siendo apenas del 30 % y se estima que para 2023 caerá al 25 % si nada cambia para mejorarlo. Lo anterior genera grandes retos al respecto, ya que se asume que en los próximos cinco años el nivel de dependencia a Internet se mantendrá en el 100 % (Accenture, 2019).

A través del Índice de Evolución Digital 2017 (Chakravorti & Ravi, 2017), se analizan los impulsores que rigen la digitalización de un país, entre ellos, el entorno de confianza digital. Este índice mide, entre otros, la evolución en la construcción de confianza digital y la efectividad de la seguridad digital. Para el caso Colombia, este índice muestra que en relación a la evolución del entorno de confianza digital, el país ocupa el puesto 32 entre un total de 42 países, con un puntaje de 2,33, ubicándose por debajo del promedio global (2,78 puntos). Si se tiene en cuenta que sin confianza digital, las personas no proporcionarán información, no se intercambiarán bienes o servicios en línea y no se darían interacciones con la información proporcionada (Foro Económico Mundial - FEM, 2018), entonces, que el

⁵ La 4RI se caracteriza por la aparición de nuevas tecnologías que están fusionando el mundo físico, digital y biológico (Schwab, 2016).

país cuente con un entorno de confianza digital por debajo del promedio, no habilita el intercambio efectivo de información, bienes y servicios en línea.

Siendo entonces la confianza y la seguridad digital una preocupación, en Colombia en el año 2011 se formuló el Documento CONPES 3701 *Lineamientos de Política para Ciberseguridad y Ciberdefensa*⁶ y posteriormente en el año 2016 el Documento CONPES 3854 *Política Nacional de Seguridad Digital*⁷, estos dos documentos procuraron el fortalecimiento y generación de capacidades en el Gobierno nacional, con un enfoque de gestión de riesgos, para brindar seguridad y defensa a los ciudadanos, así como a las instituciones en el ciberespacio. Aunque estas políticas permitieron en su momento que el país avanzara en materia de seguridad digital, cabe anotar que no se logró un avance considerable en cuestiones de confianza digital. Esto debido a que no se involucró en mayor medida a todas las múltiples partes interesadas⁸ relacionadas con la seguridad digital, más allá del Gobierno nacional, con el fin de generar confianza digital.

De esta manera se debe apuntar a que existan las medidas suficientes, tanto en el fortalecimiento de la seguridad, como en la generación de la confianza digital, respecto a una adecuada anticipación, gestión de riesgos, atención oportuna y defensa ante las amenazas existentes en el entorno digital, dentro de un marco de gobernanza nacional eficiente, acorde con las necesidades actuales y en constante desarrollo, en el que se pueda materializar rápidamente la confianza y la seguridad digital ante la aparición de nuevas tecnologías.

Finalmente, el presente documento está organizado en seis secciones incluyendo esta introducción. La segunda sección presenta los antecedentes de política pública, y la justificación por la cual se desarrolla esta política. La tercera sección establece el marco conceptual que permitirá el entendimiento de los conceptos clave para el desarrollo de esta política. Posteriormente la cuarta sección presenta y caracteriza la problemática que se busca solucionar. La quinta sección define la política nacional de confianza y seguridad digital, el cronograma de seguimiento a la implementación de sus acciones y su esquema de financiamiento. Por último, la sexta sección presenta las recomendaciones al Consejo

⁶ Disponible en <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>.

⁷ Disponible en <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>.

⁸ Según el Documento CONPES 3854 aprobado en 2016, las múltiples partes interesadas son: el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la fuerza pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades.

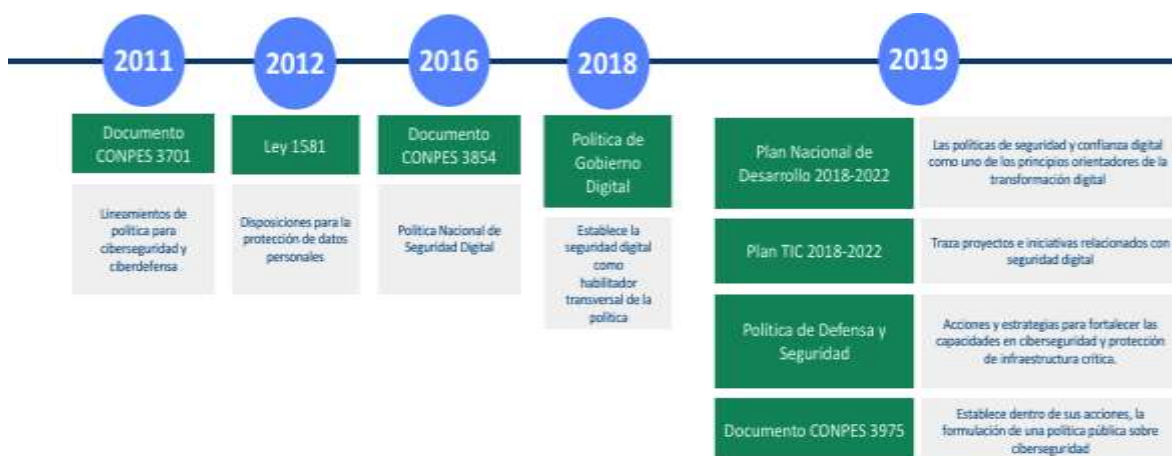
Nacional de Política Económica y Social (CONPES) para la implementación de la presente política.

2. ANTECEDENTES Y JUSTIFICACIÓN

2.1. Antecedentes

En esta sección se mostrará cómo en Colombia se han implementado las políticas y estrategias desde el Gobierno nacional para brindar seguridad y defensa en el ciberespacio, con un enfoque de gestión de riesgos (Figura 1). No obstante, dado el rápido dinamismo de la transformación digital, estas estrategias actualmente tienen una visión limitada en materia de confianza y seguridad digital.

Figura 1. Implementación de políticas y estrategias desde el Gobierno nacional para brindar seguridad y defensa en el ciberespacio



Fuente: Elaboración DNP, 2020.

En primera instancia, en Colombia se expidió en 2011 el Documento CONPES 3701 *Lineamientos de Política para Ciberseguridad y Ciberdefensa*, cuyo objetivo era fortalecer las capacidades del Estado para enfrentar las amenazas en el ámbito cibernético, creando así el ambiente y las condiciones necesarias para brindar protección en el ciberespacio. En este documento CONPES se determinaron estrategias para enfrentar las amenazas que atentan contra la seguridad y defensa del Estado relacionadas con la ciberseguridad y la ciberdefensa, tales como la creación del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), el Centro Cibernético Policial, CECIP y el Comando Conjunto Cibernético – CCOCI, bajo un modelo de coordinación intersectorial. Otra de las estrategias se enfocó en la capacitación especializada en ciberseguridad y ciberdefensa para las instituciones del Gobierno nacional y el fortalecimiento de la legislación y la cooperación

internacional en materia de ciberseguridad y ciberdefensa. Sin embargo, el enfoque de esta política se orientó mayoritariamente en el desarrollo de capacidades gubernamentales en ciberdefensa ante amenazas en materia de seguridad digital y no atendió el desarrollo de capacidades para ciudadanos u otros sectores.

Uno de los grandes avances en lo que respecta a la generación de confianza digital, se dio a través de la Ley Estatutaria 1581 de 2012⁹, cuyo objeto es desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar su información personal. En esta misma línea, se desarrolló un marco jurídico que incluye el reconocimiento de los datos e información personal como bien jurídico tutelado.

Ante la rápida evolución de las amenazas en seguridad digital, la estrategia nacional planteada en 2011 se revisó y se expidió en el año 2016 el Documento CONPES 3854 *Política Nacional de Seguridad Digital*, cuyo objetivo era fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital. Para esto, el gran aporte de esta política fue el desarrollo de estrategias que establecieron un marco institucional para la seguridad digital con un enfoque de gestión de riesgos, es decir, con una visión preventiva antes que reactiva ante las posibles amenazas en seguridad digital. También se crearon las condiciones que permitieran que las múltiples partes interesadas gestionaran el riesgo de seguridad digital, para fortalecer la seguridad de los individuos y del Estado, así como la defensa y la soberanía nacional en el entorno digital. Adicionalmente se generaron mecanismos estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital a nivel nacional e internacional y se crea la figura de Coordinador Nacional de Seguridad Digital. A pesar de lo anterior, estas políticas se dirigieron principalmente al Gobierno nacional, siendo baja la gestión frente a convenios y acuerdos de cooperación e intercambio de información con las múltiples partes interesadas y poco avance respecto a los estudios de viabilidad para la creación de nuevas instancias, en temas relacionados con la defensa y seguridad nacional en el entorno digital.

En el año 2018, se expidió el Decreto 1008¹⁰ que establece los lineamientos generales de la Política de Gobierno Digital. Esta política establece que la seguridad de la información es uno de los habilitadores transversales, es decir, que es uno de elementos fundamentales que permiten el desarrollo del gobierno digital. Desde lo relativo a la confianza digital, esta política también busca preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Para esto, dentro del *Manual de Gobierno Digital*, expedido por el Ministerio

⁹ Por la cual se dictan disposiciones generales para la protección de datos personales.

¹⁰ Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

de Tecnologías de la Información y las Comunicaciones, se establecen las pautas que deben aplicar las entidades públicas para la implementación de la Política de Gobierno Digital, entre ellas la aplicación del *Modelo de Seguridad y Privacidad de la Información (MSPI)*, cuyos lineamientos e indicadores permiten establecer el nivel de madurez en materia de seguridad digital para las entidades públicas. Además, dicho manual se encuentra alineado con las buenas prácticas en seguridad (Norma ISO /IEC 27001:2013¹¹), con la Ley 1581 de 2012 que trata de la Protección de Datos Personales y con la Ley 1712 de 2014 (conocida como ley de transparencia y del derecho de acceso a la información pública nacional) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2019). Las acciones de esta política se han centrado en las entidades del sector público y no involucran en mayor medida a los ciudadanos, ni a otros sectores del país directamente en el ámbito de seguridad de la información.

Por otro lado, mediante la Ley 1955 de 2019¹² se expidió el Plan Nacional de Desarrollo 2018–2022 *Pacto por Colombia, Pacto por la Equidad*. Específicamente, en el capítulo VII *Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento*, se busca que el país se encamine hacia una sociedad digital y hacia la industria 4.0, a través de la generación de confianza en el entorno digital y del desarrollo de estrategias sobre seguridad digital en los territorios. Por su parte en el capítulo I *Pacto por la legalidad: seguridad efectiva y justicia transparente para que todos vivamos con libertad y en democracia*, se establece como estrategia para promover el control integral marítimo, terrestre, aéreo, fluvial, espacial y ciberespacial que el Gobierno nacional fortalezca las capacidades de ciberseguridad y ciberdefensa para garantizar los intereses nacionales.

Adicionalmente, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales esta ley, a través del artículo 147 *Transformación Digital Pública*, establece la inclusión y actualización permanente de políticas

¹¹ La norma ISO /IEC 27001 es una familia de estándares que ayudan a las organizaciones en la administración de la seguridad de los activos tales como la información financiera, la propiedad intelectual, la información de los empleados o de aquella información de terceros de la cual la organización es garante. Esta familia de estándares provee los requerimientos que debe cumplir un *Sistema de Gestión de Seguridad de la Información* (<https://www.iso.org/isoiec-27001-information-security.html>).

¹² La Ley 1955 de 2019, por la cual se expide el *Plan Nacional de Desarrollo 2018-2022*, establece en su artículo 147 como uno de los principios de los proyectos estratégicos de transformación digital en la administración pública la “aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales”. Adicionalmente, el artículo 148 establece que la Política de Gobierno Digital como política de gestión y desempeño institucional, debe contemplar como acción prioritaria el aprovechamiento de tecnologías emergentes en el sector público, incremento de la confianza y seguridad digital y el fomento a la participación y la democracia por medios digitales (subrayado fuera de texto).

de seguridad y confianza digital, así como, la aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, como principios orientadores para los proyectos estratégicos de transformación digital.

Los mayores esfuerzos se han dado con políticas más recientes, que han dispuesto lineamientos respecto al fortalecimiento y la generación de capacidades en la sociedad colombiana, promoviendo la confianza digital y favoreciendo la inclusión y la competitividad en el futuro digital. Así en el año 2019, el Ministerio de Defensa Nacional formuló la *Política de Defensa y Seguridad para la legalidad, el emprendimiento y la equidad de Colombia*, que busca generar condiciones de seguridad y convivencia para preservar y potencializar los intereses nacionales, la independencia, soberanía e integridad del Estado. En el marco de esta política se establecen estrategias para fortalecer las capacidades militares de defensa en el ciberespacio y para liderar la lucha contra el delito transnacional, en áreas como la ciberseguridad y protección de infraestructura crítica.

De manera similar, el Ministerio de Tecnologías de la Información y las Comunicaciones presentó el Plan TIC 2018-2022 *El Futuro Digital es de Todos*, con los proyectos e iniciativas del sector TIC, varios de estos relacionados con seguridad digital. Entre ellos se pueden nombrar la generación de habilidades enfocada en igualdad de género, la creación y potencialización de emprendimientos femeninos, al igual que el fortalecimiento de las capacidades nacionales para impulsar la transformación digital del Estado.

Finalmente, en noviembre de 2019 se expidió el Documento CONPES 3795 *Política Nacional para la Transformación Digital e Inteligencia Artificial*¹³, cuyo objetivo es aumentar la generación de valor social y económico a través de la transformación digital del sector público y del sector privado, para que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la 4RI. Dicha política, además de ser el marco para temas digitales en el país, establece dentro de sus acciones, la formulación de una política pública sobre ciberseguridad para mejorar las capacidades del país al respecto.

Esto permite evidenciar que es hasta el año 2019 que han aparecido algunas políticas que contemplan de manera más amplia la generación de confianza digital y el mejoramiento de la seguridad digital con un enfoque hacia los ciudadanos y los demás sectores del país.

En relación con iniciativas de generación de capacidades en materia de seguridad digital, el Ministerio de Tecnologías de la Información y las Comunicaciones adelantó las iniciativas *Hacker Girls* con apoyo de la OEA y *Por TIC Mujer* la cual tiene como objetivo

¹³ Disponible en <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf>.

empoderar a las mujeres en el uso y apropiación de las TIC. Por otro lado, algunas específicas de formación en seguridad digital a jóvenes también con apoyo de la OEA, como el programa internacional Creación de una Trayectoria Profesional en Seguridad Digital, dirigido a jóvenes de escasos recursos económicos y estudiantes universitarios de ingeniería. A pesar del desarrollo de estas iniciativas, no se han realizado evaluaciones ni establecido condiciones para gestionar riesgos de seguridad digital de comunidades en condiciones especiales de vulnerabilidad, tales como los líderes sociales, lo cual podría limitar el ejercicio de sus derechos y de su actividad.

Concluyendo, de lo expuesto anteriormente, puede evidenciarse que las políticas públicas y estrategias relacionadas con seguridad digital, en mayor medida han propiciado el fortalecimiento y la generación de capacidades al interior del gobierno nacional, abarcando de manera tangencial a los ciudadanos y los demás sectores del país. Relativo a la generación de confianza digital, son pocas las disposiciones que abordan directamente este tema, por lo que es imperante el fortalecimiento de la confianza digital, favoreciendo la inclusión y la competitividad en el futuro digital.

2.2. Justificación

Como consecuencia de la rápida y significativa inserción de tecnologías en la vida cotidiana a nivel global, la protección de la privacidad y la seguridad de los datos se convierte en un problema crítico que es transversal a todos los sectores de la economía (Organización para la Cooperación y el Desarrollo Económicos - OCDE, 2019). Colombia no es ajena a esta realidad y esto implica la necesidad de adelantar todas las iniciativas que permitan asumir de manera responsable y oportuna este fenómeno, con el objetivo de generar confianza digital en el país.

Esta inserción de tecnologías obliga a los gobiernos a repensar e incluir temas relacionados con privacidad y la seguridad en todos los ámbitos de política. (Organización para la Cooperación y el Desarrollo Económicos - OCDE, 2019). Para Colombia se convierte en un asunto primordial garantizar de forma permanente la soberanía, la seguridad, la defensa del país y la de sus instituciones en el ciberespacio, así como la generación de confianza digital, tal como se expresa en la *Política de defensa y seguridad para la legalidad, el emprendimiento y la equidad de Colombia*. A esto se suma que cada vez son más los efectos en la sociedad colombiana que se derivan de un mayor nivel de exposición a los riesgos de seguridad digital por el uso incremental del entorno digital en el mundo y como efecto de la 4RI.

En conclusión es crucial que Colombia aumente tanto la confianza digital, así como que continúe mejorando la seguridad digital de modo que se maximice la generación de

valor socioeconómico a través del Internet y del ciberespacio (Banco Interamericano de Desarrollo - BID, 2016). Es por ello que adquiere relevancia ampliar el marco de acción en la formulación de políticas de seguridad cibernética, lo cual permite que los ciudadanos y los sectores económicos continúen con la adopción de estas políticas, y que se aproveche el enfoque basado en la gestión de riesgos. Esto debe lograr que participen activamente y con confianza de las buenas prácticas de seguridad, y que además conozcan los riesgos a los que pueden estar expuestos en un mundo cada vez más conectado y permeado por las tecnologías digitales en las actividades humanas.

3. MARCO CONCEPTUAL

Siendo la generación de confianza digital y la mejora de la seguridad digital las preocupaciones que aborda este documento, en la presente sección en primer lugar se desarrollará lo que debe entenderse por confianza digital y sus elementos constitutivos, para lo cual se propone usar varios elementos del marco de trabajo propuesto por el índice de Evolución Digital (Chakravorti & Ravi, 2017). Posteriormente se definirá lo que debe entenderse por *capacidades* en relación con seguridad digital, para lo cual se propone el uso de un marco de trabajo internacionalmente aceptado como lo es el de la Unión Internacional de Telecomunicaciones (UIT).

En términos generales la confianza puede entenderse como la probabilidad suficientemente alta de que un actor externo realice una acción que es beneficiosa (o al menos no perjudicial) para nosotros, de forma que se considere una cooperación con dicho actor (Gambetta, 2000). Debido a esto, la confianza es la base de todas las interacciones humanas.

Esto se refleja de igual manera en el entorno digital. Según el FEM, la confianza digital es la base de todas y cada una de las interacciones en el futuro digital (Foro Económico Mundial - FEM, 2018). A medida que una mayor actividad empresarial y gubernamental está mediada en línea en el futuro digital, la confianza digital y los niveles de confianza social se correlacionan cada vez más (Foro Económico Mundial - FEM, 2018). Por esto, sin confianza digital, las personas no proporcionarán información, no se intercambiarán bienes o servicios en línea y no se darían interacciones con la información proporcionada (Foro Económico Mundial - FEM, 2018).

Ahora bien, dado que en el entorno digital, la confianza digital puede percibirse de muchas maneras, es importante entenderla como la calidad de la interacción¹⁴ (Chakravorti

¹⁴ Los parámetros relacionados con calidad de la interacción para la confianza digital son: ambiente, experiencia, actitudes y comportamiento.

& Ravi, 2017), que se deriva de la actividad empresarial y gubernamental mediada en línea. La confianza digital se establece a través de la privacidad, la seguridad, la responsabilidad, la transparencia y las prácticas participativas efectivas y exigibles. (Foro Económico Mundial - FEM, 2018). En el Anexo B se presenta el detalle de los parámetros relacionados con calidad de la interacción para la confianza digital.

Por otro lado, la seguridad digital es la situación de normalidad y de tranquilidad en el entorno digital (Departamento Nacional de Planeación (DNP), 2016), y a su vez es uno de los elementos a través de los cuales se establece la confianza digital. Por tanto, este documento se enfocará en la seguridad digital, como elemento clave y necesario para aumentar y generar confianza digital, lo que redundará en el uso controlado, confiable y seguro de todo el entorno digital.

Por lo que en cuanto a capacidades en seguridad digital la UIT reconoce que los países están desarrollando capacidades para mitigar las posibles amenazas y vulnerabilidades que puedan ocurrir en el ciberespacio (Unión Internacional de Telecomunicaciones (UIT), 2018). Estas capacidades en seguridad digital son el conjunto de cualidades y aptitudes de un país que le permiten generar un entorno apropiado para abordar, generar conocimientos y aumentar el grado de desarrollo en materia de seguridad digital y pueden describirse teniendo en cuenta el marco de trabajo conceptual establecido por la UIT en el *Global Cybersecurity Index 2018*, que se enfoca en 5 tipos de capacidades (legal, técnica, organizacional, de investigación e innovación y de cooperación) que deben tenerse en cuenta al momento de pensar en una cultura nacional de ciberseguridad que permita abordar la 4RI y el futuro digital. (Unión Internacional de Telecomunicaciones (UIT), 2018).

Para efectos del presente documento, se entenderán que estas capacidades son un conjunto, que debe tratarse como un todo pues la mejora en las mismas debe ser integral y homogénea. Así que, al mencionarse el término *capacidades en seguridad digital*, se estará haciendo referencia a todas ellas. En el Anexo C se presenta el alcance de cada una de las capacidades aquí mencionadas.

4. DIAGNÓSTICO

El Informe Global de Riesgos 2019 presenta que el fraude de datos, los ciberataques y las vulnerabilidades tecnológicas, aparecen como grandes preocupaciones junto a eventos climáticos o desastres naturales, ubicándose dentro de los diez principales riesgos globales con mayor grado de probabilidad de ocurrencia (Foro Económico Mundial - FEM, 2019).

Por otro lado, según previsiones del *Centro para la Ciberseguridad* (C4C, por sus siglas en inglés) del FEM, la pérdida económica debida al delito cibernético puede alcanzar los 3

billones de dólares para el año 2020, y el 74 % de las empresas del mundo podrían ser hackeadas el próximo año¹⁵, mientras que para 2021 se estima que los daños ocasionados por los ciberdelitos alcancen los 6 trillones de dólares (Foro Económico Mundial [FEM], 2020).

A estas preocupaciones se suma el hecho que ciudadanos y hogares estén expuestos a amenazas en seguridad digital y que las empresas y entidades públicas no cuenten con medidas adecuadas en seguridad digital, de por sí debilita la confianza digital.

Según el reporte *Estado de Internet 2019* (Akamai, 2019), entre noviembre de 2017 y septiembre de 2019, en Colombia se originaron alrededor de 536 millones de ataques (contados entre *inicio de sesión malicioso* y *ataques a aplicaciones web*). Por su lado, en Estados Unidos se originaron alrededor de 26.800 millones, en Rusia 7.200 millones, en China 3.200 millones, en India 3.120 millones, en Alemania 2.330 millones y en Japón 920 millones de este mismo tipo de ataques. Si consideramos que el entorno digital es un entorno que nos conecta con el resto del mundo, entonces hay un gran número de ataques a los cuales se encuentran expuestos los ciudadanos en Colombia, no sólo por los ataques que se originen en el país, sino por la sumatoria de ataques que se originan globalmente. Indudablemente esto lleva a una sensación de desconfianza en el entorno digital.

Lo anterior se refleja en el Índice de Evolución Digital 2017 (Chakravorti & Ravi, 2017) que, entre otros, evalúa los parámetros relacionados con la confianza digital¹⁶ (ambiente, experiencia, actitudes y comportamiento) para establecer un grado de avance de esta, en los 42 países que hacen parte de este índice. En la (Tabla 1) se muestran los resultados para Colombia por cada parámetro de evaluación.

Tabla 1. Índice de Confianza Digital para Colombia por parámetro de evaluación

Parámetro	Puntaje	Promedio	Posición (entre 42 países)
Ambiente	2,33	2,78	32
Experiencia	1,53	2,42	34
Actitudes	1,96	2,47	42
Comportamiento	3,01	2,50	7

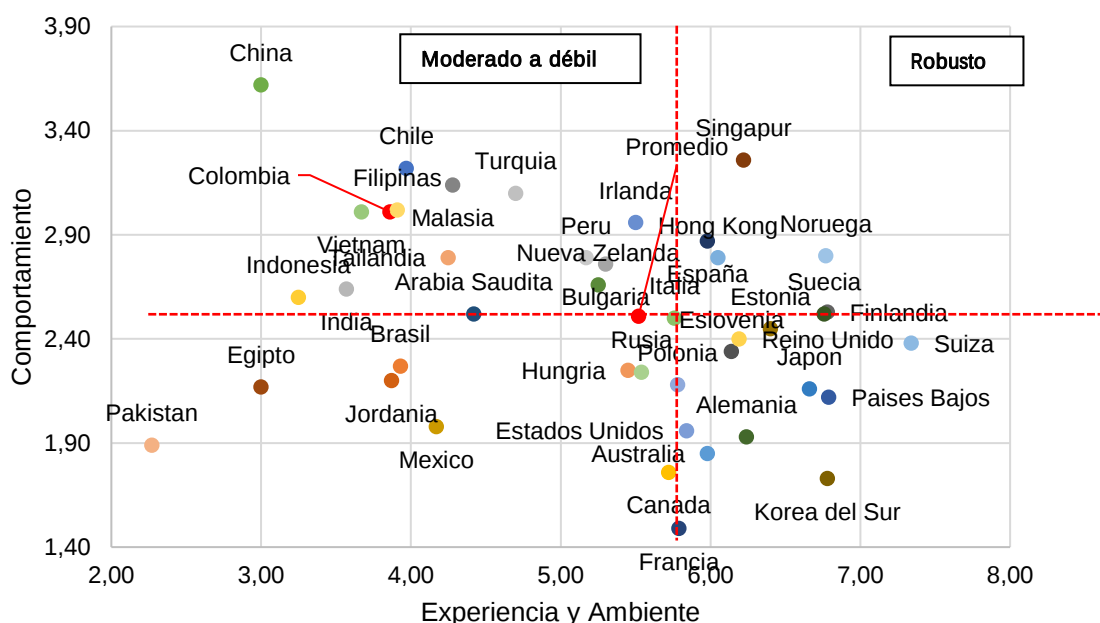
Fuente: Elaboración DNP con datos de (Chakravorti & Ravi, 2017).

¹⁵ <https://www.weforum.org/centre-for-cybersecurity/>.

¹⁶ Estos parámetros se encuentran definidos en el marco conceptual del presente documento.

Derivado de estos puntajes, los resultados de este índice arrojan que Colombia se encuentra en un estado moderado a débil frente al avance de la confianza digital (Chakravorti & Ravi, 2017) (Gráfico 1).

Gráfico 1. Panorama del índice de confianza digital para los países evaluados



Fuente: elaboración DNP con datos de Digital Planet 2017 (Chakravorti & Ravi, 2017).

Así encontramos que las preocupaciones en torno al avance de la confianza digital en el país no son menores y por tanto no pueden ser desconocidas por el Gobierno nacional.

4.1. Debilidades en las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado

El mundo se encuentra en el camino de la 4RI, que se caracteriza por la aparición de nuevas tecnologías que están fusionando el mundo físico, digital y biológico (Schwab, 2016), reestructurando todas las actividades humanas. Teniendo en cuenta que estas tecnologías se adoptan de diferente manera y velocidad en cada país dependiendo de sus capacidades, el desarrollo de la 4RI no es homogéneo a nivel global y conlleva el riesgo de ampliar las divisiones sociales entre países dependiendo de lo digitalizada que se encuentre su economía (Foro Económico Mundial, 2020).

Esta situación no es ajena a la seguridad digital, por lo que resulta relevante que cada país trabaje en el fortalecimiento de sus propias capacidades en esa materia, tanto para los ciudadanos, el sector público y el sector privado.

Respecto a los ciudadanos, en el ámbito nacional se dan casos que pueden generar diferencias sociales relacionadas con la seguridad digital. Si se observan las Bases del *Plan Nacional de Desarrollo 2018-2022: Pacto por Colombia Pacto por la Equidad*, la meta del cuatrienio para el *porcentaje de hogares con conexión a Internet suscrita* es del 70 % de hogares, teniendo como línea base el 50 % de hogares conectados. Para el cumplimiento de estas metas se adelantan iniciativas que se encuentran priorizadas en beneficio de la población pobre y vulnerable, o en zonas apartadas y que tienen una baja interacción con la tecnología y por ende menos capacidades en seguridad digital. Esto conlleva a que el número de hogares adicionales que se pretenden conectar, una vez entren al entorno digital, estarán expuestos en mayor medida y de manera inmediata a amenazas en seguridad digital. En ese sentido, si se generan capacidades en seguridad digital en esta población con condiciones especiales de vulnerabilidad, de manera temprana; se tendrá la posibilidad de que manejen mejor su exposición a las amenazas digitales.

Complementario a lo anterior, según datos de las pruebas PISA 2018 para los países OCDE, los estudiantes pasan alrededor de 3 horas diarias en línea entre semana y alrededor de 3,5 horas diarias en línea los fines de semana (Organización para la Cooperación y el Desarrollo Económicos - OCDE, 2018). Por tanto, es evidente que existe una ventana de riesgo cibernético para ellos. Al analizar el Índice de Protección Infantil en Línea en inglés Children Online Safety Index (*COSI*) que mide el nivel de seguridad en línea para los niños, en el ámbito global¹⁷. La medición 2020¹⁸ del COSI ubica a Colombia en el puesto 20 entre 30 países, con un puntaje general de 34 puntos por debajo del promedio global de 42 puntos en lo que a seguridad en línea para los niños se refiere (DQ Institute, 2020).

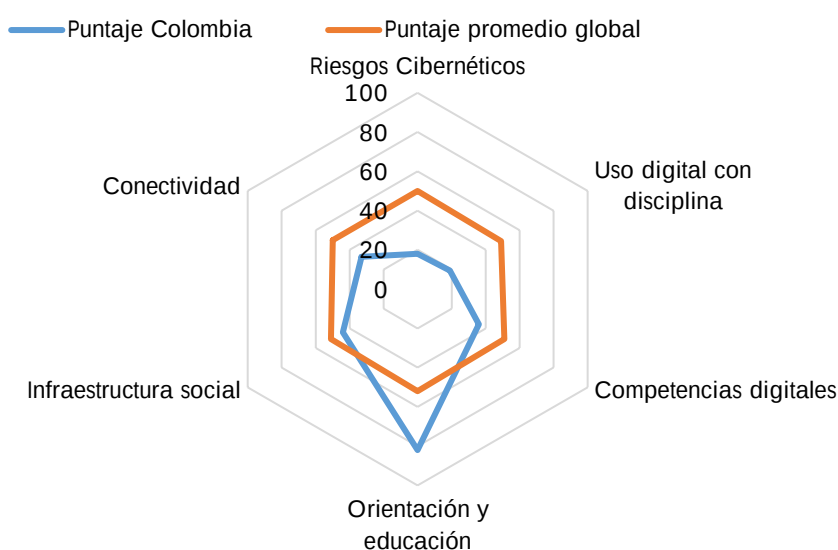
¹⁷ El *Children Online Security Index* basa su medición en 6 pilares: (i) Riesgos cibernéticos, que mide la exposición de los niños a riesgos cibernéticos (bullying, contactos riesgosos o uso desordenado de la tecnología), (ii) Uso digital con disciplina, que mide si los niños gastan demasiado tiempo en el uso de dispositivos digitales, (iii) Competencias digitales, que mide si los niños poseen habilidades digitales que les permitan minimizar riesgos cibernéticos y ser buenos ciudadanos digitales, (iv) Orientación y educación, que mide si los niños cuentan con el apoyo de acudientes y de la educación escolar en respecto a seguridad en línea, (v) Infraestructura social, que mide si los gobiernos y la industria operan protegiendo a los niños de riesgos cibernéticos, y (vi) Conectividad, que mide si los niños pueden acceder a Internet con velocidades suficientes.

¹⁸ La medición 2020 comprende datos recopilados de 145.426 niños y adolescentes diferentes entre 2017 y 2019.

Al observar el puntaje desagregado por cada pilar (Gráfico 2) se observa que para el pilar *competencias digitales* el desempeño del país es bajo obteniendo 36 puntos con respecto al promedio global que corresponde a 52 puntos, ocupando así el puesto 20 entre 30 países.

Esto muestra que los niños colombianos se encuentran en un entorno digital con un nivel de seguridad en línea por debajo del promedio global y en alta exposición a riesgos cibernéticos, a lo que se suma que no poseen habilidades digitales que les permitan minimizar riesgos cibernéticos y ser buenos ciudadanos digitales¹⁹.

Gráfico 2. Resultados del *Children Online Security Index 2020 para Colombia*



Fuente: elaboración DNP con datos del *Children Online Safety Index*, 2020.

Respecto a la generación de capacidades a través de la educación formal en materia de seguridad digital, el Índice de Ciberseguridad Nacional en inglés *National Cyber Security Index (NCSI)*²⁰ es un índice que mide en uno de sus pilares la educación y desarrollo

¹⁹ El Ministerio de Tecnologías de la Información y las Comunicaciones entiende la ciudadanía digital como el resultado de la transformación digital y productiva de los ciudadanos. En ese sentido se entiende que un ciudadano digital es aquel que cuenta con un conjunto de competencias y habilidades digitales mínimas relacionados con el uso apropiado, responsable y seguro de las TIC <https://colombiatic.mintic.gov.co/679/w3-propertyvalue-36666.html>.

²⁰ Este índice es desarrollado y soportado por el *e-Governance Academy (eGA)*, que es un tanque de pensamiento y organización consultiva sin ánimo de lucro que nace de una iniciativa conjunta del Gobierno de Estonia, el *Open Society Institute (OSI)* y el Programa de Desarrollo de las Naciones Unidas (ONU). Esta iniciativa tiene como fin crear y transferir conocimiento y mejores prácticas en transformación digital (gobierno electrónico, e-democracia y ciberseguridad nacional). <https://ega.ee/about-us/>

profesional en materia de seguridad digital. Colombia en este pilar obtiene un avance del 44 %, lo que muestra un bajo avance al respecto. Esto se refuerza al analizar la existencia de programas de educación superior a través del Sistema Nacional de Información de la Educación Superior (SNIES) del Ministerio de Educación Nacional, en el cual se evidencia que existen 41 programas activos relacionados con seguridad digital, de los cuales 36 son de nivel académico posgrado con sólo 3 maestrías. También se cuentan 5 programas que corresponden a nivel académico pregrado con 4 de formación tecnológica o técnica y 1 programa universitario.

En contraste, al inspeccionar programas dentro del ámbito TIC, tales como los relacionados con sistemas de información se encuentran 81 programas activos, de los cuales 20 son de nivel académico posgrado entre los que se cuenta 1 maestría y adicionalmente se encuentran 61 programas de nivel académico pregrado, de los cuales 4 son programas universitarios. Esto evidencia que la oferta de programas educativos relacionados con seguridad digital es baja en el nivel de académico pregrado.

Con lo anterior como contexto, es claro que se debe incrementar la oferta académica en materia de seguridad digital sin descuidar que el acceso a las Tecnologías de la Información y las Comunicaciones (TIC) sea equitativo para todos. Según datos disponibles en 2015 del Observatorio de Tecnologías de la Información (TI)²¹, la participación de mujeres en empresas de *Teleinformática, Software y TI* fue del apenas del 39 %, mientras que los hombres representaron un 61 %. En el campo de seguridad digital, el estudio *Genero y TIC en América Latina* (5G Américas, 2019), resalta cómo las TIC se presentan como una herramienta para mejorar las condiciones de vida de mujeres y niñas y llama la atención sobre la importancia de que se realicen esfuerzos conjuntos entre los sectores públicos y privado para generar diferentes estrategias que busquen potenciar el acceso de las mujeres a las TIC.

En lo concerniente al sector público, el *Global Cybersecurity Index* (Unión Internacional de Telecomunicaciones (UIT), 2018), mide el compromiso de los 175 países evaluados en torno a la ciber seguridad y generando un ranking mundial al respecto. Esta evaluación se realiza a través de 5 pilares (legal, técnico, organizacional, construcción de nuevas capacidades y cooperación), que como se describió en el marco teórico, describen adecuadamente las capacidades que se deben generar en el país para mejorar la confianza y la seguridad digital. En este índice, Colombia pasó del puesto 46 en la versión 2017 al puesto 73 en la versión 2018, perdiendo así varias posiciones en corto tiempo, lo cual

²¹Encuesta Estudio de caracterización ocupacional del sector de Teleinformática, Software y TI en Colombia, 2015. iniciativa del Ministerio de Tecnologías de la Información y las Comunicaciones y la Federación Colombiana de la Industria de Software y TI.

evidencia que Colombia no ha mejorado sus capacidades para dar respuesta oportuna a incidentes y amenazas en seguridad digital.

Por otro lado, el NCSI²² es un índice que mide la preparación de los países para prevenir amenazas y gestionar incidentes, relacionados con seguridad digital. La medición de este índice se enfoca en 4 aspectos relacionados con la implementación en ciberseguridad: (i) legislación vigente, (ii) unidades establecidas, (iii) marco de cooperación y (iv) resultados. (National Cyber Security Index - NCSI, 2020). En los resultados de dicho índice²³ Colombia obtiene un puntaje global de 46,75 sobre un total de 100, lo que muestra una baja preparación en seguridad digital comparado contra Grecia, país que obtiene el puntaje más alto en este índice (96,10).

Analizando el comportamiento de Colombia a través de los indicadores de este índice se evidencia que en la versión más reciente de resultados (a 13 de febrero de 2019), de 12 indicadores, 8 tienen un avance menor al 60 % (Gráfico 3). En la versión anterior del índice (5 de junio de 2017), el total de indicadores en la misma condición eran 9.

Por su lado, Grecia sólo cuenta con 3 indicadores por debajo de dicho porcentaje²⁴, tal como registra en la versión del índice a 27 de febrero de 2019. Cabe anotar que Grecia cuenta con una medición más reciente de este índice (al 27 de abril de 2020) en la que en todos los indicadores superan el 80 % de avance.

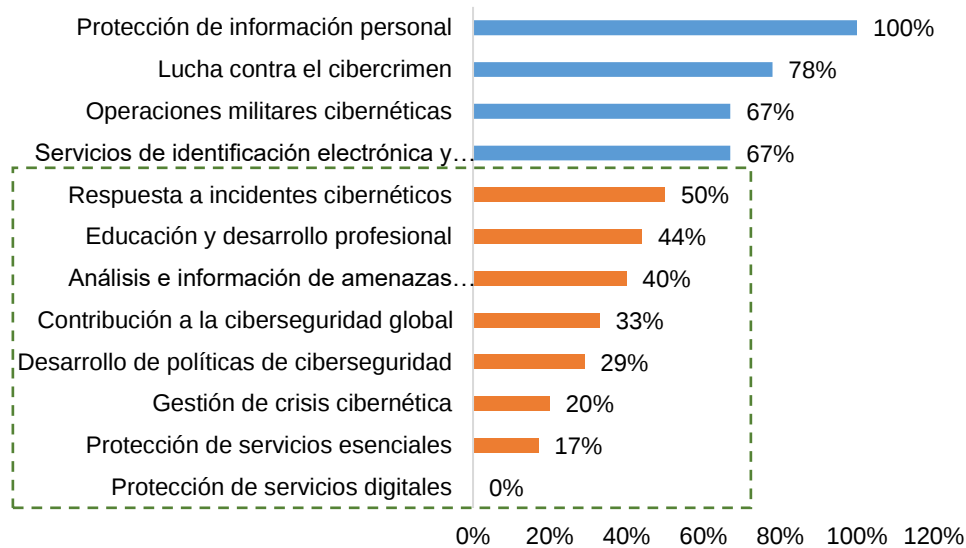
Los indicadores a los que hace referencia el NCSI resultan ser críticos para el desarrollo de la confianza y la seguridad digital, pues se relacionan con la manera en que el país puede abordar y reaccionar frente a incidentes en materia de seguridad digital. Entonces el comportamiento evidenciado para Colombia deja en claro que las capacidades en seguridad digital no son suficientes para generar cambios notorios en el entorno digital del país, reflejando la necesidad de aumentar dichas capacidades.

²² Este índice es desarrollado y soportado por el *e-Governance Academy (eGA)*, que es un tanque de pensamiento y organización consultiva sin ánimo de lucro que nace de una iniciativa conjunta del Gobierno de Estonia, el *Open Society Institute (OSI)* y el Programa de Desarrollo de las Naciones Unidas (ONU). Esta iniciativa tiene como fin crear y transferir conocimiento y mejores prácticas en transformación digital (gobierno electrónico, e-democracia y ciberseguridad nacional). <https://ega.ee/about-us/>

²³ Resultados disponibles en el sitio web <https://ncsi.ega.ee/country/co/>.

²⁴ Desarrollo de políticas de ciberseguridad (57 %), gestión de crisis cibernética (20 %) y operaciones militares cibernéticas (50 %).

Gráfico 3. Resultados del *National Cyber Security Index 2019* – Porcentaje de avance por indicador



Fuente: elaboración DNP con datos del *National Cyber Security Index* (2019).

Para el sector privado en Colombia, el *Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales*, analizó las medidas de seguridad implementadas para recolectar, almacenar, usar, circular o tratar datos personales en 31.410²⁵ empresas (entre privadas, sin ánimo de lucro y mixtas) del país (Superintendencia de Industria y Comercio - SIC, 2019). Este estudio refleja que el 44 % de las empresas que hacen parte del estudio, tienen un nivel de implementación menor o igual al 25 % de las medidas apropiadas y efectivas para garantizar la seguridad de los datos personales y sólo el 15 % tienen un nivel de implementación igual o superior al 76 %, de todos los requerimientos de seguridad emitidos por la SIC. Esto muestra una falta de preparación para garantizar la seguridad de los datos personales y por ende una ausencia de capacidades al respecto.

En conclusión, se evidencia que en Colombia hay deficiencias en todo el conjunto de las capacidades relacionadas con la seguridad digital, por parte de los ciudadanos, del sector público y del sector privado. Esto causa que el país presente bajos niveles de preparación y de avance en la materia, lo que a su vez incrementa la vulnerabilidad del país ante ataques y amenazas cibernéticas, deteriorando la confianza y el normal desarrollo de nuestro entorno digital.

²⁵ El período del estudio comprende entre el año 2015 hasta el 18 de septiembre de 2019. La base de este estudio son las organizaciones que registraron sus bases de datos en la SIC, como responsables del tratamiento de datos (Superintendencia de Industria y Comercio - SIC, 2019).

4.2. El marco de gobernanza en materia de seguridad digital no ha alcanzado un grado de desarrollo adecuado

En materia de seguridad digital, existen dos instancias de alto nivel dentro del marco de gobernanza en Colombia. La primera es la figura del coordinador nacional de seguridad digital que dispuso el Documento CONPES 3854 aprobado en 2016. A la fecha, esta figura se encuentra en cabeza de la Consejería de Asuntos Económicos y Transformación Digital de la Presidencia de la República. La consejería actúa como ente asesor para la Presidencia de la República y entidades del Gobierno nacional en los temas a su cargo, entre los cuales la seguridad digital es uno de ellos. No obstante, expresamente en las funciones de esta consejería no se establece que opere de manera exclusiva como una unidad de política de ciberseguridad de manera transversal y vinculante en sus decisiones frente a las demás entidades del Gobierno nacional. Esto limita su rol como coordinador nacional de seguridad digital y dificulta la coordinación de acciones y el seguimiento efectivo a las tareas relacionadas con la seguridad digital del país.

La otra instancia es el Comité de Seguridad Digital creado con el Acuerdo no. 002 de 2018 del Consejo para la Gestión y el Desempeño Institucional. Este comité tiene como objeto estudiar temas específicos de seguridad digital en niveles estratégicos y técnicos. Dentro de sus funciones se encuentra proponer lineamientos y recomendaciones en temas de orientación, ejecución de la Política de Seguridad Digital, así como asesorar en los criterios de evaluación de la gestión de dicha política. Sin embargo, la coordinación de acciones y el seguimiento efectivo a las tareas relacionadas con la seguridad digital no se encuentra a cargo de este comité, que igualmente se comporta como un ente asesor en seguridad digital.

Esta falta de enfoque efectivo del coordinador nacional de seguridad digital y del Comité de Seguridad Digital se percibe a través del NCSI. Este índice mediante sus subindicadores da claros indicios del panorama óptimo respecto al marco de gobernanza en seguridad digital, evaluando en cada país la creación efectiva de un total de nueve unidades o autoridades²⁶ relacionadas con la seguridad digital en diferentes ámbitos. Aunque Colombia cumple con la creación de seis de estas unidades o autoridades, el índice

²⁶ Las Unidades o Autoridades a las que se refiere el National Cyber Security Index (NCSI) son: (i) Unidad de política de ciberseguridad, (ii) Unidad de análisis de amenazas cibernéticas, (iii) Autoridad de supervisión competente para la protección de servicios esenciales, (iv) Autoridad de supervisión competente para los servicios de identificación electrónica y confianza, (v) Autoridad para protección de datos personales, (vi) Unidad de respuesta a incidentes, (vii) Unidad de cibercrimen, (viii) Unidad forense digital y (ix) Unidad de operaciones cibernéticas.

presenta como pendiente la creación de una unidad de política de ciberseguridad. Esto significa que ninguna de las instancias en cuestión es considerada por el NCSI como una unidad de política de ciberseguridad²⁷.

Por otro lado, en relación al marco de gobernanza, también se evidencia en la evaluación de Colombia en el NCSI la ausencia de un marco de coordinación de políticas de ciberseguridad, que es un subindicador que se pondera dentro del indicador *desarrollo de políticas de ciberseguridad*, y en el cual el país no obtiene ningún puntaje. Esto es relevante y crítico teniendo en cuenta que el marco de coordinación de políticas armoniza la manera que las diferentes entidades aportan al desarrollo de las políticas en materia de seguridad digital y que a su vez existen en el país diversas instituciones que trabajan en torno a la seguridad digital, tales como ColCERT del Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOCI) del Comando General de las Fuerzas Militares de Colombia, el Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia, el Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL), la Delegatura de protección de datos de la Superintendencia de Industria y Comercio (SIC), el Grupo interno de trabajo de seguridad y privacidad de la información de la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones, el Comité de ciberdefensa de las Fuerzas Militares, y las Unidades cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana. Entonces la articulación entre dichas entidades no puede ser clara y eficiente al no contar con dicho marco de coordinación.

Así pues, Colombia dentro de su marco de gobernanza y al carecer de un marco de coordinación de políticas de ciberseguridad no puede lograr una adecuada interacción e identificación entre las diversas entidades alrededor del tema. Lo anterior genera la desarticulación y la duplicación de esfuerzos, así como una baja cohesión y coordinación para dar respuesta a incidentes y a contener amenazas que se den en el entorno digital. A esto se le suma que no se cuenta con una instancia lo suficientemente robusta y especializada para coordinar adecuadamente los aspectos de seguridad digital a nivel nacional. Estos factores se constituyen en una debilidad para el avance en materia de seguridad digital y terminan debilitando la confianza digital en el país.

²⁷ Una unidad de política de ciberseguridad además de dar orientaciones, coordinar la acción y supervisar la ejecución de la estrategia, debe velar por el diseño, desarrollo e implementación permanente de instrumentos políticos en materia de seguridad digital, que permitan el cumplimiento de objetivos nacionales con relación al avance de la confianza y seguridad digital. Estos instrumentos deben abarcar los requisitos de gobernanza, operacionales y técnicos, definirán las funciones y responsabilidades de las múltiples partes interesadas y darán orientaciones o establecerán mecanismos específicos en relación con la confianza y la seguridad digital (Unión Internacional de Telecomunicaciones (UIT), 2018).

4.3. Se requiere la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital con énfasis en nuevas tecnologías

Los ciberataques están ampliando su rango de acción a partir del uso de nuevas tecnologías. Por ejemplo, los ataques a nivel global a dispositivos IoT (*Internet of Things*, por sus siglas en inglés) se incrementaron en un 300 % en el primer semestre de 2019 y si se tiene en cuenta que actualmente existen casi 21 billones de dichos dispositivos en el mundo, el riesgo de ataques es alarmante. Ahora bien, si para 2025 se espera que la cifra de dichos dispositivos se duplique (Foro Económico Mundial, 2020), es evidente el incremento en el riesgo que implican los ataques cibernéticos.

La aparición de ataques cibernéticos basados en nuevas tecnologías también conlleva costos para cualquier empresa o entidad pública, ya que el principal factor que incide en el aumento de los costos de contención de ataques cibernéticos es la creciente complejidad y sofisticación de estos (Accenture, 2019). Teniendo en cuenta que el estudio *Top 10 Strategic Technology Trends for 2020* (Gartner, 2020), determina las principales tendencias tecnológicas que generarán disrupciones digitales²⁸ significativas en los próximos 5 a 10 años, se observa que hay un extenso panorama en el cual la complejidad y sofisticación tanto de la tecnología, como de los mismos ataques cibernéticos que pueden derivarse a partir de estas, supera hasta las más altas expectativas. Ante estos cambios derivados de la tecnología, la respuesta yace en la capacidad de investigación e innovación en materia de seguridad digital de cada país.

EL NCSI cuenta entre sus indicadores uno denominado *Análisis e Información de Amenazas Cibernéticas* que se relaciona con la manera en que el país puede abordar y reaccionar frente a incidentes en materia de seguridad digital. En este indicador Colombia presenta un avance del 40 %, lo que deja claro que la identificación de amenazas cibernéticas no es suficiente en el entorno tecnológico actual. En consecuencia, si no se hace una rápida adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, en el futuro esta identificación será poco efectiva ante la aparición de nuevas tecnologías.

Considerando que el mundo se encuentra en el camino de la 4RI, caracterizada por la aparición de nuevas tecnologías (Schwab, 2016), las cuales además de traer grandes oportunidades para la sociedad también implican grandes retos en lo concerniente a confianza y seguridad digital es posible visualizar que, si desde ahora no se mejoran rápidamente las capacidades en seguridad digital del país, en especial las relacionadas con

²⁸ La disrupción digital es un efecto que cambia las expectativas y comportamientos fundamentales en una cultura, mercado, industria o proceso que es causado o expresado a través de capacidades, canales o activos digitales (<https://www.gartner.com/en/information-technology/glossary/digital-disruption>).

la identificación de amenazas derivadas de las nuevas tecnologías, Colombia muy posiblemente enfrentará amenazas y ataques de alta complejidad y sofisticación para los cuales no estará preparado.

5. DEFINICIÓN DE LA POLÍTICA

5.1. Objetivo general

Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

5.2. Objetivos específicos

OE 1. Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país.

OE 2. Actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y mejorar el avance en seguridad digital del país.

OE 3. Analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías para preparar al país a los desafíos de la 4RI.

5.3. Plan de acción

5.3.1. Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país

En primer lugar, el Departamento Administrativo de la Presidencia de la República, a través del Coordinador Nacional de Seguridad Digital, en conjunto con el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, el Ministerio de Educación Nacional, la SIC y el Servicio Nacional de Aprendizaje (SENA), coordinará y diseñará una estrategia de formación en capacidades en materia de seguridad digital, en la cual se unifiquen las iniciativas de sensibilización y generación de habilidades en los ciudadanos en Colombia en materia de seguridad digital, con la intención de mitigar la duplicación de esfuerzos aislados y fortalecer las capacidades en seguridad digital de los ciudadanos. Esta estrategia definirá una hoja de ruta para su institucionalización, de forma

que se logre su ejecución de manera permanente. Esta actividad iniciará en junio de 2021 y finalizará en diciembre de 2022.

En segundo lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones, unificará en una hoja de ruta las iniciativas para fortalecer las competencias en seguridad digital con enfoque diferencial e inclusivo de género para mujeres o los ciudadanos que se identifiquen con este género, de manera que se incluyan las iniciativas definidas y en ejecución, e iniciativas adicionales que se requieran para promover la participación del género femenino en los diferentes sectores: público, privado y academia. Esta hoja de ruta identificará las iniciativas que pueden ser de ejecución permanente con el fin de desarrollar capacidades con enfoque diferencial, promoviendo en la ciudadanía la concientización, el desarrollo de competencias en seguridad digital. Esta hoja de ruta definirá una línea de acción para su institucionalización, de forma que se logre su ejecución de manera permanente. Esta actividad iniciará en julio de 2020 y finalizará en diciembre de 2022.

En tercer lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones desarrollará e implementará una hoja de ruta correspondiente, para el desarrollo de iniciativas de promoción para la participación de las comunidades en condiciones especiales de vulnerabilidad, tales como los líderes sociales, en el fortalecimiento de capacidades en seguridad digital, bajo un enfoque diferencial e inclusivo. En esta hoja de ruta se deberá establecer la forma en la cual se institucionalizarán sus actividades para su desarrollo de manera permanente. Esta actividad iniciará en julio de 2020 y finalizará en diciembre de 2022.

En cuarto lugar, el Ministerio de Educación Nacional diseñará e implementará una estrategia para la creación de hábitos de uso seguro y responsable de las TIC que posibilite generar en la trayectoria educativa completa el desarrollo de competencias y la formación en seguridad y confianza digital. Esto, con el fin de aumentar la cultura en seguridad digital y ciber higiene²⁹, que puedan incorporarse en los diferentes niveles de formación educativa. Esta actividad iniciará en julio de 2020 y finalizará en julio de 2022.

En quinto lugar, el SENA, con apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, diseñará programas de formación profesional con enfoque para el trabajo y desarrollo humano, los cuales atenderán las necesidades sectoriales que se identifiquen durante el desarrollo de esta acción, para fortalecer las competencias en áreas como la seguridad digital, seguridad de la información, ciberseguridad e infraestructuras

²⁹ La ciber higiene es un principio fundamental relacionado con la seguridad de la información y, siguiendo la analogía con respecto a la higiene personal, es el equivalente a establecer medidas simples de rutina para minimizar los riesgos de las amenazas cibernéticas (European Union Agency for Network and Information Security (ENISA), 2016).

críticas. El Ministerio de Tecnologías de la Información y las Comunicaciones aportará expertos temáticos para apoyar la identificación de necesidades sectoriales y para que participen en las jornadas de diseño, desarrollo curricular y en la validación técnica para garantizar el número suficiente, la pertinencia y calidad de los programas de formación profesional, los cuales promoverán la gestión efectiva de los riesgos de seguridad digital, adoptando buenas prácticas y referentes tales como el marco para el desarrollo de fuerza laboral en ciberseguridad de la Iniciativa Nacional de Educación en Seguridad Cibernética (NICE, por sus siglas en inglés). Esta actividad iniciará en junio de 2021 y finalizará en marzo de 2022.

En sexto lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones, elaborará y ejecutará un programa de desarrollo de capacidades dirigido a organizaciones públicas (tanto del orden nacional como territorial), en el marco de la Política de Gobierno Digital, con el fin de promover la gestión efectiva de los riesgos de seguridad digital, adoptando buenas prácticas y marcos de referencia de ciberseguridad para tecnologías de amplia utilización y para tecnologías de la 4RI. Los resultados y logros de este programa deberán presentarse anualmente al Comité de Seguridad Digital. Esta acción iniciará en julio de 2020 y finalizará en diciembre de 2022.

En séptimo lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones en conjunto con el Ministerio de Defensa Nacional y el Departamento Administrativo de la Función Pública y con el apoyo del coordinador nacional de seguridad digital, elaborará y pondrá en marcha un programa de desarrollo de capacidades dirigido a los niveles directivos y ejecutivos de organizaciones públicas del orden nacional como territorial, de modo que les permita identificar, valorar y gestionar adecuadamente los riesgos de seguridad digital. Lo anterior con la finalidad de mejorar el marco de acción para la toma de decisiones en esta materia y el fortalecimiento de capacidades en las organizaciones públicas. Este programa deberá contemplar el impacto sobre la seguridad digital de las nuevas tecnologías y de las tecnologías emergentes. Esta actividad iniciará en febrero de 2021 y finalizará en diciembre de 2022.

En octavo lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones elaborará y pondrá en marcha un programa de desarrollo de capacidades dirigido a los niveles directivos y ejecutivos de organizaciones privadas, así como a las organizaciones privadas que se consideren como operadores de infraestructuras críticas o prestadores de servicios esenciales, de modo que les permita identificar, valorar y gestionar adecuadamente los riesgos de seguridad digital. Lo anterior con la finalidad de promover el cierre de brecha en capacidades y la gestión de riesgos de seguridad digital en el país. Esta actividad iniciará en febrero de 2021 y finalizará en diciembre de 2022.

En noveno lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones elaborará y ejecutará una estrategia de fortalecimiento de las empresas de la industria de Tecnologías de la Información que provean bienes y servicios de seguridad digital, contemplando la articulación con el Programa de formación de fuerza laboral en ciberseguridad³⁰, de forma que se promueva el desarrollo de talento pertinente y cualificado para esta industria y evaluando acciones complementarias y articular con los clústeres TI³¹ del país en los temas relacionados con seguridad digital, con apoyo de las Cámaras de Comercio, de forma que apalanque su fortalecimiento en iniciativas y programas de desarrollo empresarial bajo su cargo. Esta actividad iniciará en enero de 2021 y finalizará en diciembre de 2022.

En décimo lugar, El Ministerio de Justicia y del Derecho con el apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, la Fiscalía General de la Nación, el Ministerio de Defensa Nacional, con el acompañamiento de las entidades públicas y privadas que consideren pertinentes, realizarán el diagnóstico y las consecuentes recomendaciones de solución de los posibles problemas existentes en el marco normativo vigente que puedan afectar: (i) el ejercicio libre y pacífico de la ciudadanía digital; (ii) la defensa y seguridad nacional y (iii) la persecución, investigación y sanción de la comisión de conductas punibles a través del uso de las Tecnologías de la Información y las Comunicaciones (TIC). Esta actividad iniciará en julio de 2020 y finalizará en diciembre de 2022.

En décimo primer lugar, el Departamento Administrativo de la Presidencia de la República, a través del coordinador nacional de seguridad digital, con el apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, con el apoyo de la Fiscalía General de la Nación, la SIC, la Dirección Nacional de Inteligencia, y en caso de requerirse, con el apoyo del Ministerio de Defensa Nacional y del Ministerio de Relaciones Exteriores, diseñará e implementará una ruta de acción que permita avanzar en el desarrollo de la normatividad en materia de seguridad digital, para lo cual tendrá en cuenta, entre otros, el impacto del Internet de las cosas (IoT), las Redes y Sistemas OT, el Big Data, la Computación en la Nube, la Inteligencia Artificial (IA), el *Machine Learning* e Interfaces de Programación de Aplicaciones (API) y otras tecnologías emergentes, en materia de confianza y seguridad digital. Para avanzar en el desarrollo de dicha ruta de acción, se tendrán en cuenta las normas existentes y aquellas que se encuentren en desarrollo, así como las medidas

³⁰ El marco para el desarrollo de fuerza laboral en ciberseguridad es un lineamiento de la *Iniciativa Nacional de Educación en Seguridad Cibernética* (NICE, por sus siglas en inglés).

³¹ Según la comisión de UE son agrupaciones o grupos organizados de empresas independientes, así como organizaciones de investigación y difusión del conocimiento y otros actores económicos relacionados y diseñados para estimular la actividad, promoviendo el intercambio de instalaciones, conocimiento y experiencia.

establecidas por todas las autoridades regulatorias del sector ejecutivo, tales como: la Comisión de Regulación de Comunicaciones (CRC), la Comisión de Regulación de Energía y Gas Combustible y la Comisión de Regulación de Agua Potable y Saneamiento Básico, entre otras, de manera que se logre un marco normativo armónico. Esta actividad iniciará en julio de 2021 y finalizará en diciembre de 2022.

En décimo segundo lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional y la Dirección Nacional de Inteligencia (DNI), elaborarán el diagnóstico actual y el plan de mejoramiento continuo de sus propias capacidades operativas, administrativas, humanas, científicas y de infraestructura tecnológica. Lo anterior con el fin de apalancar recursos para el fortalecimiento de dichas entidades en materia de seguridad digital. Se presentará anualmente un informe ante la Consejería Nacional de Asuntos Económicos y Transformación Digital de la Presidencia de la República, o quien haga sus veces, sobre el desarrollo de este plan de mejoramiento continuo. Esta actividad iniciará en julio de 2020 y finalizará en diciembre de 2022.

En décimo tercer lugar, el Ministerio de Defensa Nacional definirá los lineamientos que permitan la conformación de una red de participación cívica digital que permita a las múltiples partes interesadas interactuar y cooperar frente a una amenaza cibernética. Lo anterior, con el propósito de fortalecer y ampliar las capacidades de seguridad digital en Colombia. Dicha red de participación cívica digital actuará en el marco de los principios fundamentales de la presente política, en particular la salvaguarda de los derechos humanos, así como del derecho internacional humanitario. Esta actividad iniciará en julio de 2020 y finalizará en diciembre de 2021.

En décimo cuarto lugar, el Departamento Nacional de Planeación a través de la Dirección de Estudios Económicos, en coordinación con el Archivo General de la Nación, el Ministerio de Tecnologías de la Información y las Comunicaciones, la Agencia Nacional Digital y todas las entidades públicas que integran el Sistema de Seguridad Social Integral³², conforme a sus competencias y de acuerdo con lo que se requiera, coordinará la elaboración de lineamientos para los planes de mejora en seguridad digital con el fin de fortalecer las capacidades de dicho sistema en el manejo, gestión e intercambio de la información, dada la condición de infraestructura crítica cibernética del Sistema de Seguridad Social Integral. Dichos planes de mejora se desarrollarán según las condiciones y capacidades técnicas de cada una de las entidades públicas que integran el Sistema de Seguridad Social Integral y

³² El Sistema de Seguridad Social Integral es el conjunto armónico de entidades públicas y privadas, normas y procedimientos y está conformado por los regímenes generales establecidos para pensiones, salud, riesgos profesionales y los servicios sociales complementarios que se definen en la Ley 100 de 1993.

se enmarcarán en el Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Para esto, el Departamento Nacional de Planeación a través de la Dirección de Estudios Económicos velará para que se establezca por las entidades competentes como mínimo: (i) las condiciones mínimas de seguridad esperadas para cada subsistema del Sistema de Seguridad Social Integral y sus entidades involucradas, (ii) los lineamientos para la medición del nivel de madurez en seguridad digital para las entidades involucradas en los subsistemas del Sistema de Seguridad Social Integral, (iii) los lineamientos para el diseño de una hoja de ruta de acciones para disminuir la brecha en seguridad digital de cada subsistema del Sistema de Seguridad Social Integral y sus entidades involucradas y (iv) los lineamientos para el modelo de seguimiento y evaluación del plan de mejora. Adicionalmente, estos planes deben profundizar sobre la necesidad de la clasificación de expedientes, documentos e información confidencial, la identificación temprana de amenazas, el análisis de las implicaciones de compartir información y la tipificación de vulnerabilidades y el control del riesgo de divulgación, alteración o pérdida de documentos o expedientes que corresponda a información clasificada, reservada de seguridad nacional o que atenten contra los derechos fundamentales de los ciudadanos, así como la identificación y protección de los documentos vitales o esenciales para asegurar la continuidad y el funcionamiento en caso de materializarse alguna amenaza, incidente o ataque cibernético. Esta actividad iniciará en octubre de 2020 y finalizará en marzo de 2022.

En décimo quinto lugar, el Ministerio de Defensa Nacional, con el apoyo del Departamento Nacional de Planeación a través de la Dirección de Estudios Económicos, establecerá dentro del Modelo Nacional de Gestión de Incidentes³³, los lineamientos con las condiciones especiales para la gestión de riesgos y el manejo de incidentes en seguridad digital relacionados con el manejo, gestión e intercambio de la información del Sistema de Seguridad Social Integral. Esto con el fin de asegurar la información y que se dé la atención en condiciones de prioridad a los incidentes que lleguen a ocurrir. Estas condiciones especiales deberán integrarse con el procedimiento general de atención a incidentes ya existente establecido por el Comité de Seguridad Digital. Esta actividad iniciará en septiembre de 2021 y finalizará en marzo de 2022.

En décimo sexto lugar, el Departamento Nacional de Planeación a través de la Dirección de Estudios Económicos, con el apoyo del Ministerio de Tecnologías de la

³³ Según lo define el Ministerio de Tecnologías de la Información y las Comunicaciones, el Modelo Nacional de Gestión de Incidentes de seguridad digital facilita la generación de un enfoque estructurado que permite a las instancias ciber de Estados y autoridades judiciales, actuar de manera articulada con el fin de gestionar los incidentes de impacto, de defensa y seguridad nacional, mediante protocolos de actuación establecidos.

Información y las Comunicaciones coordinará la incorporación de los mecanismos idóneos del caso (técnicos, legales, organizacionales, etc.) que permitan recopilar la evidencia digital necesaria en caso de materialización de algún incidente cibernético dentro del manejo, gestión e intercambio de la información del subsistema de Salud del Sistema de Seguridad Social Integral. Estos mecanismos deberán alinearse con la normatividad nacional que haya sido expedida al respecto. Esta actividad iniciará en abril de 2021 y finalizará en diciembre de 2022.

En décimo séptimo lugar, el Departamento Nacional de Planeación a través de la Dirección de Estudios Económicos con apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, el Archivo General de la Nacional, y las demás autoridades rectoras del Sistema de la Seguridad Social Integral - SSSI diseñarán, estructurarán y presentarán el proyecto de implementación del Equipos de Respuestas ante Incidentes de Seguridad en inglés *Computer Security Incident Response Team* (CSIRT) del Sector de la Seguridad Social Integral, el cual será socializado ante la comunidad del sector previa la revisión técnica que se efectuará con el Ministerio de Defensa Nacional. Esta actividad iniciará en diciembre de 2020 y finalizará en diciembre de 2022.

En décimo octavo lugar, la Dirección Nacional de Inteligencia (DNI), diseñará, estructurará y presentará el proyecto de implementación del CSIRT del Sector Inteligencia, con el fin que contribuya en la protección de la seguridad digital nacional. Este proyecto buscará principalmente que este CSIRT del sector de inteligencia (i) apoye la toma de decisiones en términos de valoración de los riesgos cibernéticos que se presenten en las entidades del sector y (ii) facilite la difusión de información técnica de alto valor de amenazas al Comité de Seguridad Digital referente a los distintos fenómenos que se generen en el Ciberespacio; mediante la integración e implementación de capacidades tecnológicas de última generación que aporte a la protección de los entornos de la Economía Digital del Estado. También dentro del diseño de este CSIRT se contemplará la armonización con las demás instancias de Seguridad Digital existentes en el país y se propiciará la analítica correlacional de los eventos e incidentes desarrollados en el ciberespacio que permita la identificación y traza de fenómenos que puedan afectar la seguridad del estado. Este proyecto será socializado ante la comunidad del sector de inteligencia en las instancias de la Junta de Inteligencia Conjunta (JIC). Esta actividad iniciará en julio de 2020 y finalizará en diciembre de 2022.

En décimo noveno lugar, el Ministerio de Defensa Nacional con el apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con las instancias nacionales a cargo de la gestión de incidentes de seguridad digital (CoICERT, CECIP, CCOCI, el CSIRT Gobierno y la DNI), bajo los lineamientos del Coordinador Nacional de

Seguridad Digital y dentro de un marco colaborativo entre los diferentes sectores y múltiples partes interesadas, diseñarán una propuesta del registro central único de incidentes de seguridad digital a nivel nacional, con el fin de analizar las tipologías de los incidentes y valorar periódicamente la necesidad de priorizar estrategias y recursos para su gestión.

Dicho registro central único de incidentes deberá integrar los reportes existentes en la materia realizados por las múltiples partes interesadas procurando simplificar el envío, determinando medios seguros de entrega y garantizando la confidencialidad, conservación y uso adecuado de la información que se intercambie entre partes. Para la concepción de este registro: (i) se aprovecharán las capacidades de los diferentes CSIRT sectoriales (existentes o que lleguen a existir) para facilitar la centralización de la información proveniente de cada sector, (ii) se tendrán en cuenta las experiencias previas que existan en el país al respecto, (iii) se implementarán los mecanismos de obligatoriedad de notificaciones de incidentes de seguridad digital para las entidades del Gobierno nacional y (iv) se atenderán las disposiciones y protocolos para el manejo de la evidencia digital, así como la obligatoriedad de la denuncia, conforme lo establecido en el Código de Procedimiento Penal Colombiano. Esta propuesta de diseño se deberá presentar ante el Comité de Seguridad Digital para su puesta en consideración. Esta actividad iniciará en mayo de 2021 y finalizará en diciembre de 2021.

5.3.2. Actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y mejorar el avance en seguridad digital del país

En primer lugar, el Departamento Administrativo de la Presidencia de la República, a través del coordinador nacional de seguridad digital, liderará y pondrá a consideración ante el Comité de Seguridad Digital la estructuración oficial de la gobernanza de seguridad digital en el país, definiendo los objetivos, alcance, roles, responsabilidades y competencias tanto de las diferentes instancias encargadas de la seguridad digital en el país, como las correspondientes a una unidad de política de ciberseguridad. Igualmente, se establecerán los mecanismos dinámicos y protocolos de coordinación y articulación estratégica, que: (i) cuenten con un esquema de representación de todas las múltiples partes interesadas, (ii) definan los roles y las responsabilidades, en el marco de sus funciones, de las múltiples partes interesadas; (iii) generen una matriz de comunicación y seguimiento entre las instancias máximas, el coordinador nacional y las múltiples partes interesadas. Lo anterior con el fin de coordinar la ejecución de las acciones relacionadas con la política nacional de confianza y seguridad digital. Esta actividad iniciará en julio de 2020 y finalizará en julio de 2022.

En segundo lugar, el Departamento Administrativo de la Presidencia de la República, a través del coordinador nacional de seguridad digital, presentará ante el Comité de

Seguridad Nacional las decisiones prioritarias que puedan requerirse para la implementación de la política de confianza y seguridad digital y para todo lo relacionado en materia de seguridad digital. Lo anterior con el fin fortalecer los mecanismos de toma de decisiones para la articulación estratégica en torno a la seguridad digital en Colombia. Esta actividad iniciará en julio de 2020 y finalizará en diciembre de 2022.

En tercer lugar, el Departamento Administrativo de la Presidencia de la República, a través del Coordinador Nacional de Seguridad Digital, presentará anualmente ante el Comité de Seguridad Digital anualmente los resultados del seguimiento a la agenda nacional de seguridad digital. Esto con el fin de fortalecer, a través de la divulgación dichos resultados, los mecanismos de información y toma de decisiones preventiva, para la articulación estratégica en torno a la seguridad digital en Colombia. Esta actividad iniciará en diciembre de 2020 y finalizará en diciembre de 2022.

En cuarto lugar, el Ministerio de Defensa Nacional creará un sistema nacional de gestión de incidentes cibernéticos que tendrá como fin: (i) articular los esfuerzos institucionales para la gestión oportuna de los incidentes cibernéticos, (ii) ser la fuente oficial de las estadísticas de los incidentes cibernéticos reportados en el país, (iii) estandarizar un mecanismo de reporte periódico de incidentes y vulnerabilidades cibernéticas que permita identificarlos, evaluarlos y comunicarlos a los interesados y (iv) servir de fuente para la toma de decisiones por parte del Gobierno nacional. La información de este sistema la podrán consultar en tiempo real los organismos de seguridad del Estado. Para adelantar esta acción se contará con el apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones. Esta actividad se ejecutará desde octubre de 2020 hasta diciembre de 2022.

En quinto lugar, el Ministerio de Defensa Nacional establecerá, a través de un documento, un modelo para la divulgación periódica de vulnerabilidades en todos los sectores con un alcance definido entre los puntos de contacto de los propietarios y operadores de activos que soportan actividades críticas y las instancias pertinentes del Gobierno nacional. Este modelo deberá incluir, entre otros: (i) el objetivo del intercambio, (ii) la definición de estándares para el intercambio, (iii) el (los) punto(s) único(s) de contacto, (iv) las responsabilidades en el intercambio de información dentro de un marco de confidencialidad y privacidad de la información, (v) los actores relevantes y (vi) los mecanismos de apoyo. Para el desarrollo de este modelo se involucrarán a las múltiples partes interesadas y se contemplarán experiencias internacionales al respecto. Esta actividad iniciará en julio de 2020 y finalizará en junio de 2021.

En sexto lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones establecerá un procedimiento para la promoción y difusión del modelo de divulgación

periódica de vulnerabilidades, con el fin de garantizar que las debilidades detectadas por un descubridor sean comunicadas en condiciones adecuadas para las partes y a su vez atendidas y subsanadas por las entidades, propietarios u operadores de infraestructuras críticas de manera oportuna. Lo anterior, dentro de un marco de divulgación responsable. Esta acción iniciará en marzo de 2021 y finalizará en agosto de 2021.

En séptimo lugar, el Ministerio de Defensa Nacional creará e implementará un sistema de intercambio de información cibernética, con miras a facilitar la divulgación de indicadores de compromiso entre los actores que interactúan en el entorno digital a nivel nacional e internacional. Dicho sistema se articulará con el registro central único de incidentes de seguridad digital. Esta actividad se ejecutará desde julio de 2020 hasta mayo de 2021.

En octavo lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones generará un estudio para la actualización del modelo de gobernanza de la seguridad digital en Colombia, para los sectores público y privado. Con el objetivo de apoyar en el fortalecimiento de la organización de seguridad digital en el país. Esta actividad iniciará en julio de 2020 y finalizará en diciembre de 2020.

En noveno lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones con el apoyo del Departamento Nacional de Planeación, realizará la medición de impacto de los incidentes de seguridad digital en el sector público colombiano para definir la viabilidad de inversión en las acciones de prevención y mitigación de los riesgos de seguridad digital. Esta medición comprende el levantamiento de información detallada sobre cómo las entidades invierten sus recursos para la gestión de los riesgos, cómo los distribuyen para estrategias de prevención y reacción sobre incidentes de seguridad digital, qué tan consientes son de sus vulnerabilidades, o qué tanto gestionan la seguridad de la información a partir de las fuentes primarias. Esta actividad iniciará en enero de 2022 y terminará en diciembre de 2022.

En décimo lugar, el Ministerio de Defensa Nacional en conjunto con el Ministerio de Tecnologías de la Información y las Comunicaciones elaborará un reporte anual para el coordinador nacional de seguridad digital, sobre los logros y avances de ejecución (desde las perspectivas cualitativa y cuantitativa) de los planes de fortalecimiento de las capacidades para cada una de las instancias y entidades responsables de la ciberseguridad y ciberdefensa de la Nación. Dicho reporte debe tener como objetivo fomentar la prevención en seguridad digital, la promoción de toma de decisiones y la mejora continua de la gestión y respuesta a incidentes cibernéticos a nivel nacional. Esta actividad iniciará en diciembre de 2021 y finalizará en diciembre de 2022.

5.3.3. Analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías para preparar al país a los desafíos de la 4RI

En primer lugar, el Departamento Administrativo de la Presidencia de la República, a través del coordinador nacional de seguridad digital, formulará el decreto reglamentario para la aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permita la adecuada gestión de riesgos de seguridad digital y respuesta a incidentes del sector. Lo anterior, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales y la inclusión y actualización permanente de políticas de seguridad y confianza digital. La formulación de dicho decreto se hará en coordinación con el Comité de Seguridad Digital, evaluando los mejores estándares, modelos, normas, herramientas y buenas prácticas con enfoque en el análisis e información de amenazas cibernéticas, que se apliquen mejor a la realidad del país. Esta actividad se ejecutará desde julio de 2020 hasta diciembre de 2020.

En segundo lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones en conjunto con el Ministerio de Defensa Nacional y la Dirección Nacional de Inteligencia, crearán una serie de guías metodológicas para la identificación y gestión de riesgos de seguridad digital en la adopción que las entidades del sector público hagan de tecnologías de la 4RI, tales como, IoT, *blockchain*, *big data*, computación en la nube e inteligencia artificial. Lo anterior, con el propósito de integrar estas nuevas tecnologías a partir de los estándares expuestos. Esta actividad iniciará en septiembre de 2020 y finalizará en marzo de 2021.

En tercer lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones expedirá los lineamientos y guías que faciliten a las entidades públicas adelantar los procesos de adopción y actualización de tecnologías con el fin de disminuir las vulnerabilidades derivadas de la obsolescencia tecnológica y así favorecer la seguridad digital en el país. Dichos lineamientos y guías se integrarán a la actual política de Gobierno Digital y se enmarcarán en los principios establecidos en el artículo 147 de la Ley 1955 de 2019 por la cual se expide el Plan Nacional de Desarrollo *2018-2022 Pacto por Colombia, Pacto por la Equidad*, y cómo mínimo deberán contener: (i) recomendaciones sobre buenas prácticas en la actualización de tecnología, (ii) recomendaciones acerca de metodologías y tiempos en los que una entidad debería actualizar sus equipos y sistemas informáticos. Esta actividad iniciará en agosto de 2020 y finalizará en octubre de 2021.

5.4. Seguimiento

En primera medida se hará seguimiento a los indicadores del Plan de Acción y Seguimiento (PAS) ([Anexo A](#)) en el período comprendido entre 2020 y 2022, en las fechas establecidas en la

Tabla 2. Como principal herramienta para hacer seguimiento a la ejecución física y presupuestal de las acciones de la presente política. El reporte periódico al PAS se realizará por parte de todas las entidades involucradas en este documento, que a su vez será consolidado por el DNP en un Informe de cierre, de acuerdo con lo estipulado en la

Tabla 2. Cabe aclarar que el cumplimiento de los indicadores contenidos en el PAS por parte de las diferentes entidades estará sujeto a la disponibilidad de recursos que se apropien para tal fin, sin perjuicio del seguimiento a los compromisos establecidos en este para la ejecución de la presente política.

Tabla 2. Cronograma de seguimiento

Corte	Fecha
Primer corte	31 diciembre de 2020
Segundo corte	30 de junio de 2021
Tercer corte	31 diciembre de 2021
Cuarto corte	30 de junio de 2022
Informe de cierre	31 diciembre de 2022

Fuente: DNP (2020).

5.5. Financiamiento

Para efectos del cumplimiento de los objetivos de esta política, las entidades involucradas en su ejecución gestionarán y priorizarán, en el Marco Fiscal de Mediano Plazo, los recursos para la financiación de las estrategias que se proponen.

La política tiene un costo total aproximado de 8.342 millones de pesos. En la Tabla 3 se muestra los costos por año para cada una de las entidades ejecutoras de las acciones aquí contenidas.

Tabla 3. Financiamiento estimado indicativo de la política

(cifras en millones de pesos)

Entidad	2020	2021	2022	Total
Departamento Administrativo de la Presidencia de la República	-	-	-	-
Departamento Nacional de Planeación	-	1.990	1.010	3.000
Dirección de Nacional de Inteligencia	-	600	-	600
Ministerio de Defensa Nacional	-	-	-	-
Ministerio de Educación Nacional	-	-	-	-
Ministerio de Justicia y del Derecho	24	68	72	164
Ministerio de Tecnologías de la Información y las Comunicaciones	450	2.250	1.850	4.550
SENA	-	14	14	28
Total	474	4.922	2946	8.342

Fuente: DNP (2020).

6. RECOMENDACIONES

El Departamento Nacional de Planeación y el Ministerio de Tecnologías de la Información y las Comunicaciones recomiendan al Consejo Nacional de Política Económica y Social:

1. Aprobar la Política Nacional de Confianza y Seguridad Digital junto con su Plan de Acción y Seguimiento, para lograr establecer medidas para desarrollar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.
2. Solicitar a las entidades del Gobierno nacional involucradas en este documento priorizar los recursos para la puesta en marcha de las estrategias contenidas en el mismo, acorde con el Marco de Gasto de Mediano Plazo del respectivo sector.
3. Solicitar al Departamento Nacional de Planeación, consolidar y divulgar la información del avance de las acciones según lo planteado en el Plan de Acción y Seguimiento (Anexo A). La información deberá ser proporcionada por las entidades involucradas en este documento de manera oportuna según lo establecido en la sección de seguimiento.
4. Solicitar a la Presidencia de la República:
 - a. Establecer e implementar una ruta de acción que permita avanzar en el desarrollo de la normatividad en materia de seguridad digital.
 - b. Formular el decreto reglamentario para la aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permita la adecuada gestión de riesgos de seguridad digital y respuesta a incidentes del sector.
5. Solicitar al Ministerio de Defensa Nacional:
 - a. Dentro de un marco colaborativo entre los diferentes sectores y múltiples partes interesadas, diseñar una propuesta del registro central único de incidentes de seguridad digital a nivel nacional.
 - b. Establecer un modelo para la divulgación periódica de vulnerabilidades en todos los sectores con un alcance definido entre los puntos de contacto de los propietarios y operadores de activos que soportan actividades críticas y las instancias pertinentes del Gobierno nacional.
 - c. Crear e implementar un sistema de intercambio de información cibernética, con miras a facilitar la divulgación de indicadores de compromiso entre los actores que interactúan en el entorno digital a nivel nacional e internacional.

6. Solicitar al Ministerio de Educación Nacional diseñar e implementar una estrategia que contemple acciones para la generación de hábitos de uso seguro y responsable de las TIC que posibilite generar en la trayectoria educativa completa el desarrollo de competencias y la formación en seguridad y confianza digital.
7. Solicitar al Ministerio de Justicia y del Derecho, realizar el diagnóstico y las consecuentes recomendaciones de solución de los posibles problemas existentes en el marco normativo vigente que puedan afectar: (i) el ejercicio libre y pacífico de la ciudadanía digital; (ii) la defensa y seguridad nacional y (iii) la persecución, investigación y sanción de la comisión de conductas punibles a través del uso de las Tecnologías de la Información y las Comunicaciones (TIC).
8. Solicitar al Ministerio de Tecnologías de la Información las Comunicaciones:
 - a. Elaborar y ejecutar un programa de desarrollo de competencias y capacidades dirigido a organizaciones públicas (tanto del orden nacional como territorial), con el fin de promover la gestión efectiva de los riesgos de seguridad digital, adoptando buenas prácticas y marcos de referencia de ciberseguridad para tecnologías de amplia utilización y para tecnologías de la Cuarta Revolución Industrial.
 - b. Elaborar y poner en marcha un programa de desarrollo de competencias dirigido a los niveles directivos y ejecutivos de organizaciones privadas, así como a las organizaciones privadas que se consideren como operadores de infraestructuras críticas o prestadores de servicios esenciales, de modo que les permita identificar, valorar y gestionar adecuadamente los riesgos de seguridad digital.
 - c. Generar un estudio para la actualización del modelo de gobernanza de la seguridad digital en Colombia.
 - d. Expedir los lineamientos y guías que faciliten a las entidades públicas adelantar los procesos de adopción y actualización de tecnologías con el fin de disminuir las vulnerabilidades derivadas de la obsolescencia tecnológica y así favorecer la seguridad digital en el país.
9. Solicitar al Servicio Nacional de Aprendizaje (SENA) diseñar programas de formación profesional con el enfoque de la formación para el trabajo y desarrollo humano, los cuales atenderán las necesidades sectoriales para fortalecer las competencias en áreas como la seguridad digital, seguridad de la información, ciberseguridad e infraestructuras críticas.

GLOSARIO

Amenaza: posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí.

Estas amenazas pueden darse de manera no premeditada y accidental o, por el contrario, de manera intencional con el fin de causar daño, generar problemas o adelantar una agresión cibernética con el objetivo del propio beneficio o para desestabilizar la población, el territorio y la organización política del Estado. (Ministerio de Defensa de Colombia) (Rec. UIT-T X.800, 3.3.55).

Ataque: amenaza intencional que se concreta.

CERT: (Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas. Se refiere a una institución definida y concreta con capacidad centralizada para la coordinación de gestión de incidentes. (Universidad Carnegie – Mellon).

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

Ciberdelincuencia: conjunto de acciones y actividades ilícitas que son cometidas total o parcialmente en el entorno digital, asociadas con el uso de las Tecnologías de la Información y las Comunicaciones o la utilización de un bien o servicio informático con el fin de causar daño, generar problemas o adelantar una agresión cibernética con el objetivo del propio beneficio o para desestabilizar la población, el territorio y la organización política del Estado.

Ciberdelito / Delito cibernético: actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia)

Ciberespacio: es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

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

CSIRT: Equipo de Respuesta a Incidentes de Seguridad cibernética, por su sigla en inglés. Se refiere a una institución definida y concreta que tiene la responsabilidad de proveer capacidades de gestión de incidentes a una organización/sector en especial. Su objetivo es minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.

Descubridor: se trata de aquella parte interesada que tiene conocimiento de la existencia una vulnerabilidad propia o de uno o varios terceros.

Divulgación responsable: es cuando un descubridor revela una vulnerabilidad a la(s) parte(s) interesada(s) que la posee o a las autoridades competentes, con la intención que se proceda a su corrección o a la toma de medidas al respecto. Esta divulgación no se entiende de carácter público, hasta que la(s) parte(s) interesada(s) que posee(n) la vulnerabilidad o las autoridades competentes lo consideren conveniente, sea para generar alarmas oportunas, para efectos estadísticos o para la documentación del caso.

Entorno digital: ambiente, tanto físico como virtual sobre el cual se soportan las interacciones del futuro digital, tales como la economía digital.

Incidente: cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital.

Infraestructura crítica: es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación. (Resolución CRC 2258 de 2009).

Infraestructura crítica cibernética nacional: se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en

el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

Múltiples partes interesadas: estarán comprendidas por el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades.

Riesgo informático: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (ISO Guía 73:2002)

Seguridad digital: es la situación de normalidad y de tranquilidad en el entorno digital (cibespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Vulnerabilidad: es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

ANEXOS

Anexo A. Plan de Acción y Seguimiento (PAS)

Ver archivo Excel adjunto.

Anexo B. Parámetros relacionados con calidad de la interacción para la confianza digital

La confianza digital se entiende como la calidad de la interacción que se deriva de la actividad empresarial y gubernamental mediada en línea, es pertinente puntualizar todos los parámetros que la componen para evitar un entendimiento sesgado de lo que es la confianza digital en sí. Estos parámetros se describen a continuación:

Ambiente: se refiere a los mecanismos utilizados para construir confianza en un entorno digital. Estos deben propender por una efectiva seguridad digital, evitando al máximo los ciber ataques, promoviendo la responsabilidad de la información y favoreciendo la implementación de sistemas de gestión de identidad que ayuden a mitigar el mal uso de la identidad digital del usuario respetando la privacidad y protegiendo el anonimato de información personal.

Experiencia: se refiere al estado en el cual los usuarios experimentan el ambiente de la confianza digital. La experiencia tiene como fin la no existencia de *fricción*³⁴ en los procesos de interacción en línea y viene de la mano del *ambiente*, ya que la utilización de medidas en exceso en temas de seguridad, responsabilidad de la información y privacidad, aumentan la fricción y por ende pueden terminar disminuyendo la confianza digital del usuario.

Actitudes: se refiere a la percepción de los usuarios frente a la confianza digital. Estas actitudes permiten que un usuario se manifieste respecto al *ambiente* y la *experiencia* y sea un actor clave en la promoción del entorno digital, dependiendo, entre otras, de su percepción frente a la infraestructura tecnológica y su grado de obsolescencia, así como del grado en que otros actores depositen su confianza en instituciones y empresas. Esta percepción es lo que al final brinda al usuario una medida de la calidad de las interacciones con empresas y entidades.

Comportamiento: se refiere a la reacción de los usuarios respecto al *ambiente* y a la *experiencia*. El comportamiento se enfoca en el nivel de tolerancia de los usuarios, dado cierto nivel de *fricción*, persistiendo y completando una transacción en el entorno digital.

³⁴ Se entiende en este contexto que la fricción es cualquier cosa que dificulte las transacciones o interacciones en línea y su correcta finalización. Estas dificultades se refieren, entre otras, a velocidades de carga lentas, páginas innecesarias o reingreso de contraseña. Debe anotarse que la experiencia en línea siempre tendrá algún tipo de fricción, y algunas de sus formas son necesarias para la seguridad digital. En consecuencia, no se trata de su eliminación total, sino de encontrar un equilibrio adecuado en la cantidad de fricción (Chakravorti & Ravi, 2017).

Anexo C. Alcance de cada una de las capacidades en seguridad digital

El marco de trabajo conceptual establecido por la UIT en el *Global Cybersecurity Index 2018*, se enfoca en 5 tipos de capacidades que deben tenerse en cuenta al momento de pensar en una cultura nacional de ciberseguridad que permita abordar la 4RI y el futuro digital.

Capacidad legal: se refiere a la existencia de instituciones y marcos normativos y regulatorios que permiten el manejo de situaciones relacionadas con ciberseguridad, ciberdefensa y ciberdelitos, incluyendo los mecanismos de investigación y judicialización de los delitos y la imposición de sanciones por incumplimiento de la ley. El objetivo de esta capacidad es contar con la legislación suficiente y necesaria que haga más expedito el combate nacional e internacional contra toda actividad ilícita y toda conducta irresponsable, que se desarrollen en el ciberespacio.

Capacidad técnica: se refiere a la existencia de instituciones y estándares técnicos que permitan abordar y entender las situaciones de seguridad digital. Esto incluye las competencias y mecanismos técnicos para prevenir, detectar, mitigar y responder a las amenazas, incidentes y ataques cibernéticos. El objetivo de esta capacidad es contar con un mínimo de condiciones técnicas aplicables de confianza y seguridad, que evite y minimice las vulnerabilidades en seguridad digital.

Capacidad organizacional: se refiere a la existencia de instituciones que coordinen las políticas y las estrategias para el desarrollo de la seguridad digital, así como la capacidad de intercambio de información entre las múltiples partes interesadas. Incluye las medidas indispensables para la implementación de una iniciativa nacional en seguridad de la información. El objetivo de esta capacidad es contar con una estrategia nacional, un modelo de gobernanza e instituciones que supervisen los esfuerzos en los diferentes sectores, evitando los conflictos en las acciones y generando una armonización efectiva entre las múltiples partes interesadas.

Capacidad de investigación e innovación: se refiere a la existencia de investigación, desarrollo e innovación, educación y programas de entrenamiento, así como profesionales certificados y entidades del sector público o privado que, actuando como multiplicadores, concienticen, informen, capaciten o formen en materia de seguridad digital. Este conocimiento se genera en relación con los tres pilares anteriores. Esto incluye también el desarrollo social, económico, político y humano implícito en la seguridad digital. El objetivo de esta capacidad es la construcción de conocimiento, conciencia y nuevas competencias, así como lograr disponer de los profesionales cualificados en materia de seguridad digital.

Capacidad de cooperación: se refiere a la existencia de alianzas, trabajo cooperativo e intercambio de información en el ámbito nacional e internacional. Dado que la ciberseguridad y el cibercrimen son de naturaleza transnacional, se requiere del concurso de múltiples partes interesadas en el ámbito nacional e internacional. El objetivo de esta capacidad es fortalecer la seguridad digital nacional a través del establecimiento de acuerdos bilaterales y multilaterales e instrumentos internacionales y de la participación en espacios internacionales de cooperación en la materia. Esto en pro de aunar esfuerzos para detectar y responder a amenazas, incidentes y ataques.

BIBLIOGRAFÍA

- 5G Américas. (2019). *Género y TIC en América Latina*. Obtenido de Género y TIC en América Latina: <http://brechacero.com/wp-content/uploads/2019/05/Genero-y-TIC-ES.pdf>
- Accenture. (2019). *Securing the Digital Economy. Reinventing the Internet for Trust*. Obtenido de https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf
- Accenture. (2019). *The Cost of Cybercrime*. Obtenido de https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
- Akamai. (2019). *State of the Internet - A year in review*. Obtenido de <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-a-year-in-review-report-2019.pdf>
- Banco Interamericano de Desarrollo - BID. (2016). *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?* Obtenido de <https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe>
- Chakravorti, B., & Ravi, C. (2017). *Digital Planet 2017*. Obtenido de https://sites.tufts.edu/digitalplanet/files/2017/05/Digital_Planet_2017_FINAL.pdf
- Comisión de Regulación de Comunicaciones - CRC. (2017). *El Comercio electrónico en Colombia. Análisis integral y perspectiva regulatoria*. Obtenido de https://www.crcm.gov.co/recursos_user/2017/ComElecPtd_0.pdf
- 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>
- DQ Institute. (2020). *Child Online Safety Index*. Obtenido de <https://www.dqinstitute.org/child-online-safety-index/>
- European Union Agency for Network and Information Security (ENISA). (2016). *Review of Cyber Hygiene practices*. Obtenido de https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport

- Foro Económico Mundial - FEM. (2018). *Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society*. Obtenido de http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf
- Foro Económico Mundial - FEM. (2019). *Informe Global de Riesgos 2019*. Obtenido de Informe Global de Riesgos 2019: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
- Foro Económico Mundial - FEM. (2019). *Regional Risks for Doing Business 2019*. Obtenido de Regional Risks for Doing Business 2019: http://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2019.pdf
- Foro Económico Mundial - FEM. (2019a). *Regional Risks for Doing Business 2019*. Obtenido de Regional Risks for Doing Business 2019: http://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2019.pdf
- Foro Económico Mundial - FEM. (2020). *The Global Risks Report 2020*. Obtenido de http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
- Foro Económico Mundial. (2019). *Shaping the Future of Digital Economy and New Value Creation*. Obtenido de <https://www.weforum.org/platforms/shaping-the-future-of-digital-economy-and-new-value-creation>
- Gambetta, D. (2000). *Can We Trust Trust?* Obtenido de https://pdfs.semanticscholar.org/542a/ce96c6daa25922e626aaa8ca4aa904c2a2b0.pdf?_ga=2.269167731.324165317.1590624604-1814789925.1590624604
- Gartner. (2020). *Top 10 Strategic Technology Trends for 2020*. Obtenido de <https://emtemp.gcom.cloud/ngw/globalassets/en/publications/documents/top-tech-trends-2020-ebook.pdf>
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2019). *Manual de Gobierno Digital*. Obtenido de https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf
- National Cyber Security Index - NCSI. (7 de febrero de 2020). *National Cyber Security Index*. Obtenido de <https://ncsi.ega.ee/>
- Organización para la Cooperación y el Desarrollo Económicos - OCDE. (2018). *PISA 2018 Insights and Interpretations*. Obtenido de

<http://www.oecd.org/pisa/PISA%202018%20Insights%20and%20Interpretations%20FINAL%20PDF.pdf>

Organización para la Cooperación y el Desarrollo Económicos - OCDE. (2019). *Vectors of Digital Transformation*. Obtenido de https://www.oecd-ilibrary.org/science-and-technology/vectors-of-digital-transformation_5ade2bba-en

Schwab, K. (2016). *The Fourth Industrial Revolution*. Ginebra: World Economic Forum.

Superintendencia de Industria y Comercio - SIC. (2019). *Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales*. Bogotá D.C.: SIC.

Unión Internacional de Telecomunicaciones (UIT). (2018). *Global Cybersecurity Index 2018*. Obtenido de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Unión Internacional de Telecomunicaciones (UIT). (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad*. Obtenido de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf

Unión Internacional de Telecomunicaciones (UIT). (2019). *Global Cybersecurity Index (GCI) 2018*. Obtenido de Global Cybersecurity Index (GCI) 2018: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf