Documento CONPES

3854

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

POLÍTICA NACIONAL DE SEGURIDAD DIGITAL

Ministerio de Tecnologías de la Información y las Comunicaciones
Ministerio de Defensa Nacional
Dirección Nacional de Inteligencia
Departamento Nacional de Planeación

Versión aprobada

Bogotá, D.C., 11 de abril de 2016

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL
CONPES

Juan Manuel Santos Calderón
Presidente de la República

Germán Vargas Lleras
Vicepresidente de la República

María Lorena Gutiérrez Botero
Ministra de la Presidencia

Juan Fernando Cristo Bustos
Ministro del Interior

Mauricio Cárdenas Santamaría
Ministro de Hacienda y Crédito Público

Luis Carlos Villegas Echeverri
Ministro de Defensa Nacional

Alejandro Gaviria Uribe
Ministro de Salud y Protección Social

María Lorena Gutiérrez Botero
Ministra de Minas y Energía (E)

Gina Parody d'Echeona
Ministra de Educación Nacional

Luis Felipe Henao Cardona
Ministro de Vivienda, Ciudad y Territorio

Natalia Abello Vives
Ministra de Transporte

María Ángela Holguín Cuéllar
Ministra de Relaciones Exteriores

Yesid Reyes Alvarado
Ministro de Justicia y del Derecho

Aurelio Iragorri Valencia
Ministro de Agricultura y Desarrollo Rural

Luis Eduardo Garzón
Ministro de Trabajo

Cecilia Álvarez-Correa Glen
Ministra de Comercio, Industria y Turismo

Gabriel Vallejo López
Ministro de Ambiente y Desarrollo Sostenible

David Luna Sánchez
Ministro de Tecnologías de la Información y las Comunicaciones

Mariana Garcés Córdoba
Ministra de Cultura

Simón Gaviria Muñoz
Director General del Departamento Nacional de Planeación

Luis Fernando Mejía Alzate
Subdirector Sectorial

Manuel Fernando Castro Quiroz
Subdirector Territorial y de Inversión Pública

Resumen ejecutivo

El creciente uso del entorno digital en Colombia para desarrollar actividades económicas y sociales, acarrea incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente. No hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en este entorno.

El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del país; y (ii) lucha contra el cibercrímen. Si bien esta política ha posicionado a Colombia como una de los líderes en la materia a nivel regional, ha dejado de lado la gestión del riesgo en el entorno digital. Enfoque esencial en un contexto en el que el incremento en el uso de las TIC para realizar actividades económicas y sociales, ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Hecho que demanda una mayor planificación, prevención, y atención por parte de los países.

Es precisamente por esto que la política nacional de seguridad digital, objeto de este documento, cambia el enfoque tradicional al incluir la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital. Esto lo hace bajo cuatro principios fundamentales y cinco dimensiones estratégicas, que rigen el desarrollo de esta política. De los primeros destaca que la política nacional de seguridad digital debe involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas. Principios que se reflejan en las dimensiones en las que esta política actuará, las cuales determinan las estrategias para alcanzar su objetivo principal: fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital. Para lograrlo, se implementarán acciones en torno a cinco ejes de trabajo.

En primer lugar, se establecerá un marco institucional claro en torno a la seguridad digital. Para esto, se crearán las máximas instancias de coordinación y orientación superior en torno a la seguridad digital en el gobierno, y se establecerán figuras de enlace sectorial en todas las entidades de la rama ejecutiva a nivel nacional. En segundo lugar, se crearán las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación activa y permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos responsables en el entorno digital. Como tercera medida, se fortalecerá la defensa y seguridad nacional en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos. Por

último, se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Para poner en marcha esta política, se ha construido un plan de acción que se ejecutará durante los años 2016 a 2019 con una inversión total de 85.070 millones de pesos. Las principales entidades ejecutoras de esta política son el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación.

Se estima que la implementación de la política nacional de seguridad digital al año 2020 podría impactar positivamente la economía de Colombia, generándose durante los años 2016 a 2020 alrededor de 307.000 empleos y un crecimiento aproximado de 0,1% en la tasa promedio de variación anual del Producto Interno Bruto (PIB), sin generar presiones inflacionarias.

Clasificación: L86, F52.

Palabras clave: Seguridad digital, ciberdefensa, ciberseguridad, ciberlavado, ciberterrorismo, cibercrímen, gestión de riesgos, entorno digital, economía digital, prosperidad económica y social, amenazas cibernéticas, infraestructuras críticas cibernéticas nacionales, ciberespacio.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

SIGLAS Y ABREVIACIONES

CCOC	Comando Conjunto Cibernético del Comando General de las Fuerzas Militares de Colombia
CCP	Centro Cibernético Policial de la Policía Nacional de Colombia
CICTE	Comité Interamericano Contra el Terrorismo de la OEA
colCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia
CONPES	Consejo Nacional de Política Económica y Social de Colombia
CRC	Comisión de Regulación de Comunicaciones de Colombia
CSIRT	Equipos de Respuestas ante Incidentes de Seguridad (en inglés, *Computer Security Incident Response Team*)
CSIRT PONAL	CSIRT de la Policía Nacional de Colombia
DANE	Departamento Administrativo Nacional de Estadística
DNI	Departamento Administrativo Dirección Nacional de Inteligencia
DNP	Departamento Nacional de Planeación
ECV	Encuesta de Calidad de Vida del DANE
INTERPOL	Organización Internacional de Policía Criminal
ITI	Consejo mundial de la industria de tecnologías de la información (en inglés, *Information Technology Industry Council)*
MEGC	Modelo de Equilibrio General Computable
MIPYMES	Micro, Pequeñas y Medianas empresas
OCDE	Organización para la Cooperación y Desarrollo Económico
OEA	Organización de Estados Americanos
OTAN	Organización del Tratado del Atlántico Norte
PIB	Producto Interno Bruto
TIC	Tecnologías de la Información y las Comunicaciones
UIAF	Unidad de Información y Análisis Financiero de Colombia
UIT	Unión Internacional de Telecomunicaciones

1. INTRODUCCIÓN

El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica[1] y el incremento en la oferta de servicios disponibles en línea[2], evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país.

Desafortunadamente, el incremento en la participación digital de los ciudadanos, trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo. El primer enfoque corresponde al adoptado por el Documento CONPES 3701 *Lineamientos de política para ciberseguridad y ciberdefensa*[3] para contrarrestar las amenazas cibernéticas en el entorno digital. Política que enmarca los esfuerzos que ha adelantado el Gobierno nacional en el tema, y que logró (i) implementar en el país la institucionalidad existente en cuanto a seguridad y defensa digital; y (ii) posicionar a Colombia a nivel internacional como uno de los líderes en ciberseguridad y ciberdefensa.

No obstante el éxito de la política de ciberseguridad y ciberdefensa, se hace necesario complementar sus esfuerzos teniendo en cuenta el segundo enfoque mencionado anteriormente, la gestión de riesgos. En este sentido, la política nacional de seguridad digital, objeto de este documento, además de contemplar la defensa y seguridad nacional en el entorno digital, incluidas las infraestructuras críticas cibernéticas nacionales, incluye componentes como la gobernanza, la educación, la regulación, la cooperación internacional

---

[1] Como ejemplo, según la Superintendencia Financiera de Colombia (2015), el número de operaciones financieras (monetarias y no monetarias) en Colombia mediante el canal *Internet* aumentó en un 45% de 2012 a 2014 y mediante el canal *Telefonía móvil* en un 252%. En el primer semestre de 2015, el sistema financiero colombiano realizó 2.026 millones de operaciones por 3.237,8 billones de pesos, de los cuales mediante el canal *Internet* se realizaron 863 millones de operaciones (un 43% del total) por valor de 1.092,61 billones de pesos (un 34% del total).

[2] Según el Programa Gobierno en línea del Ministerio de Tecnologías de la Información y las Comunicaciones, el porcentaje de ciudadanos colombianos que usan canales o medios electrónicos para (i) obtener información, (ii) realizar trámites, (iii) obtener servicios, (iv) presentar peticiones, quejas o reclamos, o (v) participar en la toma de decisiones, pasó del 30% en 2009 al 65% en 2014. Lo mismo sucedió con las empresas colombianas, pasando del 24% en 2009 al 81% en 2014. Adicionalmente, por medio del portal del Estado colombiano se realizaron 1.038 trámites en línea en el 2015.

[3] Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

y nacional, la investigación y desarrollo, y la innovación. Adicionalmente, amplía la población objetivo, del Estado (política de ciberseguridad y ciberdefensa) a todos los ciudadanos, sectores económicos y organizaciones (múltiples partes interesadas[4]). Lo anterior, reconociendo la necesidad de diferenciar los objetivos de ciberseguridad y ciberdefensa, de los de prosperidad económica y social, y fortaleciendo este último.

El desarrollo de una economía digital sólida y segura es primordial para el país, ya que esta contribuye positivamente a la prosperidad económica y social del mismo. Su crecimiento y correcto funcionamiento requiere la construcción de un entorno digital abierto[5], seguro y confiable, acorde con el aumento y dinamismo de las actividades digitales de los individuos. Características que se logran más efectivamente desde un enfoque de gestión del riesgo que involucra a todas las partes interesadas, lo cual es estratégico al permitirles tomar decisiones socioeconómicas informadas para maximizar las oportunidades en el entorno digital. Para esto, se debe abordar el riesgo de seguridad digital como un reto económico y social en lugar de un reto puramente técnico.

El presente documento está organizado de la siguiente manera, siendo esta sección la introducción. La segunda sección presenta los antecedentes normativos y de política pública que motivan esta política. La tercera sección explica el marco conceptual; mientras que la cuarta sección presenta y caracteriza la problemática que esta política busca solucionar. La quinta sección define la Política nacional de seguridad digital para Colombia, presentando su objetivo general, los objetivos específicos y las estrategias que se implementarán para alcanzarlos. En la misma sección se presenta el cronograma de seguimiento a la implementación de esta política y el esquema para su financiamiento. Finalmente, en la sexta sección se presentan las recomendaciones para la implementación de la política.

2. ANTECEDENTES Y JUSTIFICACIÓN

La rápida evolución y adopción de las TIC como base para cualquier actividad socioeconómica, el creciente uso de las mismas por toda la sociedad, la rápida expansión de las redes de telecomunicaciones, y el fenómeno de convergencia[6], han marcado la dinámica del sector de las TIC y las economías de los países durante los últimos años (UIT, 2015); y la seguirán marcando, ya que las tendencias internacionales muestran que el entorno digital es dinámico y crece continuamente (Tabla 1). Entorno donde se ha consolidado una economía basada en tecnologías (economía digital), cuya evolución y maduración genera impactos positivos en todos los ámbitos de la sociedad y en todos los

[4] En la sección 3.1 del documento se define este término.

[5] En el glosario del documento se define este término.

[6] Evolución tecnológica que consiste en suministrar todos los servicios de comunicaciones por la red de Internet.

sectores económicos que han estado a la vanguardia de esta tendencia para lograr mayor conocimiento de sus clientes, mayor productividad, competitividad y creación de nuevos modelos de negocio (CEPAL, 2014).

Tabla 1. Proyecciones de algunos indicadores de uso de las TIC a nivel global

Proyecciones	2015	2020	Incremento porcentual
Más usuarios de banda ancha móvil	3 mil millones	4 mil millones	33%
Más terminales conectados	16,3 mil millones	24,4 mil millones	49%
Más datos generados	8,8 zettabytes	44 zettabytes	400%
Más tráfico IP de red (mensual)	72,4 exabytes	168 exabytes	132%
Dispositivos (Internet de las cosas)	15 mil millones	200 mil millones[(a)]	1200%
Tamaño del mercado de la nube pública global	USD 97 mil millones	USD 159 mil millones	63%

Fuente: Adaptado de INTEL SECURITY (2015a).
Nota: [(a)] Proyección a 2018.

No obstante lo anterior, la creciente relevancia del entorno digital sobre las actividades socioeconómicas, y su alto dinamismo, ha traído consigo un conjunto de incertidumbres, riesgos, amenazas, vulnerabilidades e incidentes de diversos tipos[7], a los que se encuentran expuestos los individuos y las organizaciones, públicas y privadas. La Tabla 2 resume algunos casos relevantes sobre ataques cibernéticos en el mundo durante el 2014, en donde se puede apreciar que estos afectan a cualquier sector de la economía, con consecuencias que pueden impactar de manera negativa a millones de personas en el mundo, a la defensa y seguridad nacional y, en consecuencia, a la prosperidad económica y social.

Previendo esta realidad mundial, y en vista de los ataques cibernéticos que sufrían diferentes países del mundo en la década pasada, y del incremento en el uso de las TIC en Colombia durante ese tiempo; en el 2011, el Gobierno nacional de Colombia estableció los lineamientos de política para ciberseguridad y ciberdefensa. Política que se presenta

[7] Los incidentes digitales se basan, generalmente, en algún software malintencionado, diseñado para perjudicar o hacer un uso no lícito de los sistemas de información de las organizaciones. En particular, el malware (término compuesto en inglés -*malicious software*- para llamar a cualquier software malicioso) es un tipo de software que tiene como propósito infiltrarse y dañar un terminal o un sistema de información sin el consentimiento de sus propietarios. Los tipos de amenazas cibernéticas más comunes alrededor del mundo en 2014 y 2015, fueron los troyanos (en inglés, *trojans*), los gusanos (en inglés, *worms*) y los virus (en inglés, *viruses*) (ISS, 2014). También se destaca el malware de suplantación de identidad (en inglés, *phishing*) caracterizado por intentar adquirir información confidencial de forma fraudulenta.

brevemente en la siguiente sección, junto con sus principales logros y las actividades de revisión realizadas a la fecha.

Tabla 2. Grandes casos de ataque cibernéticos en el mundo en el 2014

Organización afectada	Sector	Impacto
Snapchat	Red social	4,5 millones de nombres y números móviles comprometidos
Kickstarter	*Crowd funding*	5,6 millones de víctimas
Korean Telecom	Telecomunicaciones	12 millones de suscriptores comprometidos
Heartbleed	*Software*	Primera de tres vulnerabilidades de fuente abierta
Ebay	Compras	Base de datos de 145 millones de compradores comprometida
PF chang´s	Comidas	Más alta violación de información de alto nivel del mes
Energetic bear	Energía	Operación de ciberespionaje a la industria de energía
Cybervor	Tecnología	1,2 billones de credenciales comprometidas
iCloud	Entretenimiento	Cuentas de celebridades comprometidas
Sandworm	Tecnología	Ataque cibernético a la vulnerabilidad de Windows
Sony Pictures	Entretenimiento	Más alta violación de alto nivel del año
Inception Framework	Sector público	Operación de ciberespionaje a sector público

Fuente: Adaptado de Verizon (2015).

2.1. Política pública nacional

Con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, en el 2011, el Gobierno nacional expidió el Documento CONPES 3701 *Lineamientos de política para ciberseguridad y ciberdefensa*[8]. Esta política concentró los esfuerzos del país en contrarrestar el incremento de las amenazas informáticas que lo afectaban significativamente[9], y en desarrollar un marco normativo e institucional para afrontar retos en aspectos de seguridad cibernética. A continuación se presentan de manera general los avances en la implementación de dichos lineamientos de política, y las actividades de revisión de los mismos durante los años 2014 y 2015.

[8] Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

[9] Un caso a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo *hacktivista* autodenominado Anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en línea y de los Ministerios del Interior, de Justicia, de Cultura y de Defensa, dejando fuera de servicio sus páginas web por varias horas (DNP, 2011).

El objetivo general del Documento CONPES 3701 fue fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa)[10], creando un ambiente y unas condiciones para brindar protección en el ciberespacio. Para cumplir este objetivo general, se formularon tres objetivos específicos: (i) implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional; (ii) brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad; y (iii) fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.

Respecto al cumplimiento de los indicadores establecidos para el seguimiento al documento CONPES mencionado, se evidencia el cumplimiento del 79% de las actividades propuestas en el plan de acción. Lo anterior, de acuerdo a lo establecido por el Departamento Nacional de Planeación (DNP), mediante reporte con corte a junio de 2015. Los principales avances en materia de institucionalidad, capacitación, legislación y cooperación se presentan a continuación.

Institucionalidad

El principal logro alcanzado por la política de ciberseguridad y ciberdefensa, fue el fortalecimiento de la institucionalidad en el tema. Lo anterior, fue posible por medio de la creación de nuevas instancias tales como el Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOC) 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 en la Superintendencia de Industria y Comercio, la Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones, el Comité de ciberdefensa de las Fuerzas Militares, y

[10] El Documento CONPES 3701 definió *Ciberseguridad* como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética; y *Ciberdefensa* como la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

las Unidades cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana.

Adicionalmente, en el marco del Documento CONPES 3701, se creó la Comisión Nacional Digital y de Información Estatal, mediante el Decreto 32 de 2013[11] del Ministerio de Tecnologías de la Información y las Comunicaciones. Instancia que tiene el objeto de ejercer la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para interacción con los ciudadanos, y el uso efectivo de la información en el Estado colombiano.

Capacitación

La capacitación y entrenamiento se han fortalecido desde diferentes frentes de actuación. Desde aspectos como campañas de sensibilización para el uso responsable de Internet con énfasis en niños y jóvenes, hasta la provisión de formación especializada a servidores públicos.

El equipo de colCERT adelantó procesos de capacitación en los que participaron funcionarios del Estado y de empresas del sector privado, así como programas de sensibilización y concientización para los ciudadanos en general respecto a la ciberseguridad y ciberdefensa. Por su parte, el CCOC fortaleció las capacidades de ciberdefensa propias y las de las unidades cibernéticas. De igual manera, brindó lineamientos y directrices al interior de las instituciones en este tema, con el fin de garantizar la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional. Por otro lado, el CCP ha ejecutado campañas de sensibilización dirigidas a la ciudadanía en general en torno a la ciberseguridad, así como acciones para fortalecer la investigación y judicialización de delitos cibernéticos.

Adicionalmente, el país ha avanzado significativamente en la generación de oferta académica especializada en esta materia. En el año 2011, Colombia contaba con doce programas académicos a nivel nacional, desde el nivel técnico hasta el de maestría, mientras que a la fecha cuenta con más de cincuenta programas, y con una amplia gama de cursos de educación no formal, que incluyen certificaciones de reconocimiento internacional.

Legislación

En el marco de la política de ciberseguridad y ciberdefensa, el país desarrolló y aprobó normas destinadas específicamente a aspectos tales como la protección de datos personales,

[11] Por el cual se crea la Comisión Nacional Digital y de Información Estatal.

la regulación sobre protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual a menores de edad.

Adicional a lo anterior, se adoptaron diferentes leyes de protección a los derechos fundamentales. Por ejemplo, la Ley 1581 de 2012[12] tuvo por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. En esta misma línea, se desarrolló un marco jurídico que incluye el reconocimiento de los datos e información como bien jurídico tutelado.

Cooperación y posicionamientointernacional

En 2013, a través del Ministerio de Relaciones Exteriores, el país solicitó formalmente la adhesión a la Convención de Europa sobre cibercriminalidad, también conocido como Convenio de Budapest[13]. Este Convenio establece los principios de un acuerdo internacional sobre seguridad cibernética y la sanción de delitos cibernéticos. En el mismo año, se estableció un convenio multilateral con el Foro Económico Mundial, para identificar y abordar los riesgos sistemáticos globales derivados de la conectividad, cada vez mayor, entre personas, procesos y objetos.

A través del Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), se ha logrado trabajar con varios Equipos de respuesta ante incidencias de seguridad (CSIRT) en la región. Colombia es parte de una red de alerta que proporciona formación técnica a personal especializado, promueve el desarrollo de estrategias nacionales sobre seguridad cibernética, y fomenta el desarrollo de una cultura que permita su fortalecimiento en el continente.

En este mismo frente, el país ha suscrito acuerdos con organizaciones internacionales como el Antiphishing Working Group. Lo anterior, con el fin de acceder a recursos y programas específicos en ciberseguridad y ciberdefensa, y hacer parte de esta coalición con empresas de la industria, autoridades legales y entidades de gobierno, que colaboran en función de contar con mejores mecanismos de alarma y respuesta frente a ataques

[12] Por la cual se dictan disposiciones generales para la protección de datos personales.

[13] El 11 de septiembre de 2013, como resultado del análisis de la normatividad de Colombia en materia de delito cibernético, el Consejo de Ministros del Consejo de Europa dio su aprobación para invitar a Colombia a adherirse a la Convención sobre delito cibernético. En esa oportunidad, también se abrió la puerta para que fuera parte de su Protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. A partir de tal decisión, Colombia tiene un máximo de cinco años para adherir al instrumento internacional.

cibernéticos. Estas alianzas también se han fortalecido en el contexto local con actores de la industria nacional.

Por su parte, la Policía Nacional, a través del CCP, sostiene mecanismos de cooperación con homólogos en otros países y agencias de ley a nivel mundial, tales como: la Organización Internacional de Policía Criminal (INTERPOL), la Oficina Federal de Investigaciones de los Estados Unidos (FBI), la Administración para el Control de Drogas de los Estados Unidos (DEA), el Centro Europeo contra el cibercrímen (EC3), la Comunidad de Policías de América (AMERIPOL), la Agencia Internacional de Cooperación Coreana (KOICA), la Agencia Nacional contra el crimen del Reino Unido (NCA), el Grupo de Trabajo Americano de delitos Tecnológicos del INTERPOL (GLDTA) y el Programa de Asistencia Anti-Terrorismo de Estados Unidos (ATA). Esto, con el fin de combatir el cibercrímen desde diferentes flancos.

Otro aspecto a resaltar, es que Colombia cuenta con ocho CSIRT con membresía en el Foro de equipos de seguridad y respuesta de incidentes, llamado FIRST[14] por sus siglas en inglés. Esto les permite responder de manera más eficaz a incidentes de seguridad, al tener acceso a información acerca de las mejores prácticas, ser invitados a eventos y a capacitaciones y cursos relacionados con la seguridad digital.

En el ámbito regional, Colombia se ha posicionado como uno de los países que más ha avanzado en aspectos relacionados con ciberseguridad y ciberdefensa. Lo anterior, se refleja en indicadores de eficiencia comparativa como el *índice mundial de ciberseguridad* de la Unión Internacional de Telecomunicaciones (UIT). Según este, en 2014 el país se ubicaba en el quinto lugar del ranking a nivel regional, siendo superado por Estados Unidos, Canadá, Brasil y Uruguay; mientras que en el plano mundial comparte la novena posición, junto con países como Dinamarca, Egipto, Francia y España.

Finalmente, en materia de cooperación nacional, el CCOC viene adelantando el proceso de elaboración del catálogo de infraestructuras críticas cibernéticas nacionales en el país. El catálogo en mención permitirá, a futuro, coordinar y gestionar los planes y programas de protección y defensa a infraestructuras críticas cibernéticas nacionales. A 2015, el Ministerio de Defensa Nacional había elaborado la Guía para la Identificación de Infraestructura Crítica Cibernética, la cual se constituye como el insumo principal de dicho catálogo, construido en coordinación con las múltiples partes interesadas.

[14] FIRST es la principal organización mundial y líder reconocido en respuesta a incidentes digitales. Cuenta con más de 300 miembros, repartidos en África, América, Asia, Europa y Oceanía. Este foro reúne una variedad de equipos de respuesta a incidentes del gobierno, industria y academia, y tiene como objetivo fomentar la cooperación y la coordinación en la prevención de incidentes, para estimular la reacción rápida ante los mismos, y para promover el intercambio de información entre los miembros y la comunidad en general.

2.1.1. Revisión y evaluación de los lineamientos de política

A pesar de los avances logrados mediante el desarrollo de las acciones establecidas en el Documento CONPES 3701, los resultados no pueden interpretarse como una capacidad suficiente, integral y efectiva de preparación y respuesta ante ataques cibernéticos. Esto, por la continua evolución, crecimiento y sofisticación de los ataques cibernéticos, que ponen de manifiesto la necesidad de adoptar nuevas medidas y controles que permitan proteger a los ciudadanos y al Estado.

El incremento en el volumen de incidentes es resultado de varios factores. Uno de ellos es la migración de las actividades criminales al entorno digital, lo que ha impulsado la profesionalización de los ataques cibernéticos. Otro factor es la aparición de nuevos tipos de terroristas, y sus respectivos seguidores, quienes han extendido sus acciones al entorno digital, multiplicando los ataques a sitios de internet que afectan a la infraestructura física y a la población en general (OCDE, 2015a).

En febrero de 2014, el Presidente Juan Manuel Santos, consciente del incremento de incidentes digitales, solicitó la creación de una comisión de alto nivel con el fin de trabajar en el fortalecimiento de las políticas de ciberseguridad y ciberdefensa para el país. Fortalecimiento que busca fomentar el uso de un entorno digital seguro para el ciudadano y para el propio Estado, a fin de promover y robustecer el desarrollo político, económico y social (i) respetando los derechos constitucionales; (ii) evaluando las vulnerabilidades a las que se encuentra expuesta Colombia en este campo; y (iii) valorando la necesidad de adecuarse a los retos impuestos por los avances tecnológicos y las amenazas cibernéticas. La comisión es liderada por los ministros de Defensa Nacional, de Justicia y del Derecho, y de Tecnologías de la Información y las Comunicaciones, apoyados por una comisión internacional.

A partir del establecimiento de esta comisión, los ministerios a cargo convocaron la realización de mesas de trabajo durante los años 2014 y 2015 con expertos nacionales e internacionales. El equipo de expertos de alto nivel contó con la participación de miembros de los ministerios que conforman la comisión, del colCERT, del CCOC, del CCP, de las unidades cibernéticas de las Fuerzas Militares, y del sector público y privado. El equipo internacional tuvo el apoyo de la OEA, y contó con la presencia de expertos de los gobiernos de Canadá, España, Estados Unidos, Estonia, Corea del Sur, Israel, Reino Unido, República Dominicana y Uruguay, así como con miembros del Foro Económico Mundial, de la OCDE, del Consejo de Europa y de la INTERPOL.

En la mesa de expertos nacionales, la discusión se orientó en la revisión de los aspectos ya existentes de la política, y en los que aún se encuentran ausentes, girando en torno a cinco dimensiones: (i) gobernabilidad y coordinación efectiva; (ii) preparación y prevención; (iii)

conocimiento de la situación actual; (iv) resiliencia, recuperación y respuesta; y (v) efectiva cooperación e intercambio de información (OEA, 2014).

Por su parte, la mesa internacional emitió recomendaciones enfocadas en la necesidad de: (i) desarrollar una visión estratégica global para la ciberseguridad; (ii) adoptar un enfoque nacional de la gestión de riesgos; (iii) establecer un marco institucional claro; (iv) establecer un proceso sistemático para involucrar a todos los interesados en el desarrollo de la estrategia y su implementación; y (v) adoptar una estrategia para la protección y defensa de las infraestructuras críticas cibernéticas nacionales, siendo conscientes de la necesidad de fortalecer las capacidades operativas, administrativas, humanas, científicas, tecnológicas y de infraestructura física de las instituciones (OEA, 2014).

Tanto la mesa nacional como la internacional coincidieron en la necesidad de incorporar nuevos elementos a las estructuras institucionales, a la legislación y a las acciones existentes; y de incluir en la política principios, lineamientos y directrices en lo relacionado a los derechos humanos en el entorno digital. Esto, porque se concluyó que aunque la política existente había sido efectiva en contrarrestar ataques cibernéticos que atentaban contra la defensa y seguridad nacional, en ella no se tuvieron en cuenta objetivos relacionados con la prosperidad económica y social (que se creían implícitos en los de defensa y seguridad nacional). Objetivos que pueden ser alcanzados garantizando un entorno digital seguro y abierto, que genere confianza en los ciudadanos para que se incrementen sus participantes, y se fortalezca la economía digital. Así lo han reconocido diferentes países del mundo, que han adaptado su política en la materia al nuevo contexto.

2.2. Mejores prácticas internacionales

Durante la última década, los gobiernos han venido utilizando instrumentos e implementando estrategias para reducir las incertidumbres y los riesgos, así como para contrarrestar adecuadamente las amenazas cibernéticas y los incidentes en el entorno digital. En las regiones desarrolladas del mundo, las estrategias de seguridad digital tienen un enfoque integral, que abarca aspectos económicos, sociales, educativos, jurídicos, de aplicación de la ley, técnicos, diplomáticos, militares y relacionados con la inteligencia. Las consideraciones de soberanía en la formulación de políticas de seguridad cibernética son cada vez más relevantes y se puede notar una mayor participación de los militares y de las ramas de inteligencia del gobierno. No obstante, cuando las estrategias de seguridad cibernética se centran exclusivamente en asuntos militares y de inteligencia, es posible que no alcancen un equilibrio adecuado entre la seguridad y los derechos, tales como la privacidad y la libertad de expresión y de asociación (BID & OEA, 2016).

Varias organizaciones multilaterales – como la OTAN, la OCDE, la UIT y la OEA – y gremios globales del sector privado, han analizado cómo abordar la seguridad digital bajo

las condiciones actuales del entorno digital. Todos los estudios[15] coinciden en que los gobiernos deben adoptar un enfoque de política que se adapte a los cambios del mercado, y permita que las organizaciones y los ciudadanos entiendan, evalúen y tomen medidas correctas para manejar las incertidumbres y los riesgos en el entorno digital. Enfoque que llaman de *gestión de riesgos.* OCDE (2015a) explica que la gestión de riesgos es estratégica para la toma de decisiones socioeconómicas, y que las medidas que se toman bajo este enfoque soportarán los objetivos de las actividades socioeconómicas y no las debilitará.

Según UIT (2011), las medidas para gestionar los riesgos en el entorno digital deben tener en cuenta la *salvaguarda de los derechos humanos y de los valores nacionales*. Lo anterior, debido a que en el entorno digital aplican reglas sociales básicas, de tal forma que los derechos humanos y valores nacionales se extienden a dicho entorno, y se deben considerar las consecuencias (positivas o negativas) sobre estos al definir las medidas de seguridad digital. Medidas que según los estudios en discusión deben afectar positivamente el desarrollo de actividades socioeconómicas en el entorno digital.

Con respecto a los involucrados en la política como agentes creadores de un entorno digital seguro, todos los estudios coinciden en que cada actor que depende del entorno digital para desarrollar algunas o todas sus actividades económicas y sociales, debe ser vinculado y debe tener un papel particular en esta labor. Esto es llamado un *enfoque de múltiples partes interesadas,* en el que además se debería promover una *responsabilidad compartida entre todas las partes*. Responsabilidad para gestionar los riesgos de seguridad digital, de acuerdo con su rol, el contexto y su habilidad para actuar (UIT, 2011).

Por su parte, el Consejo mundial de la industria de tecnologías de la información (ITI por sus siglas en inglés) expone que para lograr un enfoque de múltiples partes interesadas y responsabilidad compartida, los gobiernos deben orientar sus estrategias a la gestión de riesgos, pero también a la *concientización, sensibilización y educación*. Los gobiernos deben buscar que todas las partes interesadas sean conscientes de su papel con el fin de hacer frente a los riesgos de seguridad digital. El ITI resalta que los esfuerzos deben incluir la sensibilización, a través de los sistemas educativos, a los ciudadanos de todas las edades sobre la seguridad digital, y que las múltiples partes interesadas necesitan saber cómo afrontar las incertidumbres y reducir los riesgos.

Al revisar diferentes políticas o estrategias nacionales de ciberseguridad y ciberdefensa, se evidencia que estas han evolucionado o migrado hacia estrategias nacionales de seguridad digital que aplican las recomendaciones expuestas en los párrafos anteriores, especialmente la gestión de riesgos y la responsabilidad compartida (Anexo B).

[15] El marco técnico de referencia lo componen los siguientes documentos: UIT (2011), OTAN (2012), OEA, (2014a), OEA (2015a), OCDE (2015b), ITI (2011) e ITI (2012).

Se pasó del diseño de estrategias de ciberseguridad y ciberdefensa, que se centran principalmente en objetivos de defensa y seguridad nacional en el entorno digital, hacia el diseño de estrategias integrales con un conjunto de principios que se enmarca en la gestión de riesgos de seguridad digital. Lo anterior, se hace distinguiendo los objetivos de prosperidad económica y social de los objetivos de defensa del país, de lucha contra el crimen y contra la delincuencia en este entorno. Es el caso de República Checa, Islandia, Portugal, Malta, Irlanda y Francia. Países que actualizaron sus estrategias nacionales en el 2015, siendo Francia el único país que actualizó su política después (19/10/2015) de que la OCDE emitiera recomendaciones sobre la gestión de riesgos de seguridad digital (17/09/2015).

El Anexo B presenta un análisis comparativo de las estrategias y políticas nacionales de seguridad digital de Francia, República Checa, Malta, Irlanda y Portugal, en donde se concluye que los principales componentes de las mismas son: (i) principios fundamentales que rigen la estrategia, como el Estado de derecho, la subsidiariedad, la proporcionalidad, el enfoque de gestión de riesgos o la responsabilidad compartida; (ii) objetivos estratégicos, como combatir el cibercrímen, fortalecer la ciberdefensa nacional, promover la cooperación nacional e internacional o proveer educación y desarrollo de conocimiento; y para Malta y Portugal, (iii) dimensiones estratégicas en las que actúa la estrategia, como el marco político, el marco legal, la gestión de riesgos, la cultura o la educación. Dichas estrategias, como ya fue mencionado, encuentran una característica común en el enfoque integral basado en riesgos, que diferencia el objetivo de prosperidad económica y social de los objetivos de ciberseguridad y ciberdefensa.

2.3. Marco normativo

En esta sección se presenta brevemente el marco normativo internacional y nacional relacionado con la seguridad digital.

2.3.1. Normativa nacional

A nivel nacional, algunos fundamentos constitucionales en torno a la seguridad digital se encuentran en: (i) el artículo dos en donde se establece como fin esencial del Estado la promoción de la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; (ii) el capítulo 1 del título II de la Constitución Política, que trata sobre los derechos fundamentales, en particular el artículo 15 que reconoce el derecho a la intimidad personal y familiar y al buen nombre, y la obligación del Estado de respetarlos y hacerlos respetar, y el artículo 20 en donde se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación; (ii) el artículo

76 que establece que el espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado; (iii) el artículo 101 que incluye al espectro electromagnético como parte del territorio colombiano; o (iv) el artículo 217 que establece que las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional, entre otros.

En lo referente a otras normas, Colombia enmendó el Código Penal en 2009, mediante la Ley 1273[16], y el Código de Procedimiento Penal en 2011, mediante la Ley 1453[17]. Es decir, se cuenta con una legislación procesal penal integral y efectiva para abordar los delitos cibernéticos, y reconoce los tratados internacionales con INTERPOL y EUROPOL. Adicionalmente, las fuerzas del orden y el poder judicial están habilitados legalmente para investigar y manejar casos de delincuencia cibernética. La Ley 1581 establece un marco básico para la protección de datos, divulgación y denuncia de las violaciones de seguridad.

Frente a las leyes de carácter ordinario, adicionalmente existen varios instrumentos que regulan diversos temas asociados con la seguridad digital, de manera compleja y dispersa. Temas como el comercio electrónico, la pornografía y la explotación sexual de menores en el ciberespacio, la racionalización de trámites y procedimientos, los derechos de autor y conexos, entre otros.

También se aprecia un desarrollo reglamentario de leyes que contienen asuntos particulares frente a temas como el habeas data, la firma electrónica, los mecanismos de autenticación, las entidades de certificación abierta y el registro nacional de bases de datos.

Finalmente, existen otros decretos y actos administrativos relevantes que regulan diversas actividades relacionadas con el entorno digital, tales como la Circular Externa de la Superintendencia Financiera de Colombia 052 de 2007 (estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios), las Resoluciones CRC 3066 y 3067 de 2011 (Régimen integral de protección de los derechos de los usuarios e indicadores de calidad para los servicios de telecomunicaciones), Decreto 1704 de 2012 (interceptación legal de comunicaciones), Decreto Ley 019 de 2012 (entidades de certificación digital), Resolución de la Superintendencia de Industria y Comercio de Colombia (SIC) No. 76434 de 2012 (protección de datos personales), Decreto 2573 de 2014 (Gobierno en línea), entre otros.

---

[16] Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

[17] Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad.

El Anexo C presenta una descripción del marco normativo nacional.

2.3.2. Normativa internacional

Entre los instrumentos internacionales que tienen relación con la seguridad digital se encuentran el Convenio sobre Ciberdelincuencia del Consejo de Europa (conocido como el convenio sobre Cibercriminalidad de Budapest) mediante el cual se adopta una legislación que facilita la prevención de las conductas delictivas y contribuye con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas. También destaca la Resolución AG /RES 2004 (XXXIV-O/04) de la Asamblea General de la OEA, mediante la cual se establece una estrategia integral para combatir las amenazas a la seguridad cibernética con un enfoque multidimensional y multidisciplinario, para la creación de una cultura de la seguridad cibernética, y la Decisión 587 de la Comunidad Andina por la cual se establecen los lineamientos de la Política de seguridad externa común andina.

Desde el punto de vista de ciberdefensa, se destaca la Declaración de la Cumbre de Gales de la OTAN en 2014, en donde se resaltan acuerdos para abordar la ciberseguridad en los países de dicha alianza.

Finalmente, se destaca la Declaración sobre la protección de infraestructura crítica ante las amenazas emergentes (aprobado durante la quinta sesión plenaria, celebrada el 20 de marzo de 2015). En esta, entre otros, la Secretaría Ejecutiva del CICTE de la OEA desarrolla un proyecto de asistencia técnica que permite a los Estados americanos miembros la elaboración de un listado de su infraestructura crítica y su clasificación, basados en sus respectivos activos, sistemas, redes y funciones esenciales, para hacer posible la mejor evaluación de vulnerabilidades, brechas, amenazas, riesgos e interdependencia.

El Anexo D presenta el marco normativo internacional.

Los antecedentes nacionales e internacionales expuestos en esta sección, han mostrado que la política de ciberseguridad y ciberdefensa adoptada por Colombia en el 2011, debe ser complementada para responder adecuadamente a los nuevos tipos de incertidumbres e incidentes digitales, los cuales son el resultado de un entorno digital creciente y dinámico. Incidentes que pueden afectar a cualquier sector de la economía o ciudadano, y no solo al Estado; y que, según diversos estudios, deben ser abordados desde un enfoque de riesgos en el que se involucren a todas las partes interesadas, distinguiendo así los objetivos de prosperidad económica y social (fortalecer la economía digital), de los objetivos de ciberseguridad y ciberdefensa.

Esta sección también permitió evidenciar que Colombia dispone de un marco normativo nacional disperso en torno a la seguridad digital que comprende leyes, decretos y otros actos expedidos bajo condiciones diferentes a las actuales. Teniendo en cuenta todo lo anterior, se

hace necesario plantear una nueva política nacional de seguridad digital que responda a los retos actuales, fomente el crecimiento de la economía digital e incorpore los elementos que nos permitan continuar siendo parte de los países líderes en el tema.

3. MARCO CONCEPTUAL

En primer lugar, esta sección expone los conceptos básicos sobre la seguridad digital. Paso seguido, describe las características generales que debe tener una estrategia de gestión de riesgos de seguridad digital según las mejores prácticas internacionales; y finalmente, a partir de estas y teniendo en cuenta el contexto nacional, establece los principios y dimensiones estratégicas que definen la política nacional de seguridad digital en el país.

3.1. Conceptos básicos

Después de un trabajo de más de dos años de revisión y análisis, y de más de treinta años de experiencias respecto a la manera como se abordaron las incertidumbres y los incidentes digitales en diferentes países, la OCDE emitió, el 17 de septiembre de 2015, las *Recomendaciones sobre gestión de riesgos de seguridad digital para la prosperidad económica y social*. Este documento guía la formulación de la nueva generación de estrategias respecto a la gestión de la seguridad digital, con el objetivo de optimizar los beneficios económicos y sociales que se esperan por el desarrollo de actividades en un entorno digital abierto.

El documento en mención aconseja que las estrategias o políticas de seguridad digital de los países deben tener una visión estratégica general, bajo un modelo institucional eficiente y de vinculación integral de las múltiples partes interesadas. Lo anterior implica la definición de una o varias instancias de alto nivel en el gobierno, que sean responsables de la coordinación o emisión de lineamientos generales a nivel nacional para lograr que la estrategia o política de seguridad digital cumpla con los objetivos establecidos y asigne de manera eficiente los recursos disponibles. Para esto, se requiere de una institucionalidad clara, con roles y funciones bien definidas, para evitar duplicación de esfuerzos al desarrollar acciones bajo las estrategias planteadas.

La OCDE también recomienda distinguir claramente el objetivo de prosperidad económica y social de los objetivos de defensa y seguridad nacional en el entorno digital. Esto significa que una estrategia o política de seguridad digital no debe diseñarse solo para contrarrestar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (problema técnico). La política además debe incorporar de manera diferenciada el objetivo de prosperidad económica y social. En lugar de continuar tratando el riesgo de seguridad digital como un problema técnico que necesita soluciones técnicas, este también

debería abordarse como un riesgo económico que debe gestionarse en cualquier proceso de toma de decisiones.

A continuación se presentan algunas de las definiciones establecidas por la OCDE, en el documento en discusión, que serán tomadas como referencia para el desarrollo de la política objeto de este documento.

> *Riesgo:* es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.
>
> *Riesgo de seguridad digital:* es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.
>
> *Gestión de riesgos de seguridad digital*: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

Adicionalmente, las recomendaciones de la OCDE sobre seguridad digital propone: (i) implementar un conjunto de principios en todos los niveles del Gobierno y de las organizaciones públicas; y (ii) adoptar una estrategia nacional para la gestión de riesgos de seguridad digital (OCDE, 2015a).

Respecto al conjunto de principios, la OCDE recomienda que sean de dos tipos: generales y operativos. Los principios generales están dirigidos a las múltiples partes interesadas quienes, directa o indirectamente, desarrollan algunas o todas sus actividades socioeconómicas en el entorno digital. Los principios operativos están dirigidos a los líderes o tomadores de decisiones, quienes por su alto nivel en las organizaciones deben enfocar sus acciones hacia la adopción del marco general de gestión del riesgo de seguridad digital.

La OCDE propone los siguientes principios generales:

Conocimiento, capacidades y empoderamiento: las múltiples partes interesadas deben entender los riesgos de seguridad digital. Deben ser conscientes de que el riesgo de seguridad digital puede afectar el logro de sus objetivos económicos y sociales, y el de otros. Deben estar educados al respecto, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto.

Responsabilidad: las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales.

Derechos humanos y valores fundamentales: las múltiples partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales. La implementación de la gestión de riesgos de seguridad digital debe ser compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales. Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

Cooperación: las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

A continuación, los principios operativos recomendados por la OCDE:

Evaluación de riesgos y ciclo de tratamiento: la evaluación de riesgos debe llevarse a cabo de manera sistemática y continua, evaluando las posibles consecuencias de las amenazas y las vulnerabilidades digitales en las actividades económicas y sociales en juego. El tratamiento del riesgo debería tener como objetivo reducir el riesgo a un nivel aceptable en relación con los beneficios económicos y sociales.

Medidas de seguridad: los líderes y tomadores de decisiones deben asegurarse de que las medidas de seguridad sean apropiadas y proporcionales al riesgo, y deben tener en cuenta su potencial impacto, negativo o positivo, sobre las actividades económicas y sociales que tienen por objeto proteger. La evaluación de riesgos de seguridad digital debe guiar la selección, operación y mejora de las medidas de seguridad para reducir el riesgo a niveles aceptables.

Innovación: los líderes y tomadores de decisiones deben asegurarse de que la innovación sea considerada como parte integral de la reducción del riesgo de seguridad digital. Esta debe fomentarse tanto en el diseño y funcionamiento de la economía, y de las actividades sociales basadas en el entorno digital, como en el diseño y el desarrollo de las medidas de seguridad.

Preparación y continuidad: con el fin de reducir los efectos adversos de los incidentes de seguridad, y apoyar la continuidad y la capacidad de recuperación de las actividades económicas y sociales, deben adoptarse preparaciones y planes de continuidad. El plan debe identificar las medidas para prevenir, detectar, responder y recuperarse de los incidentes y proporcionar mecanismos claros de escalamiento.

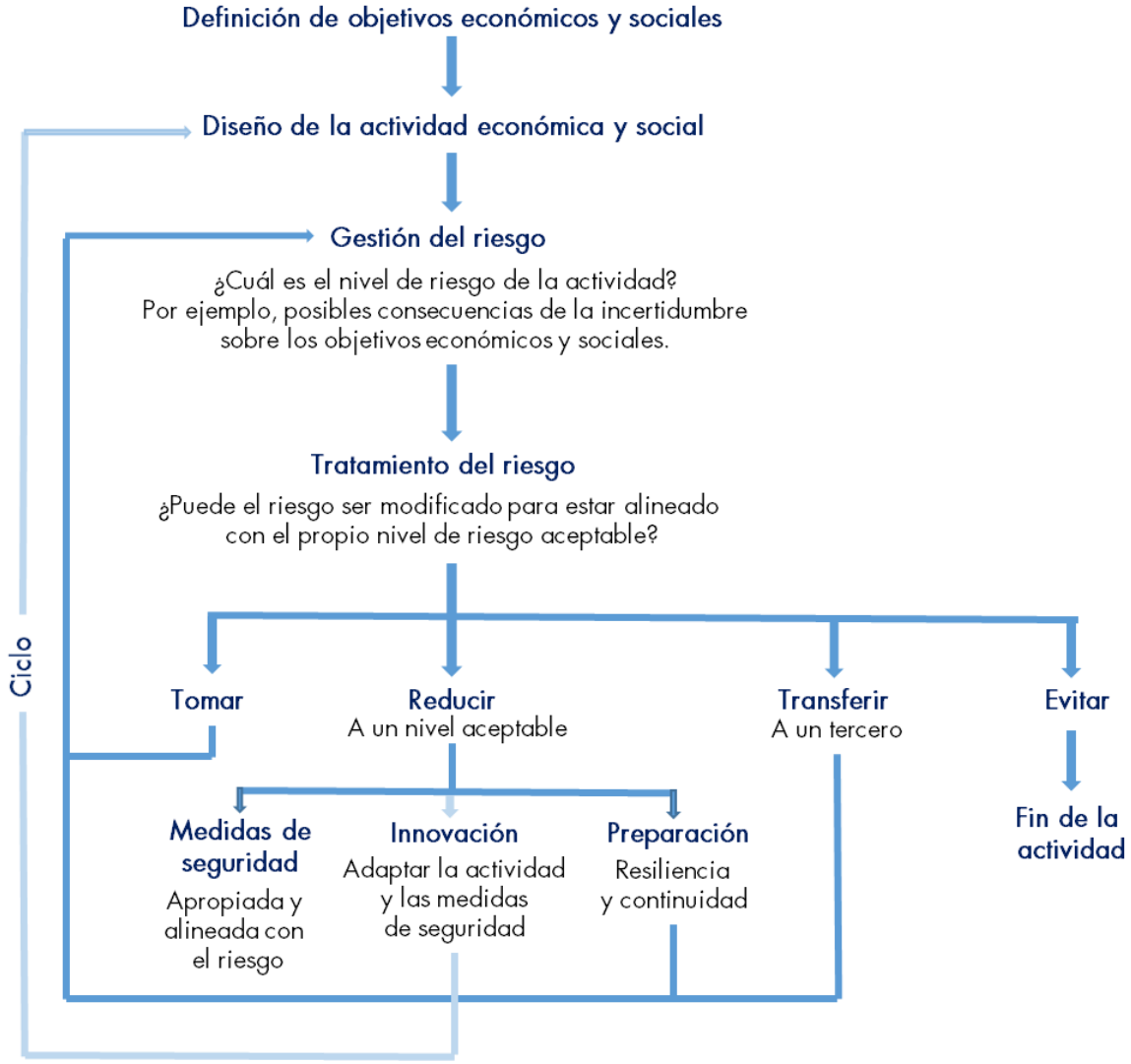
3.2. Estrategia de gestión de riesgos de seguridad digital

La estrategia de gestión de riesgos para abordar la seguridad digital debe tener un enfoque flexible y ágil para abordar las incertidumbres digitales. Lo anterior, con el fin de alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y los valores fundamentales, y proteger a las personas frente a las amenazas de seguridad digital (OCDE, 2015a).

De acuerdo con las recomendaciones de la OCDE, la estrategia nacional debe ser consistente con el conjunto de principios formulados, debe crear las condiciones para que las múltiples partes interesadas puedan gestionar la seguridad digital de sus actividades económicas y sociales, debe fomentar la confianza en el entorno digital y, además, debe: (i) estar apoyada desde el más alto nivel de gobierno; (ii) afirmar claramente que su objetivo es aprovechar el entorno digital abierto para la prosperidad económica y social; (iii) estar dirigida a todas las partes interesadas; y (iv) ser el resultado de un enfoque intra-gubernamental, coordinado, abierto y transparente, donde participen las múltiples partes interesadas.

La Figura 1 muestra una representación genérica de la gestión sistemática y cíclica de riesgos de seguridad digital, reflejando los principios operativos de la recomendación de la OCDE. Esta inicia con la definición de un objetivo o el diseño de una actividad, luego, en la etapa conocida como gestión del riesgo, se evalúa cuál es el nivel de riesgo de dicha actividad determinando todos los resultados posibles de asumirlo sobre los objetivos sociales y económicos. Posteriormente, en la etapa de tratamiento del riesgo, se determina cómo debería ser modificado el mismo, con el fin de aumentar la probabilidad de éxito de la actividad y preservar los objetivos definidos, decidiendo si el riesgo debe ser tomado, reducido, transferido o evitado. Si se decide reducirlo, se pueden seleccionar y aplicar medidas de seguridad, se puede considerar la innovación, o las medidas de preparación para su tratamiento.

Figura 1. Modelo de gestión sistemática y cíclica de riesgo de seguridad digital



Fuente: OCDE (2015a).

Así las cosas, la política nacional de seguridad digital: (i) adoptará la gestión sistemática y cíclica del riesgo; (ii) será liderada desde el alto nivel del gobierno; (iii) asegurará la defensa y seguridad nacional; (iv) estimulará la prosperidad económica y social; (v) adoptará un enfoque multidimensional, es decir, la seguridad digital será abordada tanto desde la dimensión técnica o jurídica, como desde la dimensión económica y social; (vi) tendrá en cuenta a las múltiples partes interesadas; (vii) promoverá la responsabilidad compartida; (viii) salvaguardará los derechos humanos; (ix) protegerá los valores nacionales; y (x) concientizará y educará.

Para garantizar lo anterior, y en línea con los principios recomendados por la OCDE, la política nacional de seguridad digital, objeto de este documento, se regirá por cuatro principios fundamentes (PF) definidos de acuerdo al contexto nacional.

PF1. *Salvaguardar los derechos humanos y los valores fundamentales* de los ciudadanos en Colombia, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de la intimidad y los datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia. En caso de limitación a estos derechos, debe ser bajo medidas excepcionales y estar conforme con la Constitución Política y los estándares internacionales aplicables. Estas medidas, deben ser proporcionales, necesarias y estar enmarcadas en la legalidad.

PF2. *Adoptar un enfoque incluyente y colaborativo* que involucre activamente a las múltiples partes interesadas, y que permita establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital del país y sus habitantes, y aumentar la capacidad de resiliencia nacional frente a eventos no deseados en el entorno digital.

PF3. *Asegurar una responsabilidad compartida* entre las múltiples partes interesadas, promoviendo la máxima colaboración y cooperación. Lo anterior, teniendo en cuenta el rol y el grado de responsabilidad de cada parte para gestionar los riesgos de seguridad digital y para proteger el entorno digital.

PF4. *Adoptar un enfoque basado en la gestión de riesgos*, que permita a los individuos el libre, seguro y confiable desarrollo de sus actividades en el entorno digital. Lo anterior, fomentará la prosperidad económica y social, buscando la generación de riqueza, innovación, productividad, competitividad, y empleo en todos los sectores de la economía.

Con el fin de adoptar un enfoque multidimensional, que garantice la seguridad digital y atienda las necesidades y expectativas de todas las partes interesadas, se definen cinco dimensiones estratégicas (DE). Estas dimensiones determinan los campos de acción de la política nacional de seguridad digital.

DE1. *Gobernanza de la seguridad digital*: articulación y armonización de las múltiples partes interesadas, bajo un marco institucional adecuado, con el fin de gestionar la seguridad digital, bajo el liderazgo del Gobierno nacional.

DE2. *Marco legal y regulatorio de la seguridad digital*: marco legal y regulatorio que soporta todos los aspectos necesarios para adelantar la política.

DE3. *Gestión sistemática y cíclica del riesgo de seguridad digital*: conjunto de iniciativas, procedimientos o metodologías coordinadas con el fin de abordar, de manera cíclica y holística, los riesgos de seguridad digital en el país.

DE4. *Cultura ciudadana para la seguridad digital*: sensibilización de las múltiples partes interesadas, para crear y fomentar una cultura ciudadana responsable en la seguridad digital.

DE5. *Capacidades para la gestión del riesgo de seguridad digital*: fortalecimiento y construcción de capacidades humanas, técnicas, tecnológicas, operacionales y administrativas en las múltiples partes interesadas, para adelantar la gestión de riesgos de la seguridad digital.

La política nacional de seguridad digital entenderá los conceptos de seguridad digital, múltiples partes interesadas, infraestructura crítica cibernética nacional y economía digital, como se definen a continuación.

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

Múltiples partes interesadas: 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.

Infraestructura crítica cibernética nacional: aquella 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.

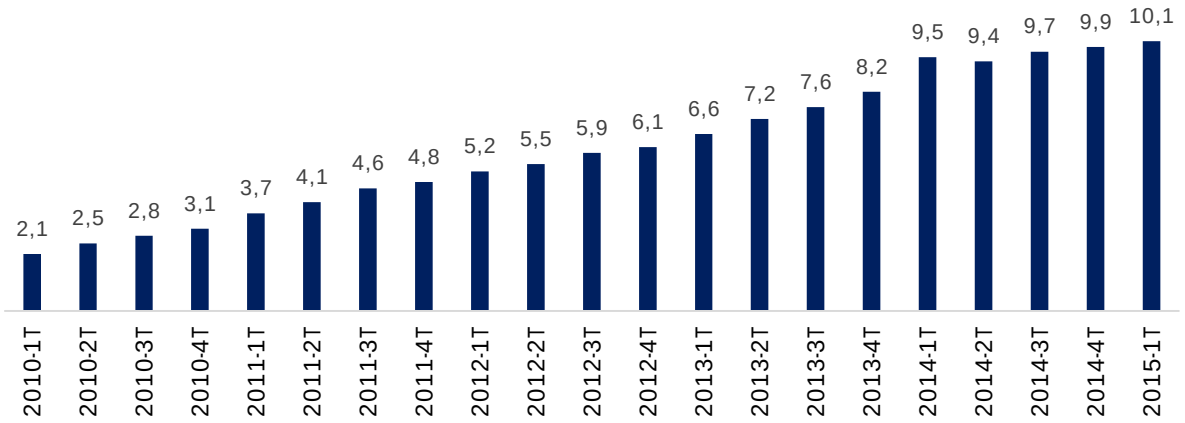
Economía digital: economía basada en el uso de tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

4. DIAGNÓSTICO

Colombia ha vivido una transformación digital durante la última década, en especial desde el año 2010. Según el Ministerio de Tecnologías de la Información y las Comunicaciones, en el país se multiplicó por cinco el número de conexiones a Internet, pasando de 213 millones en 2010, a 10,11 millones en 2015[18], tal y como se muestra en el Gráfico 1.

Gráfico 1. Evolución de conexiones de banda ancha en Colombia

Millones de conexiones de banda ancha



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2015.

El mayor número de conexiones a Internet se explica, en parte, (i) por el hecho de que actualmente están conectados a la red troncal de fibra óptica[19] 1.078 de los 1.123 municipios del país; (ii) por la instalación de 899 centros de acceso comunitario urbanos (Puntos Vive Digital) para dar formación en el uso de Internet a personas de estratos 1 y 2 en todo el país; y (iii) por la disposición de 7.621 centros de acceso comunitario en zonas apartadas y centros poblados de más de 100 habitantes (Kioscos Vive Digital). Lo anterior, evidencia que los colombianos actualmente cuentan con una base de conectividad significativa para hacer parte activa del entorno digital (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015a).

Adicionalmente, a través de la iniciativa Apps.co se construyó en Colombia una amplia red de emprendedores de Latinoamérica (80.000 emprendedores), los cuales están haciendo

[18] Según COLOMBIATIC (2015), se refiere a conexiones de banda ancha (Vive Digital) con corte a 31 de marzo de 2015. La meta establecida en el PND 2014-2018 para el año 2018 es de 27 millones de conexiones a Internet.

[19] Se trata de una red nacional de telecomunicaciones que despliega redes de transporte de fibra óptica en los municipios del país, para facilitar el acceso a la información en el entorno digital, y por consiguiente, multiplicar el número de conexiones a Internet.

realidad sus ideas de negocios basados en las TIC. Esto, aunado al hecho de que el 65% de los ciudadanos colombianos interactúan por medios electrónicos con agencias gubernamentales que disponen de más de 400 procedimientos totalmente en línea, muestra que los ciudadanos y empresas se encuentran cada día más inmersos en el entorno digital, estando dispuestos a interactuar con el Estado mediante el uso de las TIC.

El aumento en la conectividad en el país, ha hecho que las TIC se conviertan en una herramienta importante para el crecimiento de la economía. Esto, porque el incremento en la conectividad en Colombia ha aumentado la participación de la sociedad en actividades económicas y sociales soportadas en las TIC, generando mayor inclusión de la población y aumentos en productividad y competitividad, que se traducen en crecimiento económico. Así lo reconoce el Plan Nacional de Desarrollo 2014-2018 *Todos por un nuevo país,* al apoyar su ejecución en estrategias en las que las TIC juegan un papel relevante para su consecución (Departamento Nacional de Planeación, 2014).

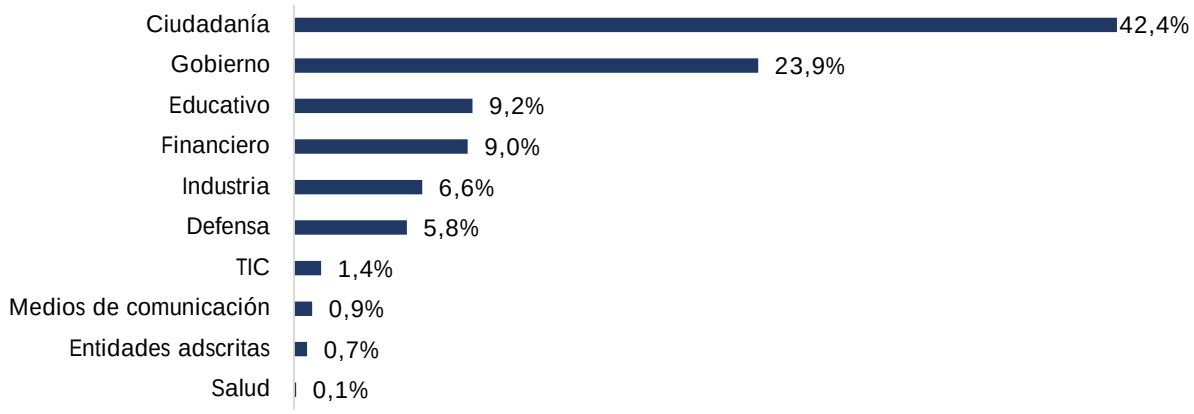
La relación entre digitalización y crecimiento económico ha sido estudiada internacionalmente. Katz (2015), encuentra que tanto la digitalización de un país como el aumento en la penetración de las TIC contribuyen positivamente al crecimiento del Producto Interno Bruto (PIB) de los países. Por ejemplo, un incremento anual en 10% en la penetración de banda ancha en un país medio de la OCDE puede contribuir al crecimiento anual de su PIB en un 0,29%; o un incremento del 10% del índice de digitalización[20] de un país generaría un aumento de 0,75% en su PIB per cápita.

No obstante, con el incremento en el uso del entorno digital también se incrementan las amenazas cibernéticas, las vulnerabilidades y los incidentes digitales[21]. Situación que afecta la seguridad de los ciudadanos, de las organizaciones públicas y privadas, e incluso de infraestructuras que hacen parte de los intereses de la nación. Durante los últimos años, Colombia ha sido foco de interés para distintos ataques cibernéticos, los cuales se han sofisticado trayendo consigo el incremento de la efectividad de los mismos y una mayor dificultad para su oportuna detección. Escenario que preocupa al Gobierno nacional toda vez que las condiciones para desarrollar actividades socioeconómicas en el país cada día se soportan más en el uso de las TIC, y los incidentes digitales en Colombia afectan a varios agentes y sectores, siendo la ciudadanía la mayor afectada (Gráfico 2).

[20] Indicador propuesto por Katz (2015) que mide las condiciones de un país o región en cuanto a la asequibilidad, confiabilidad, accesibilidad, capacidad, utilización y capital humano de las TIC.

[21] En el país se pasó de gestionar un total de 4.640 incidentes digitales en 2014 a un total de 7.323 en 2015.

Gráfico 2. Sectores afectados en Colombia por incidentes digitales, 2015



Fuente: colCERT, 2015.

La importancia del entorno digital como herramienta para el crecimiento económico, las nuevas y más sofisticadas formas para atentar contra la defensa y seguridad de los ciudadanos y la del Estado, la diversidad de afectados por incidentes digitales en el país, y la concentración de los mismos en la ciudadanía, resaltan la importancia de que el país tenga un enfoque de gestión de riesgos en seguridad digital que involucre efectivamente a todas las partes interesadas (Mejores prácticas internacionales). Su implementación atenderá cinco problemas principales: (i) no se cuenta con una visión estratégica en seguridad digital basada en la gestión de riesgos; (ii) las múltiples partes interesadas no maximizan sus oportunidades al desarrollar actividades socioeconómicas en el entorno digital; (iii) se necesita reforzar las capacidades de ciberseguridad con un enfoque de gestión de riesgos de seguridad digital; (iv) se necesita reforzar las capacidades de ciberdefensa con un enfoque de gestión de riesgos de seguridad digital; y (v) los esfuerzos de cooperación, colaboración y asistencia, nacional e internacional, relacionados con la seguridad digital no son suficientes y requieren ser articulados.

4.1. Ausencia de una visión estratégica basada en la gestión de riesgos

Actualmente Colombia no cuenta con una instancia de coordinación nacional en seguridad digital que optimice la gestión de los recursos destinados a esta materia. Dicha ausencia no permite que el país tenga una visión estratégica, que articule las funciones y actividades de la institucionalidad existente en torno a los objetivos nacionales en seguridad digital. Situación que conduce a la duplicación de esfuerzos y a una menor eficiencia.

La duplicación de esfuerzos se evidencia, por ejemplo, en las diferentes campañas de sensibilización en torno a la seguridad en el entorno digital que han adelantado distintas instituciones. Campañas que podrían generar un mayor impacto si se unifican o se realizan

de forma coordinada, definiendo claramente la población objetivo de cada una. Esta situación de esfuerzos aislados, en algunos casos dispersos, sin foco e impacto, también se presenta en actividades tales como eventos o convocatorias de capacitación, en las cuales múltiples entidades destinan recursos para el mismo fin y no coordinan los contenidos de las capacitaciones, lo que no permite maximizar la efectividad de tales actividades.

Actualmente, el colCERT es el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa, el cual presta su apoyo y colaboración a las instancias nacionales tales como el CCP y el CCOC. Este grupo tiene la función de coordinar las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. Sin embargo, aún se requiere establecer una visión global y estratégica en torno a la seguridad digital, cuya ausencia se evidencia en la forma en que se interpretan los conceptos y en el alcance de las acciones que cada entidad debe ejecutar sobre la materia. Esto genera una dispersión de los esfuerzos realizados por cada entidad en el cumplimiento de sus funciones y competencias.

A la falta de una instancia de coordinación nacional en seguridad digital, se le suma la ausencia de una instancia de orientación superior que emita lineamientos generales a nivel nacional y defina los objetivos nacionales en términos de seguridad digital. La dinámica institucional existente, bajo la coordinación de la Comisión Nacional Digital y de Información Estatal, al estar enmarcada en una política sin una visión global que no adopta el enfoque de múltiples partes interesadas (sección *2.2 Mejores prácticas internacionales*), está motivada únicamente en lograr el cumplimiento de los objetivos de (i) defensa del país; y (ii) lucha contra el cibercrímen. Es decir, de enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa), pero no en el objetivo de gestionar los riesgos de seguridad digital que maximice los beneficios de un entorno digital abierto para impulsar la prosperidad económica y social.

Al ser Colombia un país con un entorno digital creciente, un enfoque de seguridad digital no basado en la gestión de riesgos y que no involucre a todas las partes interesadas, será cada vez más insostenible y costoso, sin que efectivamente se proteja la economía y la sociedad (OEA, 2014). Los incidentes e incertidumbres digitales afectan a diferentes agentes y sectores, por lo que sus consecuencias pueden ser nacionales – sin necesidad de que sean dirigidas directamente al Estado – y de tipo económico o social. El riesgo de seguridad digital, por consiguiente, debe ser formulado en términos económicos y sociales: pérdidas financieras, pérdidas en competitividad, pérdidas de oportunidad, daños a la reputación, a la imagen o a la confianza; y debe ser gestionado debidamente por todos los interesados o posibles afectados (OCDE, 2015a).

Desde una perspectiva organizacional, lo expuesto anteriormente se traduce en tres cuestiones principales: (i) los problemas no se abordan al más alto nivel de gobierno; (ii) este último no cuenta con una evaluación exhaustiva de la situación de riesgo a nivel nacional, y por tanto, no puede tomar decisiones basadas en el riesgo; y (iii) las actividades en los niveles inferiores no se basan en la gestión del riesgo.

Adicional a las falencias organizacionales, tener una política de seguridad digital centrada en el sector defensa sin coordinación con las demás sectores interesados en el tema, limita la detección y respuesta a incidentes digitales. Así lo plantean el BID y la OEA (2016), a través de su modelo de madurez de capacidad de seguridad cibernética[22], al darle a Colombia una clasificación de "formativo"[23] en el aspecto "capacidad de respuesta a incidentes", que reconoce que el país ha trabajado en el establecimiento de un grupo de respuesta a incidentes nacional (colCERT), pero que tiene un alcance limitado en cuanto a la detección y respuesta. Esto, fruto de que las capacidades actuales no son las ideales para contar con un organismo auto-sostenible (actualmente se depende en gran medida de fuentes de información externa) apoyado desde los diferentes sectores de la sociedad, el cual trabaje de manera coordinada con ellos y sea capaz de responder adaptativamente a los cambios del entorno cibernético.

4.2. Las múltiples partes interesadas no maximizan sus oportunidades al desarrollar actividades socioeconómicas en el entorno digital

En materia de seguridad digital, en el país no se distingue actualmente el objetivo de prosperidad económica y social de los objetivos de defensa y seguridad nacional en el entorno digital. Esto significa que Colombia actualmente enfoca sus esfuerzos en contrarrestar

[22] Modelo que toma en cuenta las consideraciones de seguridad cibernética a través de cinco áreas o dimensiones de la capacidad diferentes: (i) políticas y estrategia nacional de seguridad cibernética; (ii) cultura cibernética y sociedad; (iii) educación, formación y competencias en seguridad cibernética; (iv) marco jurídico y reglamentario; y (v) normas, organización y tecnologías.

[23] Para cada capacidad se han identificado cinco niveles de madurez. Los niveles de madurez son los siguientes: (i) *inicial*: en este nivel, o nada existe, o es de naturaleza embrionaria. Incluye situaciones en las que existe un pensamiento o una observación acerca de un problema, pero no una acción; (ii) *formativo*: algunas características han comenzado a crecer y ser formuladas, pero pueden ser casuales, desorganizadas, mal definidas o simplemente nuevas; (iii) *establecido*: los elementos están establecidos y funcionando, sin embargo, no se ha considerado bien la asignación relativa de recursos, y ha habido poca toma de decisiones de compensación en relación con la inversión relativa en los distintos elementos del subfactor; (iv) *estratégico*: al nivel nacional se han elegido las partes del subfactor que son clave, así como aquellas que son menos importantes para la organización o país en particular. Estas elecciones toman en consideración un resultado esperado, una vez implementado, que contiene circunstancias particulares y otros objetivos nacionales existentes; y (v) *dinámico*: existen mecanismos claros para alterar la estrategia en función de las circunstancias imperantes, las organizaciones dinámicas han desarrollado métodos para cambiar las estrategias, de acuerdo con una manera de sentir y responder, y la toma de decisiones es rápida. La reasignación de los recursos y la atención constante a los cambios del entorno son las características de este nivel.

las amenazas cibernéticas que atenten la defensa y seguridad nacional, y no adopta una estrategia de gestión de riesgos de seguridad digital que involucre a todas las partes interesadas, mediante la cual se maximicen las oportunidades y beneficios económicos que otorga el entorno digital a la sociedad en general.

Aunque en el país existe coordinación y apoyo entre el sector público y el privado en torno a temas de ciberseguridad y ciberdefensa, es necesario llegar al siguiente nivel de madurez. Nivel en el que todos los actores de la economía y la sociedad asumen la responsabilidad de gestionar el riesgo de seguridad digital de acuerdo con su función. Dado que las múltiples partes interesadas no están lo suficientemente vinculadas en torno a la gestión de riesgos de seguridad digital, el país en conjunto no está maximizando las oportunidades que conlleva dicha gestión, ya que aún la proporción de usuarios del entorno digital es baja si la comparamos con otros países.

Aunque hoy los ciudadanos colombianos tienen una mayor interacción con el entorno digital, actualmente no están maximizando los beneficios socioeconómicos y las oportunidades potenciales que brinda la economía digital. Por ejemplo, en la Tabla 3 se aprecia que el 79,6% de los jóvenes entre 12 y 24 años usaron Internet en 2014 en Colombia, mientras esta cifra para los jóvenes entre 16 y 24 años de edad en los países OCDE, asciende a 95% (OCDE, 2015b).

Tabla 3. Uso de Internet en Colombia por rangos de edad, 2010-2014

Porcentaje

	2010	2011	2012	2013	2014
Población total	**36,5**	**40,4**	**49,0**	**51,7**	**52,6**
De 5 a 11 años	28,1	50,1	52,1	55,2	58,4
De 12 a 24 años	64,4	83,0	77,9	80,6	79,6
De 25 a 54 años	32,4	49,5	44,2	47,7	49,5
De 55 a más años	7,8	14,2	11,9	13,8	14,6

Fuente: DANE - ECV para los años 2010 a 2014.

Otro aspecto relevante para destacar, es que en Colombia tan solo el 51,1% de los individuos usó Internet todos los días de la semana (Tabla 4), frente al 75% en países de la OCDE (OCDE, 2015b), y frente al 65% en los países europeos (EURACTIV, 2015).

Tabla 4. Frecuencia de uso del Internet en Colombia, 2010-2014

	2010	2011	2012	2013	2014
Todos los días de la semana	47,0	47,1	46,0	48,3	51,1

Al menos una vez a la semana pero no cada día	40,8	41,9	42,6	41,6	41,8
Al menos una vez al mes pero no cada semana	9,8	9,2	11,3	8,8	6,2
Al menos una vez al año pero no cada mes	2,5	1,8	-	1,3	0,9

Fuente: DANE - ECV para los años 2010 a 2014.

En la Tabla 5 se aprecia que, según datos de la Encuesta de Calidad de Vida (ECV) del Departamento Administrativo Nacional de Estadística (DANE), tan sólo el 38% de los hogares tenía conexión a Internet en Colombia a 2014. Mientras que en Europa, el 81% de los hogares tiene acceso a Internet (EURACTIV, 2015).

Tabla 5. Hogares con conexión a Internet, por tipo de conexión, 2010-2014

Porcentaje

	2010	2011	2012	2013	2014
Hogares con conexión a Internet	19,2	23,4	32,1	35,7	38,0
Hogares con conexión a Internet fijo	-	-	25,1	29,1	31,7
Hogares con conexión a Internet móvil	-	-	9,9	10,9	16,0
Hogares con conexión a Internet fijo y móvil	-	-	2,8	4,3	9,8

Fuente: DANE - ECV para los años 2010 a 2014.

Mientras que el 82% de los usuarios de Internet en los países miembros de la OCDE utilizó el Internet para obtener información sobre bienes y productos, y el 72% consultó noticias en línea durante el 2014, en Colombia solo el 62% de los individuos utilizó el Internet para obtener información. Por otro lado, en los países OCDE más del 60% de los individuos usaron la banca electrónica[24] (OCDE, 2015b); mientras que en Colombia, tan sólo el 6,4% de los individuos lo hicieron (Tabla 6).

Tabla 6. Uso de Internet en Colombia según actividad, 2010-2014

Porcentaje

Actividad en línea	2010	2011	2012	2013	2014
Redes sociales			55,6	62,4	63,2
Obtener información	74,3	74,3	56,5	52,9	61,7
Correo y mensajería	76,2	78,7	62,4	58,5	57,6
Educación y aprendizaje	64,1	62,1	42,0	44,1	36,7
Actividades de entretenimiento	62,6	65,7	39,5	40,6	28,7
Consulta de medios de comunicación				17,2	9,9

[24] La banca electrónica hace referencia al tipo de banca que se realiza por medios electrónicos como puede ser cajeros electrónicos, teléfono, Internet y otras redes de comunicación.

Actividad en línea	2010	2011	2012	2013	2014
Banca electrónica	10,1	9,4	5,8	6,5	6,4
Comprar u ordenar productos o servicios	5,3	5,7	4,9	5,1	5,6
Trámites con organismos gubernamentales	3,3	4,4	5,5	5,0	4,1
Otro servicio			3,0	1,1	1,3

Fuente: DANE - ECV para los años 2010 a 2014.

El bajo, pero creciente, uso del entorno digital por parte de los colombianos, se debe a la existencia de barreras al uso de medios electrónicos. INFOMETRIKA (2014) adelantó una encuesta para el Ministerio de Tecnologías de la Información y las Comunicaciones con el fin de medir, entre otros, la percepción de uso de medios electrónicos por parte de los ciudadanos para realizar trámites y servicios en línea durante 2014. Se encontró que la principal barrera de los ciudadanos para realizar trámites mediante Internet es la desconfianza en el medio.

La desconfianza en el uso del entorno digital puede estar relacionada con el uso no responsable del mismo, actitud que genera riesgos de seguridad digital que deben ser abordados eficientemente. Estos riesgos se reflejan en el incremento de las denuncias por delitos cibernéticos. Según las estadísticas de la iniciativa *Te Protejo,* la cual se considera como un canal para la denuncia de contenidos ilegales como son el abuso sexual[25], la explotación sexual comercial y la pornografía infantil y adolescente en Colombia, este tipo de denuncias ha tenido un crecimiento anual promedio del 59% (Tabla 7). Gracias a esta iniciativa, del 1 al 29 de enero de 2016 la Dirección de Investigación Criminal de Colombia (DIJIN) ha dado orden de bloqueo a 270 sitios web con pornografía infantil, para un total de 3.643 localizadores de recursos uniformes (URL) desde su puesta en marcha.

Por otra parte, aunque hoy las empresas colombianas están más digitalizadas, actualmente todos los sectores no están maximizando los beneficios económicos y las oportunidades potenciales que brinda la economía digital. Según datos de la ECV del DANE, mientras que el 87% de las empresas del sector servicios en Colombia tenía un sitio web o página de inicio en el 2014, tan sólo el 67% de las empresas del sector industria y el 60% de las empresas del sector comercio lo tenían. En cuanto a la compra de insumos por internet, solo el 52%, el 38% y el 29% del total de empresas de los sectores de servicios, comercio e industria, respectivamente usaron Internet con este fin en el 2014. Porcentaje que descienden aún más si analizamos la venta de productos por Internet, 41%, 20% y 27%, respectivamente.

[25] Te Protejo es la primera línea virtual de denuncias en Colombia y Latinoamérica en convertirse miembro de la Fundación INHOPE, con apoyo de la Policía Nacional de Colombia. Tiene como socios al Ministerio de Tecnologías de la Información y las Comunicaciones, el Instituto de Bienestar Familiar, la Fundación Telefónica, el Foro de Generaciones Interactivas (España) y la Red PaPaz.

Tabla 7. Denuncias procesadas por la iniciativa Te Protejo en Colombia, 2012-2015

Tipo de denuncia	2012	2013	2014	2015	Total
Pornografía Infantil	462	1.493	3.724	5.827	**11.506**
Maltrato, trabajo y abuso infantil	101	1.041	988	1.311	**3.441**
Otros	918	405	606	435	**2.364**
Ciberacoso	0	0	491	539	**1.030**
Contenidos inapropiados	145	263	245	175	**828**
Venta de alcohol	143	212	143	150	**648**
Intimidación escolar	129	126	187	143	**585**
ESCNNA	0	0	36	127	**163**
No aplica	294	381	32	0	**707**
Total	**2.192**	**3.921**	**6.452**	**8.707**	**21.272**

Fuente: www.teprotejo.org, 2015.

La digitalización de la economía en forma desigual es un fenómeno que han identificado diferentes estudios, y que no afecta únicamente a Colombia. La firma PricewaterhouseCoopers (2011 y 2012) identificó que en los países de la Unión Europea, las siguientes industrias fueros las líderes en el proceso de digitalización durante los años 2011 y 2012: servicios financieros y de seguros, computadores y electrónica, medios de comunicación y automotriz. Por su parte, McKinsey Global Institute (2015) demuestra que la economía estadounidense está digitalizándose de forma desigual, con grandes disparidades entre sectores. Más allá del sector TIC, que a menudo establece el estándar más alto de digitalización, los sectores de la economía altamente digitalizados en 2015 son los medios de comunicación, los servicios profesionales, y los servicios financieros.

Con respecto a las micro, pequeñas y medianas empresas (MIPYMES), según datos de la Encuesta de Microestablecimientos (EM) del DANE, tan sólo el 25% de estas firmas de los sectores industrial, comercial y de servicios en Colombia, tuvieron acceso o usaron Internet en 2014 y tan sólo el 6% tienen presencia en la web. Mientras que la presencia en la web de las MIPYME oscila alrededor del 90% en Dinamarca, Finlandia y Suiza, y del 50% en Letonia, Portugal y México (OCDE, 2015b).

En la encuesta adelantada por INFOMETRIKA (2014) también se midió la percepción de uso de medios electrónicos por parte de las empresas para realizar trámites y servicios en línea en Colombia durante 2014. Al igual que en los ciudadanos, se encontró que una de las principales barreras de las empresas para realizar trámites mediante Internet es la

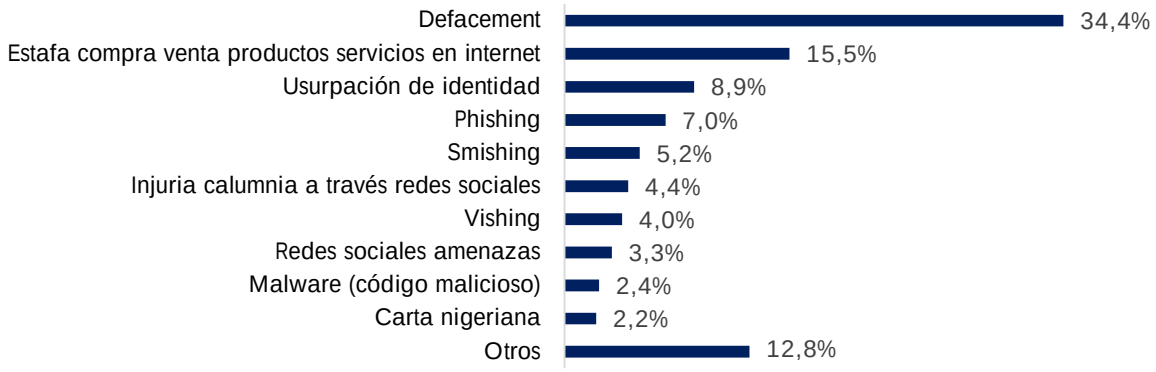
desconfianza en el medio, lo que evidencia la falta de mecanismos para ofrecer un entorno digital seguro y confiable para todos, y comunicarlo.

Aunado a lo anterior, Colombia dispone de un marco normativo, y otros actos, expedido bajo lineamientos exclusivos a la ciberseguridad y ciberdefensa. Por tanto, no incorporaba aspectos como la gestión de riesgos de seguridad digital, el establecimiento de principios generales mencionados en el Marco conceptual, y la diferenciación entre los objetivos de prosperidad económica y social, y los relacionados con la lucha contra el cibercrímen y la ciberdelincuencia.

4.3. Es necesario reforzar las capacidades de ciberseguridad con un enfoque de gestión de riesgos

En Colombia se han incrementado el tipo y número de amenazas cibernéticas. Se pasó de gestionar un total de 3.871 incidentes digitales por el CCP y el CSIRT PONAL en 2014, a gestionar 6.366 incidentes en 2015. En el Gráfico 3 se aprecia que, en el 2015, el 34,4% del total de incidentes corresponden a incidentes de *defacement*[26], el 15,5% a estafa en compra o venta de servicios en Internet, el 8,9% a usurpación de identidad, el 7% a *phishing*[27] y el 5,2% a *smishing*[28].

Gráfico 3. Incidentes digitales gestionados por CCP y CSIRT PONAL en el entorno digital en Colombia, 2015



Fuente: CCP y CSIRT PONAL, 2015.

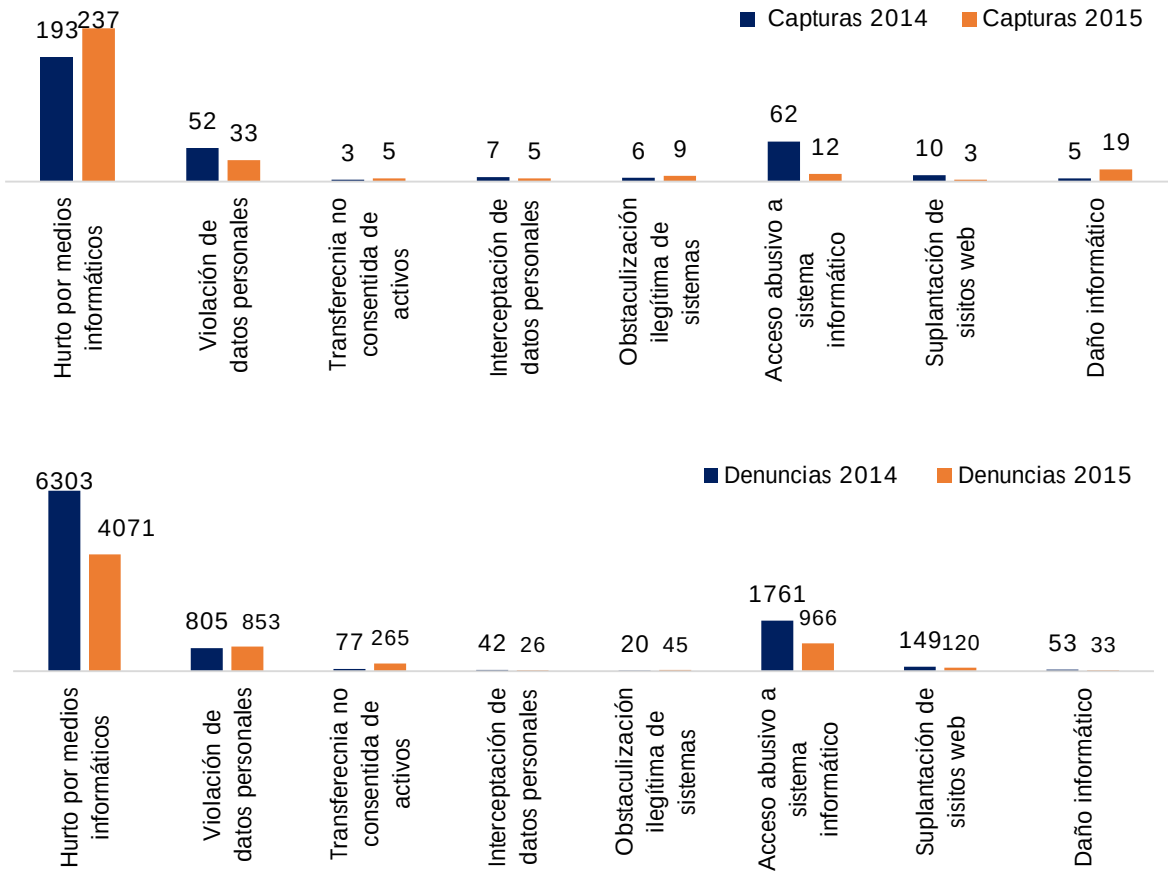
[26] Consiste en la modificación de la página de bienvenida de un sitio web por otra cuyo contenido (pornografía, política, etc.) depende de la motivación de los atacantes.

[27] Técnica utilizada para obtener información confidencial (nombres de usuario, contraseñas, etc.) mediante el envío de comunicaciones electrónicas aparentemente confiables.

[28] Variante del phishing enfocada en usuarios de telefonía móvil, mediante el empleo de mensajes de texto (SMS).

El CCP del país realizó en promedio 330 capturas al año durante 2014 y 2015. El Gráfico 4 muestra que la problemática es creciente en el país, al observar la evolución de capturas debido a incidentes digitales; y sin embargo, las cifras oficiales de denuncias disponibles no evidencian la magnitud, y complejidad de la problemática actual. Esto, dado que muchos de los incidentes digitales presentados no son reportados a las autoridades competentes, debido al desconocimiento de los procedimientos de reporte, a la débil cultura de denuncia u otros aspectos vinculados a los temas de reputación del negocio.

Gráfico 4. Capturas y denuncias de incidentes digitales en Colombia, 2015



Fuente: CCP, 2015.

Frente al incremento considerable en el número de incidentes digitales, las entidades del Estado en temas de ciberseguridad evidencian una brecha con respecto a los avances tecnológicos, debido a la baja prioridad en la asignación y ejecución de recursos humanos, físicos, lógicos y económicos en las áreas encargadas de dicho tema.

Por ejemplo, a 31 de diciembre de 2015, se encontró lo siguiente: (i) seis de cada diez entidades públicas en el país no tiene un área de seguridad informática, ni un área de

seguridad de la información; (ii) tan solo en el 21% de las entidades públicas existe un funcionario dedicado al rol de oficial de seguridad TI; (iii) en promedio, existen dos funcionarios por entidad que trabajan el tema de seguridad de la información; (iv) en las entidades públicas, los presupuestos en inversión de la seguridad son muy bajos, pues el 37% tuvo menos de 60 millones de pesos y el 24% no tuvo inversión; y (v) tan solo un 17% manifestó un aumento de presupuesto, con respecto al año anterior, dentro de la asignación del presupuesto para la inversión en seguridad. Dentro de este rubro, la inversión dirigida a protección de la red representa el 25%, y seguridad de la información el 10% (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015c).

En este mismo sentido, se identifica que los organismos, instancias y entidades encargadas del análisis, identificación, prevención, investigación y persecución al cibercrímen y la ciberdelincuencia en el país, no cuentan con los recursos humanos, técnicos y financieros suficientes para enfrentar nuevos tipos de crimen y delincuencia a nivel nacional y transnacional. Tampoco se basan en la gestión de riesgos de seguridad digital, lo que ocasiona mayor oportunidad para la materialización de amenazas cibernéticas.

Situación que resulta aún más preocupante si se tiene en cuenta que los esfuerzos de las entidades en el desarrollo de temas relacionados con investigación, desarrollo e innovación no son suficientes con relación a las necesidades y avances que se tienen de forma cotidiana en ataques cibernéticos. Hecho que repercute en la capacidad que tiene el Gobierno nacional para afrontar las amenazas cibernéticas a las que está constantemente expuesto.

Por otra parte, BID & OEA (2016) concluyen, de acuerdo a su modelo de madurez de capacidad de seguridad cibernética, que Colombia está en el nivel "establecido"[29] en los temas relacionados con el marco jurídico y reglamentario de seguridad cibernética en aspectos como privacidad, protección de datos y otros derechos humanos (Figura 2). Con esta clasificación, se reconoce que se han aplicado procedimientos reglamentarios y de legislación integral sobre protección de datos, evidenciado con la generación de la Ley 1581 de 2012, y su Decreto reglamentario 1377 de 2013. En esta ley se reconoce el derecho a la privacidad entregando la libertad al titular para elegir como serán tratados sus datos personales, así como estableciendo los responsables de dicho tratamiento. Igualmente se

[29] Según BID & OEA (2016) los elementos del subfactor están establecidos y funcionando. Sin embargo, no se ha considerado bien la asignación relativa de recursos. Ha habido poca toma de decisiones de compensación en relación con la inversión relativa en los distintos elementos del subfactor. Pero el subfactor es funcional y está definido.

indica que es necesario avanzar en temas de participación y cooperación internacional, con un intercambio efectivo de información para combatir delitos de seguridad cibernética. Esto, con el fin de aportar instrumentos de contextos transnacionales para la detección, investigación y judicialización de los responsables.

En aspectos como la investigación jurídica, Colombia quedó clasificada en un nivel "formativo"[30] para la fiscalía, por ejemplo. De esta forma se identifica que el número de fiscales capacitados para lograr construir un caso validado sobre pruebas electrónicas es limitado. Lo anterior, porque a pesar que se han tenido algunos programas de formación especializada, aún hace falta institucionalizar estos esfuerzos y ampliar los mecanismos de colaboración entre la fiscalía y la policía, obteniendo de esta forma un apoyo en la resolución de casos de delitos cibernéticos.

En atención al rol que cumplen los jueces y fiscales en el proceso judicial en torno a casos relacionados con el cibercrímen, no son suficientes las competencias técnicas de estas instancias. Se debe encaminar a construir un marco jurídico maduro que apoye los procesos judiciales, juzguen conductas de manera efectiva, apoyen procesos de investigación estructural, y cuente con la capacidad de adaptarse dinámicamente en función de las circunstancias imperantes.

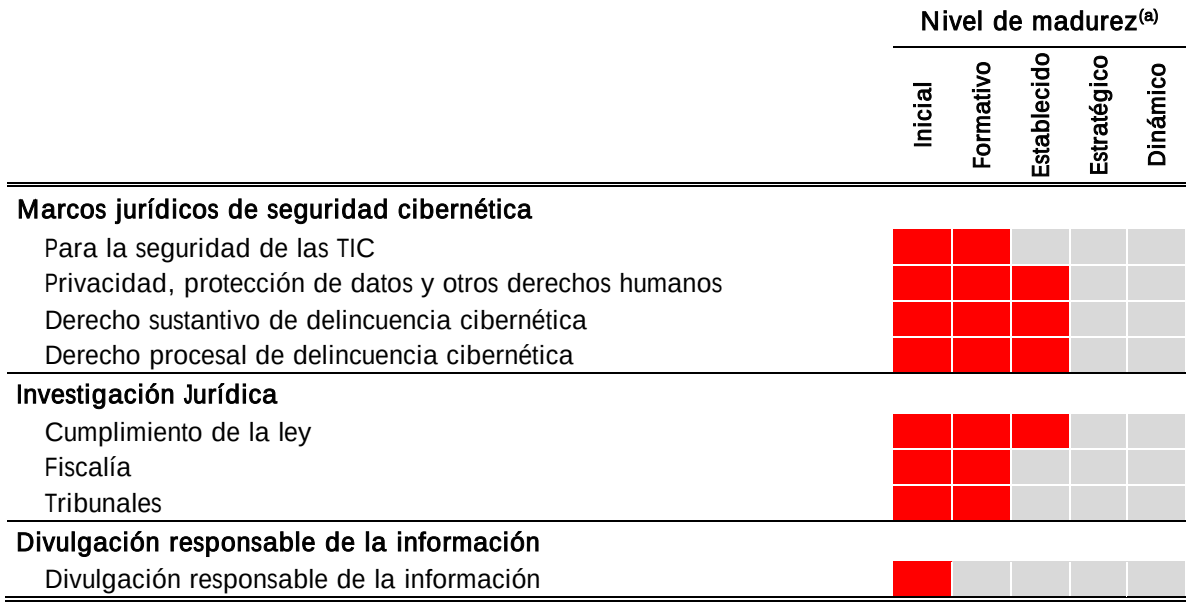
A pesar de los desarrollos normativos en la materia, se requiere la revisión y mejoramiento de cada una de las instancias judiciales, así como de las sanciones administrativas y disciplinarias sobre la comisión o prevención de un delito informático.

Dadas las nuevas formas de criminalidad, tal revisión debe considerar el hecho de que actualmente las grandes redes criminales y el crimen organizado han adquirido una pericia especial en el manejo de nuevas tecnologías, lo que ha potenciado y ampliado sus capacidades, facilitando su actuar y optimizando sus rendimientos. El crimen organizado ha escogido como una gran aliada a la tecnología, y en esa medida crimen y mundo digital se funden en una amalgama que, vista desde la perspectiva del riesgo país, constituye una amenaza contra la seguridad nacional. Por tanto, es indispensable que en el país se dé un

[30] Según BID & OEA (2016) algunas características del subfactor han comenzado a crecer y ser formuladas, pero pueden ser casuales, desorganizadas, mal definidas o simplemente nuevas.

entendimiento claro de los fenómenos tales como el de ciberlavado de activos[31], el ciberterrorismo, la ciberdelincuencia, el ciberespionaje o el cibersabotaje[32].

Figura 2. Nivel de madurez del marco jurídico y reglamentario de seguridad cibernética en Colombia, 2015



Fuente: BID & OEA (2016).
Nota: Para las definiciones referiste a la 23.

De otro lado, el incremento continuo de la comisión de las conductas delictivas cibernéticas y su reincidencia, entre otros factores, se debe al desconocimiento por parte de los administradores de justicia de la conducta criminal informática. En el marco de las nuevas tendencias y modalidades en ataques cibernéticos, y con el objetivo de ampliar las capacidades de los jueces, fiscales y policías para ejercer sus funciones acorde con la nueva política, es indispensable capacitarlos en la materia. Así, se facilitaría la comprensión respecto del ámbito de aplicación de la comisión de dichas conductas, y de la debilidad de las herramientas jurídicas para encuadrar la conducta del delito informático dentro del Código penal. El proceso probatorio requiere conocimientos sobre el alcance del tema, así

[31] Delito transnacional cuya comisión, en el ámbito de la globalización, de la sociedad informática y de redes, hace uso del ciberespacio y de las distintas tecnologías que hacen parte de este. Las tipologías de lavado de activos continuamente deben actualizarse para incluir nuevas técnicas, con el fin de realizar una adecuada actividad de prevención, detección, represión o adopción de medidas. Dentro de las modalidades de ciberlavado, es preciso tener en cuenta, principalmente, la creación de compañías de portafolios, transferencias inalámbricas entre corresponsales, ventas fraudulentas de bienes, y utilización del mercado negro de cambio del peso, bancos fantasmas y monedas virtuales.

[32] Es importante tener en cuenta el cubrimiento del Internet Superficial, el Deep Web y el Dark Web, ya que el Cibercrímen se mueve de forma clandestina y eficiente en estas porciones profundas de la Web.

un juez o un fiscal que conozca los tipos de afectaciones a la seguridad digital o la comisión de delitos cibernéticas, podrá avanzar de manera más efectiva en la investigación de estas conductas. En ese orden de ideas, la capacitación es fundamental y contribuye a una mejora en la judicialización de estas conductas

4.4. Es necesario reforzar las capacidades de ciberdefensa con un enfoque de gestión de riesgos

El año 2015 marcó el inicio de un cambio significativo hacia nuevas amenazas cibernéticas que son más difíciles de detectar, lo que significa una mayor incertidumbre frente a la seguridad digital a nivel global (INTEL SECURITY, 2015b). Los riesgos asociados a dicha incertidumbre apuntan no solo a bases de datos o sistemas de información, sino también a la infraestructura física nacional, como hidroeléctricas, redes de energía, sistemas portuarios, sistemas de defensa, o armamento de guerra, entre otros, que utilizan redes de comunicaciones como base para su funcionamiento. Lo que se conoce como infraestructuras críticas nacionales. Por citar un ejemplo, terroristas podrían tratar de apagar la captación de agua de una hidroeléctrica o tomar el control de aviones no tripulados, armas y sistemas de orientación de las fuerzas militares para causar daño a la población o, incluso, a las mismas instalaciones militares.

En Colombia, el CCOC y el colCERT pasaron de gestionar un total de 769 incidentes digitales de defensa nacional durante el año 2014, a 957 durante el año 2015. Del total de incidentes digitales de defensa en el 2015, el 27,4% corresponde a *defacement*, el 16% a malware (código malicioso), el 15,9% a infiltración lógica externa[33] y el 13,5% a infiltración lógica interna[34] (Gráfico 5).

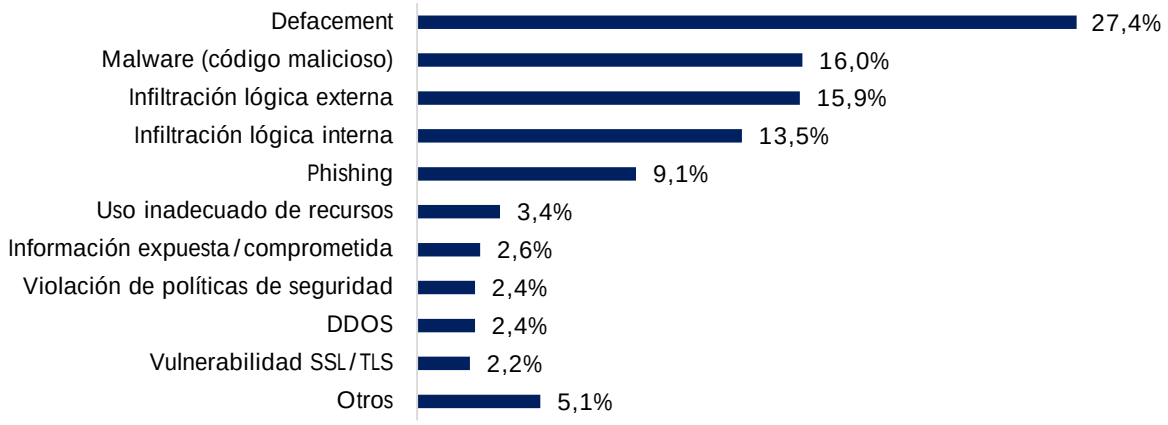
En cuanto a infraestructuras críticas nacionales, un estudio desarrollado por INTEL SECURITY (2015c) a partir de una encuesta realizada en 2015 a profesionales de la seguridad de la información de 625 organizaciones a nivel global, encuentra que casi nueve de cada diez encuestados han experimentado al menos un ataque cibernético en los sistemas de seguridad de su organización durante el 2014, con una media de cerca de veinte ataques por año. Adicionalmente, más del 70% de los encuestados piensa que las amenazas cibernéticas a su organización están aumentando, y al 48% le parece probable que un ataque para poner fuera de operación las infraestructuras críticas nacionales puede estar acompañado de pérdidas potenciales de vidas humanas. Por ejemplo, más del 59% de los

[33] Actividad de un intruso que accede de manera abusiva a un sistema informático aprovechándose de una vulnerabilidad y eligiendo un vector de ataque de la organización logrando con ello afecta la disponibilidad, confidencialidad o la integridad de los datos.

[34] Actividad que se deriva de la participación y responsabilidad de un empleado con conocimientos para acceder a un sistema informático de la organización aprovechando de las potenciales vulnerabilidades o carentes en materia de políticas de seguridad de la información.

encuestados respondió que los ataques dejaron como resultado un daño físico y más del 33% dio lugar a la interrupción del servicio.

Gráfico 5. Incidentes digitales gestionados por el CCOC y el colCERT en el entorno digital en Colombia, 2015



Fuente: CCOC y colCERT, 2015.

Se ha demostrado que las amenazas cibernéticas a las infraestructuras críticas nacionales son una realidad incuestionable y presentan una tendencia creciente. En 2015, la OEA y Trend Micro realizaron una encuesta cuantitativa en línea entre los jefes de seguridad de las principales infraestructuras críticas nacionales de todos los Estados miembros. En la encuesta también se incluyeron organizaciones privadas que gestionan la infraestructura crítica en sus países. Entre los principales resultados, se encontró que el 53% de los encuestados había observado un incremento de los incidentes digitales en sus sistemas de cómputo durante el 2014, y que el 76% de los encuestados percibía que dichos incidentes contra las infraestructuras críticas nacionales se están volviendo más sofisticados. Concluyen que los creadores de amenazas cibernéticas podrían estar apuntando a infraestructuras más vulnerables en el futuro.

A nivel local, actualmente el marco jurídico no contempla los aspectos necesarios para facilitar la protección y defensa de las infraestructuras críticas cibernéticas nacionales y, a diciembre de 2015, el país aún no contaba con un catálogo de infraestructuras críticas cibernéticas nacionales. Ausencia que incrementa el índice de riesgos de materialización de amenazas cibernéticas sobre las mismas, y facilita la inadecuada gestión de riesgos, protección y defensa. Además, dificulta la correcta planeación de recursos y los esfuerzos en materia de seguridad digital de los diferentes sectores económicos y productivos del país. La afectación o destrucción de cualquier infraestructura crítica cibernética nacional, que soporte los procesos de servicios esenciales a la población, traería consigo efectos y consecuencias

devastadoras para el país, e incluso podría ocasionar la pérdida de gobernabilidad en pocos minutos.

De esta manera, es indispensable generar una estrategia de protección de la infraestructura crítica cibernética en el país, culminando el proceso de catalogación de dicha infraestructura bajo un enfoque de gestión de riesgos de seguridad digital, y vinculando activamente a las múltiples partes interesadas, especialmente al sector privado.

En cuanto a ciberterrorismo, el informe final presentado en el 2015 por el Grupo de expertos gubernamentales sobre avances en la información y las telecomunicaciones, en el contexto de la ciberseguridad internacional de Naciones Unidas, resalta la utilización de las TIC con fines de terrorismo. Dicha utilización trasciende a las habituales actividades de reclutamiento, financiación, capacitación e incitación, llegando a la comisión de atentados terroristas contra las TIC o infraestructuras dependientes de estas tecnologías. Temas que si no se abordan pueden amenazar la seguridad ciudadana, la paz y la seguridad internacional.

Es de señalar que el país se ha visto afectado por fenómenos que pueden impactar la seguridad y los medios de defensa existentes. Estos fenómenos se caracterizan no sólo por su incremento y lugares de procedencia, sino también por su complejidad y sofisticación mediante el uso de técnicas cada vez más especializadas, trayendo como consecuencia un mayor grado de dificultad en la anticipación, detección oportuna y contención.

La situación señalada es aún más preocupante si se tiene en cuenta que el Gobierno nacional actualmente no recibe información sobre incidentes por parte de las múltiples partes interesadas, con el fin de priorizar y emitir lineamientos para garantizar la defensa y soberanía nacional. Además, existen sectores de la economía que no han creado sus equipos de respuesta y, por lo tanto, no disponen de una instancia para reaccionar a los incidentes digitales de modo centralizado y especializado, no tratan las cuestiones jurídicas en la materia de manera homogénea dentro del sector específico, no adelantan seguimiento de manera unificada a las principales tipologías de riesgos, entre otros. Por consiguiente, es necesario promover la creación de nuevos CSIRT sectoriales, que permitan la adecuada gestión de incidentes digitales en los diversos sectores de la economía.

4.5. Los esfuerzos de cooperación, colaboración y asistencia, nacionales e internacionales, relacionados con la seguridad digital son insuficientes y desarticulados

La naturaleza transnacional del delito cibernético y del cibercrímen, en particular la volatilidad de la evidencia electrónica, implican que la justicia penal no puede ser efectiva sin una cooperación internacional eficiente.

En Colombia, se evidencia que existen esfuerzos aislados de cooperación nacional e internacional por parte de los responsables de la seguridad digital, por lo que se presentan dificultades en el intercambio de conocimiento, experiencias, investigación, desarrollo de nuevas tecnologías, e información relacionada con los incidentes digitales. Los esfuerzos en materia de cooperación, colaboración y asistencia internacional en seguridad digital, no son suficientes ni responden a una estrategia permanente que maximice su aprovechamiento.

Por ejemplo, Colombia no se ha adherido a convenios internacionales en materia de seguridad digital, desaprovechando oportunidades en aspectos tales como la cooperación, el intercambio de información, la asistencia judicial recíproca y la capacitación. Esto dificulta la implementación de mejores prácticas, la identificación temprana de nuevos tipos de incertidumbres, riesgos digitales o amenazas cibernéticas, los procesos de actualización de procedimientos relacionados con la gestión del riesgo, entre otros.

A nivel nacional, no existe un mecanismo que facilite la cooperación, colaboración y asistencia entre las múltiples partes interesadas. Se evidencia que no se han establecido canales de comunicación soportados en una efectiva estrategia de comunicación entre el Gobierno nacional, el sector privado y la academia, lo cual genera duplicidad de esfuerzos y falta de efectividad en la formalización de convenios bilaterales y multilaterales.

Por otra parte, Colombia debe incrementar y articular la capacidad de acceso e intercambio de información, que contribuya a la prevención, detección y contención de amenazas cibernéticas. Según instrumentos proferidos por organismos internacionales, de los cuales hace parte Colombia, el Estado debe promover el intercambio de información entre las múltiples partes interesadas, y especialmente entre las agencias y autoridades competentes para prevenir, detectar, y orientar la toma de decisiones, y contener nuevas amenazas cibernéticas.

5. Definición de la política

En esta sección se describe la política nacional de seguridad digital, teniendo en cuenta los principios fundamentales y dimensiones estratégicas definidas en el Marco conceptual.

5.1. Objetivo general

Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

5.2. Objetivos específicos

Con el fin de cumplir el objetivo general, bajo los principios fundamentales establecidos en el Marco conceptual, se formulan cinco objetivos específicos. Estos serán alcanzados mediante la ejecución de un conjunto de estrategias, las cuales están determinadas por las dimensiones estratégicas que rigen esta política[35] (explicadas en el Marco conceptual).

5.2.1. Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos

E1.1. Establecer un marco institucional articulado que involucre a las múltiples partes interesadas para la implementación de la política nacional de seguridad digital (DE1)

E1.2. Implementar en el Gobierno nacional un modelo de gestión de riesgos de seguridad digital (DE3)

5.2.2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital

E2.1. Establecer mecanismos de participación activa y permanente de las múltiples partes interesadas en la gestión del riesgo de seguridad digital (DE1)

E2.2. Adecuar el marco legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes (DE2)

E2.3. Identificar y abordar los posibles impactos negativos que otras políticas pueden generar sobre las actividades de las múltiples partes interesadas en el entorno digital o sobre la prosperidad económica y social (DE3)

E2.4. Generar confianza en las múltiples partes interesadas en el uso del entorno digital (DE4)

E2.5. Promover en los diferentes niveles de formación comportamientos responsables en el entorno digital (DE5)

5.2.3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos

E3.1. Fortalecer las instancias y entidades responsables de ciberseguridad (DE1)

E3.2. Adecuar el marco jurídico sobre los delitos cibernéticos, cibercrímenes y fenómenos en el entorno digital (DE2)

[35] Al final de cada estrategia se indica, en paréntesis, la dimensión estratégica sobre la cual actúa.

E3.3. Socializar y concientizar las tipologías de cibercrímen y ciberdelincuencia a las múltiples partes interesadas (DE4)

E3.4. Fortalecer las capacidades de los responsables de seguridad nacional en el ciberespacio y de la judicialización de delitos cibernéticos y cibercrímenes (DE5)

5.2.4. Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos

E4.1. Fortalecer las instancias y entidades responsables de la defensa nacional en el entorno digital (DE1)

E4.2. Adecuar el marco jurídico para abordar la protección y defensa del entorno digital nacional (DE2)

E4.3. Generar una estrategia de protección y defensa de la infraestructura crítica cibernética nacional (DE3)

E4.4. Fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, con la participación activa de las múltiples partes interesadas (DE4)

E4.5. Fortalecer las capacidades de los responsables de garantizar la defensa nacional en el entorno digital (DE5)

5.2.5. Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional

E5.1. Generar mecanismos para impulsar la cooperación, colaboración y asistencia a nivel internacional, en materia de seguridad digital (DE1)

E5.2. Fortalecer la cooperación, colaboración y asistencia a nivel nacional, entre las múltiples partes interesadas en temas de seguridad digital (DE5)

5.3. Implementación de las estrategias: plan de acción

A continuación se describen las estrategias que se implementarán para alcanzar los objetivos específicos enunciados en la sección 0. El detalle de las acciones aquí expuestas se puede consultar en el Plan de Acción y Seguimiento (PAS, Anexo A), donde se establecen las entidades responsables de cada acción, los periodos de ejecución de las mismas, los recursos necesarios para llevarlas a cabo, y la importancia de cada acción para el cumplimiento del objetivo general de la política nacional de seguridad digital.

5.3.1. Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos

Con el fin de alcanzar este objetivo específico, el Gobierno nacional: (i) establecerá un marco institucional articulado para la implementación de la política nacional de seguridad digital, e (ii) implementará un modelo de gestión de riesgos de seguridad digital.

E1.1. Establecer un marco institucional articulado que involucre a las múltiples partes interesadas para la implementación de la política nacional de seguridad digital (DE1)

Con el objetivo de que el país tenga una visión estratégica en seguridad digital, el DNP creará la figura de coordinador nacional de seguridad digital. Dicha figura deberá ser creada a más tardar el 31 de diciembre de 2016, y se debe garantizar que (i) tenga la idoneidad; (ii) se definan las competencias específicas; y (iii) esté dotado de las herramientas jurídicas que le permitan desempeñar sus funciones con la mayor efectividad. Dicha figura será un funcionario dependiente del Departamento Nacional de Planeación, el cual tendrá como mínimo las siguientes funciones:

- Dirigir la implementación de la política nacional de seguridad digital y hacer seguimiento continuo de la misma.
- Llevar a cabo la coordinación interinstitucional e intersectorial en temas de seguridad digital.
- Garantizar que el alcance de la seguridad digital en el país incluya los objetivos: (i) de prosperidad económica y social; (ii) de ciberseguridad, para enfrentar nuevos tipos de crimen, delincuencia, y otros fenómenos que afecten la seguridad nacional; y (iii) de ciberdefensa.
- Garantizar que los programas, proyectos y campañas de concientización y sensibilización, así como las capacitaciones que adelanten las diferentes entidades, se diseñen a partir de los lineamientos y orientaciones que emita la Comisión Nacional Digital y de Información Estatal, o de quien haga sus veces, con el fin de evitar la duplicación de esfuerzos y garantizar la eficiencia en el manejo de los recursos.
- Recomendar nuevas acciones en colaboración con las múltiples partes interesadas, en vista de la rápida tasa de desarrollo de la tecnología y los escenarios de ataques cibernéticos.
- Coordinar (i) con la Comisión Nacional Digital y de Información Estatal, o quien haga sus veces; y (ii) con las múltiples partes interesadas, los informes respecto del cumplimiento de los lineamientos de orientación superior establecidos para la implementación de la política nacional de seguridad digital en el marco de sus principios fundamentales.

El coordinador nacional de seguridad digital tendrá a su cargo un equipo de apoyo operativo intersectorial, el cual estará conformado por representantes de, al menos, las siguientes entidades: Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional y la Dirección Nacional de Inteligencia.

Adicionalmente, el DNP, con apoyo del Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones, deberá modificar el Decreto 32 de 2013[36], a más tardar el 31 de diciembre de 2017, para armonizar la institucionalidad actual de la Comisión Nacional Digital y de Información Estatal, con el nuevo enfoque de gestión de riesgos de seguridad digital. Así, esta será la instancia de máximo nivel interinstitucional e intersectorial en el Gobierno nacional, que orientará la seguridad digital en Colombia. Las operaciones de esta comisión se modificarán para incluir dos niveles: nivel técnico (directivos técnicos), para resolver y analizar temas nacionales de seguridad digital; y nivel ministerial, para ratificar las recomendaciones del nivel técnico.

Por otro lado, con el fin de avanzar en la adopción de un enfoque de múltiples partes interesadas, el coordinador nacional de seguridad digital del DNP, con apoyo del Departamento Administrativo de la Función Pública (DAFP), definirá en cada ministerio y departamento administrativo de orden nacional el enlace sectorial en los temas de seguridad digital, a más tardar el 30 de junio de 2017. Este enlace es el interlocutor con (i) el coordinador nacional de seguridad digital; (ii) la instancia de máximo nivel en el Gobierno nacional; y (iii) las múltiples partes interesadas. Adicionalmente, el enlace sectorial será el encargado de rendir cuentas al coordinador nacional de seguridad digital, acerca de la implementación de la política nacional de seguridad digital en la respectiva entidad. Por su parte, el Ministerio de Tecnologías de la Información y las Comunicaciones deberá adelantar jornadas de sensibilización durante el año 2017 para que los entes territoriales definan un enlace en la materia.

En este mismo sentido, el Ministerio de Defensa Nacional elaborará, durante el año 2016, un plan de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del colCERT, como punto focal nacional para la gestión de incidentes digitales en Colombia. Plan que será debidamente ejecutado entre los años 2017 y 2019.

En el largo plazo, se espera que se cree una Dirección de Ciberseguridad y Ciberdefensa, dependiente del Viceministerio de Defensa para las Políticas y Asuntos Internacionales, la cual se constituiría como un elemento relevante para implementar niveles de escalonamiento para el reporte de incidentes digitales y garantizar la participación de las múltiples partes interesadas en la gestión de riesgos de la seguridad digital. En el corto plazo,

[36] Por el cual se crea la Comisión Nacional Digital y de Información Estatal.

se comenzará por implementar el plan de fortalecimiento para el colCERT. Plan que permitirá desarrollar las capacidades necesarias para implementar un esquema de gobernabilidad participativa de múltiples partes interesadas, y definir los niveles de escalamiento para el reporte de incidentes digitales. Así, en el periodo de ejecución de esta política, el colCERT continuará como una dependencia del Ministerio de Defensa Nacional

El plan incluirá un análisis detallado de las capacidades actuales, así como insumos de revisiones externas que permitan orientar las acciones requeridas en cada uno de los frentes. Este plan, además deberá considerar aspectos de orden presupuestal, y plantear estrategias para gestionar recursos provenientes de fuentes diferentes al Gobierno nacional, como por ejemplo, alianzas con gremios, instituciones privadas, el desarrollo de actividades mediante un portafolio de servicios que genere ingresos, entre otros.

E1.2. Implementar en el Gobierno nacional un modelo de gestión de riesgos de seguridad digital (DE3)

El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará un modelo de gestión de riesgos de seguridad digital, teniendo en cuenta el marco conceptual de esta política, los estándares de seguridad internacionales y el marco de gestión de riesgos integral a nivel nacional. El modelo debe (i) ser parte integral del proceso de toma de decisiones; (ii) estar soportado en el conjunto de principios fundamentales de la política nacional de seguridad digital; (iii) incluir los mecanismos para identificar, evaluar y tratar el riesgo de seguridad digital, así como para seleccionar medidas de seguridad, de preparación y de recuperación; y (iv) asegurar la aplicación de protocolos seguros y de controles respectivos para medir la efectividad en la implementación por parte de las múltiples partes interesadas. Dicho modelo debe incorporar los lineamientos y orientaciones que emita la Comisión Nacional Digital y de Información Estatal. El coordinador nacional de seguridad digital debe aprobar el modelo y velar porque lo anterior se cumpla. El modelo debe ser socializado y ajustado con base en comentarios recibidos, para luego ser publicado a más tardar el 31 de diciembre de 2018.

El coordinador nacional de seguridad digital del DNP, en colaboración con el DAFP, generará los mecanismos administrativos para que todas las entidades y departamentos administrativos de la rama ejecutiva adopten e implementen, de forma permanente, el modelo de gestión de riesgos de seguridad digital establecido. Así mismo, durante los años 2018 y 2019, el coordinador nacional realizará jornadas de promoción activa del uso del modelo de gestión de riesgos de seguridad digital por parte de las múltiples partes interesadas vinculadas a cada sector específico. También informará semestralmente a la máxima instancia de seguridad digital cómo avanza la implementación del modelo.

5.3.2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital

Con el fin de alcanzar este objetivo específico, el Gobierno nacional adelantará las siguientes estrategias: (i) establecerá mecanismos de participación activa y permanente de las múltiples partes interesadas en la gestión del riesgo de seguridad digital, (ii) adecuará el marco legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes, (iii) identificará y abordará los posibles impactos negativos que otras políticas pueden generar sobre las actividades de las múltiples partes interesadas o sobre la prosperidad económica y social en el entorno digital, (iv) generará confianza a las múltiples partes interesadas en el uso del entorno digital, y (v) promoverá comportamientos responsables en el entorno digital en diferentes niveles de formación educativa.

E2.1. Establecer mecanismos de participación activa y permanente de las múltiples partes interesadas en la gestión del riesgo de seguridad digital (DE1)

Esta estrategia busca involucrar a las múltiples partes interesadas en la gestión del riesgo de seguridad digital, de tal forma que asuman la responsabilidad que les corresponde de acuerdo a su rol y función, y participen activamente tanto en la fase de construcción de los elementos que se consignan en este documento, como en la implementación de la política. Para esto, el coordinador nacional de seguridad digital diseñará, a más tardar el 30 de junio de 2017, un mecanismo dinámico de coordinación que defina (i) los roles, las responsabilidades y las funciones de las múltiples partes interesadas; y (ii) una matriz de comunicación y seguimiento entre el coordinador nacional de seguridad digital, la instancia de máximo nivel del Gobierno y las múltiples partes interesadas, con el fin de abordar los temas de seguridad digital en Colombia.

Mediante dicho mecanismo de coordinación, se deben establecer las reglas para consultar sistemáticamente a las múltiples partes interesadas en la fase inicial y a lo largo de la implementación de la política. Además, se deben identificar los medios y procedimientos para organizar el diálogo sistemático y continuo entre las múltiples partes interesadas.

De igual forma, el coordinador nacional creará una agenda nacional de seguridad digital durante el año 2017, con el fin de priorizar los intereses nacionales en torno al tema, involucrando a las múltiples partes interesadas, e identificando variables de impacto nacional (por ejemplo, pérdidas económicas, afectación de personas, consecuencias medioambientales o correlación de la afectación con otras partes), bajo el marco de los principios fundamentales de la política nacional de seguridad digital. El coordinador nacional de seguridad digital debe incluir en la agenda un capítulo específico de vinculación de las

múltiples partes interesadas para gestionar los riesgos de seguridad digital en un escenario de posconflicto.

Finalmente, en julio de 2016, el Ministerio de Tecnologías de la Información y las Comunicaciones creará y pondrá en marcha un tanque de pensamiento con las múltiples partes interesadas para abordar la gestión de riesgos de seguridad digital mediante la investigación, el desarrollo y la innovación.

E2.2. Adecuar el marco legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes (DE2)

El Ministerio de Justicia y del Derecho conceptuará sobre la coherencia constitucional y legal de las propuestas, que presenten el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, la Superintendencia de Industria y Comercio, el Departamento Administrativo Dirección Nacional de Inteligencia (DNI) y la Unidad de Información y Análisis Financiero (UIAF), para adecuar el marco legal y regulatorio relacionado con temas de seguridad digital, en torno a la dinámica de la economía digital y sus incertidumbres inherentes. Esta adecuación se llevará a cabo bajo el marco de los principios fundamentales de la política nacional de seguridad digital.

Por su parte, la Comisión de Regulación de Comunicaciones (CRC) ajustará en 2017 el marco regulatorio del sector TIC. Lo anterior, lo hará teniendo en cuenta asuntos necesarios para la gestión de riesgos de seguridad digital, como la protección de usuarios de comunicaciones o el régimen de calidad de las redes de telecomunicaciones. Esto se hará aplicando la metodología de *Análisis de impacto normativo*, establecida en el Documento CONPES 3816[37].

E2.3. Identificar y abordar los posibles impactos negativos que otras políticas pueden generar sobre las actividades de las múltiples partes interesadas en el entorno digital o sobre la prosperidad económica y social (DE3)

Esta estrategia busca articular la gestión de riesgos de seguridad digital entre todas las entidades del Gobierno nacional, con un enfoque que sea flexible, tecnológicamente neutro y coherente. Para esto, el DNP elaborará un estudio de recomendaciones sobre las medidas que deben ser tomadas para garantizar la articulación y coherencia de la gestión de riesgos de seguridad digital con las distintas estrategias o políticas existentes, tales como el Plan Nacional de Desarrollo 2014-2018 o el Plan Vive Digital 2014-2018. Estas recomendaciones, deberán identificar los posibles impactos negativos que otras políticas pueden generar sobre las actividades de las múltiples partes interesadas en el entorno digital,

[37] Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3816.pdf

o sobre la prosperidad económica y social. Este estudio será entregado a la instancia de máximo nivel en seguridad digital a más tardar en junio de 2017.

Adicionalmente, el Ministerio de Tecnologías de la Información y las Comunicaciones adelantará, entre 2016 y 2017, un estudio sobre el impacto de los delitos y crímenes digitales en el entorno digital en el país. Este servirá de insumo al coordinador nacional de seguridad digital para ajustar la política definida en este documento y para el desarrollo de los planes futuros en la materia.

Así mismo, el coordinador nacional de seguridad digital evaluará anualmente, desde 2017, la gestión de riesgos de seguridad digital de manera integral, con el fin de estimular mejoras continuas en eficiencia y eficacia. Todas las entidades del orden nacional deberán proveer al coordinador nacional de seguridad digital los datos e información requeridos para esta evaluación.

Finalmente, en el 2019, el DNP, evaluará la viabilidad técnica de realizar una evaluación de impacto económico de la política para estimular mejoras continuas en la eficiencia y eficacia de la gestión de riesgos de seguridad digital. En caso de resultar favorable, esta evaluación será financiada por el Ministerio de Tecnologías de la Información y las Comunicaciones.

E2.4. Generar confianza en las múltiples partes interesadas en el uso del entorno digital (DE4)

El Ministerio de Tecnologías de la Información y las Comunicaciones ejecutará, durante los años 2017, 2018 y 2019, programas, proyectos y campañas nacionales de concientización y sensibilización, en alianza con el sector privado, destinadas a aumentar la confianza en el uso del entorno digital por parte de las múltiples partes interesadas. Lo anterior se hará garantizando la salvaguarda de los principios fundamentales de la política nacional de seguridad digital, y con base en los metas de la agenda nacional de seguridad digital. En el marco de esta actividad, el programa *En TIC Confío* del Ministerio de Tecnologías de la Información y las Comunicaciones será fortalecido presupuestalmente con el fin de generar conciencia en las múltiples partes interesadas sobre el uso de un entorno digital abierto, seguro y confiable en cada uno de los sectores, y se hará énfasis en la concientización y sensibilización de MIPYMES.

De igual manera, durante los años 2017 a 2019, dicho ministerio fortalecerá las capacidades de gestión de riesgos de seguridad digital en las entidades del Estado de veinticuatro sectores, de forma tal que en sus políticas, procesos y procedimientos se adopte la gestión de riesgos de seguridad. La selección de los sectores tendrá en cuenta, entre otros, el nivel de exposición de estos a incidentes digitales, así como el nivel de ocurrencia de

delitos y crímenes en el entorno digital que afectan a los mismos. Una vez hecha la selección, se capacitará a los líderes y directivos de las entidades en los sectores seleccionados en asuntos relacionados con la gestión del riesgo de la seguridad digital. Finalmente, el Ministerio de Tecnologías de la Información y las Comunicaciones asignará un equipo asesor para guiar a las entidades seleccionadas en el desarrollo de las acciones para la gestión de riesgos de seguridad digital y realizará visitas, según las necesidades identificadas en el proceso de selección y durante el acompañamiento.

Como resultado de estos procesos, se espera elevar la confianza de los ciudadanos, empresas y entidades del Estado, maximizando así las oportunidades que el entorno digital les ofrece. Los esfuerzos se enfocarán en actividades de capacitación y acompañamiento, respecto a temas de seguridad y privacidad en el entorno digital.

Adicionalmente, el mencionado ministerio diseñará e implementará esquemas tecnológicos y procedimentales para garantizar la identificación, autenticación y autorización de funcionarios, ciudadanos, activos de información y recursos[38] que acceden a la infraestructura del Estado colombiano.

Finalmente, el coordinador nacional de seguridad digital realizará jornadas de sensibilización cuatrimestrales a las múltiples partes interesadas en torno al uso de un entorno digital abierto, seguro y confiable en cada uno de los sectores, para lo cual contará con el apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones y del Ministerio de Defensa Nacional. En dichas jornadas se explicará a los asistentes cómo identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital. De igual manera, se comunicará brevemente a los asistentes el avance de la implementación de la política nacional de seguridad digital.

E2.5. Promover en los diferentes niveles de formación comportamientos responsables en el entorno digital (DE5)

Esta estrategia busca capacitar a los agentes que se encuentran en el sistema educativo, tanto estudiantes como docentes, acerca de su responsabilidad en la gestión de riesgos de seguridad digital. Esto, con el fin de promover el uso del entorno digital pero de manera responsable, lo que a su vez generará confianza en este.

El Gobierno nacional, a través del Ministerio de Educación Nacional, creará contenidos educativos complementarios relacionados con la gestión de riesgos de seguridad

[38] Activos de información y recursos se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

digital, y capacitará a los estudiantes de educación básica y media, y a los estudiantes de educación superior, a estos últimos a través del *Portal Educativo Colombia Aprende*. Dichos contenidos deben contemplar contextos pertinentes para los alumnos, de tal forma que puedan tomar decisiones concretas sobre los riesgos de seguridad digital, aún en situaciones inciertas. Igualmente, capacitará con contenidos educativos complementarios sobre medidas preventivas y correctivas, en torno a problemáticas de seguridad digital, a docentes, a través del *Portal educativo Colombia aprende* y de los diplomados del programa Computadores para educar del Ministerio de Tecnologías de la Información y las Comunicaciones.

5.3.3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos

Este objetivo busca empoderar a los ciudadanos y al Estado en relación con los riesgos del entorno digital, y consolidar las capacidades del país para hacer frente al crimen, la delincuencia y otros fenómenos que afectan la seguridad nacional desde este entorno. Para su cumplimiento, el Gobierno nacional ejecutará las cuatro estrategias que se describen a continuación.

E3.1. Fortalecer las instancias y entidades responsables de ciberseguridad (DE1)

Esta estrategia busca contribuir en la construcción de un marco institucional adecuado en materia de ciberseguridad para gestionar la seguridad digital bajo el liderazgo del Gobierno nacional. Es por esto que su campo de acción está definido por la primera dimensión estratégica de esta política: gobernanza de la seguridad digital.

Para tener un marco institucional adecuado en materia de ciberseguridad, en primer lugar se deben fortalecer las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del CCP de la Policía Nacional y de los organismos de Inteligencia del Estado, incluyendo la UIAF. Para esto, el Ministerio de Defensa Nacional (en el caso del CCP) y la Dirección Nacional de Inteligencia (en el caso del sector Inteligencia) elaborarán, durante los años 2016 y 2017, respectivamente, un plan de fortalecimiento en el que se definirán y ponderarán las actividades puntuales que se ejecutarán para robustecer las capacidades mencionadas. Se estima que el horizonte de este proyecto será hasta la vigencia 2019.

En segundo lugar, y teniendo en cuenta que la investigación e innovación son herramientas fundamentales para enfrentar los continuos avances que exhiben los ataques cibernéticos y desarrollar capacidades avanzadas, se evaluará la creación de nuevas instancias en las que se desarrolle formación, investigación e innovación, especialmente en relación con capacidades técnicas inherentes a la seguridad digital. Estas nuevas instancias apoyarían la institucionalidad existente, separando el trabajo operativo de aquel necesario

para lograr nuevos desarrollos en esta materia. Las capacidades desarrolladas por estas nuevas instancias brindarían al país mayor autonomía.

Para garantizar la pertinencia de la creación de las nuevas instancias, el Ministerio de Defensa Nacional efectuará los estudios de viabilidad que sean necesarios, y creará las que resulten viables. Deberá analizar, al menos, la viabilidad de la creación de las siguientes instancias:

- Centro criptológico nacional
- Centro de excelencia de seguridad digital
- Centro de fusión para investigación de crímenes económicos y financieros
- Centro de comunicaciones, cómputo, control y comando para la seguridad digital
- Observatorio de crímenes y delitos en el entorno digital.
- Laboratorio de informática forense.
- Centro de investigación en seguridad digital.

E3.2. Adecuar el marco jurídico sobre los delitos cibernéticos, cibercrímenes y fenómenos en el entorno digital (DE2)

Según el BID y la OEA (2016), la efectividad de la justicia penal es parte esencial de una estrategia de seguridad cibernética. Esto comprende la investigación, la fiscalización y la adjudicación de delitos en contra, y por medio de datos y sistemas informáticos, al igual que la obtención de evidencia electrónica relacionada con cualquier delito, para propósitos del proceso penal. Según los autores mencionados, el marco jurídico, que incluye el derecho sustantivo (la conducta a ser definida como delito) y el derecho procesal (los poderes investigativos para la aplicación de la ley), son fundamentales para que tenga lugar la respuesta de la justicia penal y debe cumplir con varios requisitos:

- Debe ser lo suficientemente neutral (tecnológicamente) como para responder a la evolución constante del crimen y de la tecnología, ya que de no ser así corre el peligro de volverse obsoleta cuando entre en vigor.
- Los poderes para la aplicación de la ley deben estar sujetos a salvaguardias con el fin de garantizar el cumplimiento de los requerimientos del Estado de derecho y de los derechos humanos.
- Debe operar con suficiente armonía o por lo menos ser compatible con las leyes de otros países, para permitir la cooperación internacional; por ejemplo, el cumplimiento con la condición de la doble criminalidad.

Teniendo en cuenta lo anterior, el Ministerio de Justicia y del Derecho definirá los lineamientos que faciliten los ajustes requeridos en el marco legal y regulatorio para adecuarlo a las necesidades en materia de (i) análisis, anticipación, prevención, detección, atención e investigación de delitos cibernéticos, cibercrímenes y fenómenos en el entorno digital, y de delitos y crímenes que utilicen el entorno digital como medio; (ii) persecución y criminalización de nuevos tipos delictivos, que incluya a los delitos informáticos como delitos fuente de lavado de activos; y (iii) actuación de los organismos de seguridad, defensa e inteligencia del Estado en el entorno digital, de acuerdo con los principios fundamentales de la política nacional de seguridad digital.

E3.3. Socializar y concientizar las tipologías de cibercrímen y ciberdelincuencia a las múltiples partes interesadas (DE4)

Uno de los aspectos en el que hace más énfasis esta política, es el relacionado a la responsabilidad que todas las partes interesadas tienen en cuanto a la gestión de riesgos de seguridad digital. Para el efecto, será muy importante que cada una de estas partes, incluyendo a cada ciudadano, entienda los riesgos del entorno digital y adopte medidas y comportamientos que resulten adecuados para reducir impactos negativos en el desarrollo de sus actividades económicas y sociales. Esto hace necesario adelantar procesos de sensibilización a todo nivel.

Los ejercicios de sensibilización y concientización se efectuarán de manera anual a través de la metodología de catedra o seminario, y sus contenidos serán definidos a partir de los siguientes criterios: (i) priorización de las partes interesadas más susceptibles a los ataques cibernéticos; (ii) análisis del tipo de incidente más recurrente en cada una de las múltiples partes interesadas; y (iii) tiempos de gestión a las respuestas de los incidentes presentados en cada una de las múltiples partes interesadas. Estos criterios son actualizados anualmente, con corte a 31 de diciembre, con base en las estadísticas nacionales generadas por el grupo colCERT del año inmediatamente anterior. Una vez sean actualizados, se definen las metodologías de sensibilización y concientización, y las temáticas que se abordarán en las capacitaciones de ese año. Asuntos que serán presentados al coordinador nacional por medio de un informe para garantizar que estén de acuerdo a los lineamientos dictados por la instancia de máximo nivel.

En los ejercicios de sensibilización y concientización, el Ministerio de Defensa Nacional también socializará a las mencionadas partes interesadas, los avances frente al fenómeno de cibercriminalidad y en los delitos informáticos que atenten contra la seguridad nacional en el entorno digital. Como resultado, dicho ministerio preparará anualmente, al coordinador nacional de seguridad digital, un informe de socialización y concientización. En este, se

reportará el número de ejercicios adelantados, la asistencia a los eventos, las conclusiones y las respectivas recomendaciones.

E3.4. Fortalecer las capacidades de los responsables de seguridad nacional en el ciberespacio y de la judicialización de delitos cibernéticos y cibercrímenes (DE5)

El Ministerio de Defensa Nacional diseñará contenido educativo especializado, durante 2017, para capacitar en al menos treinta entidades públicas a los funcionarios responsables de ciberseguridad y a aquellos encargados de la judicialización de delitos cibernéticos, de cibercrímenes, y de delitos y crímenes que utilicen el entorno digital como medio.

5.3.4. Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos

Este objetivo específico busca desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y defensa para garantizar los fines del Estado. Al mismo tiempo que busca mejorar la protección, preservar la integridad y la resiliencia de la infraestructura crítica cibernética nacional. Para esto, el Gobierno nacional adelantará las estrategias que se describen a continuación.

E4.1. Fortalecer las instancias y entidades responsables de la defensa nacional en el entorno digital (DE1)

El Ministerio de Defensa Nacional elaborará, entre junio y octubre de 2016, un plan de fortalecimiento que permita al sector Defensa generar una autonomía cibernética conducente a identificar, detectar y atender posibles amenazas en contra del Estado y su infraestructura critica. Dicho plan se concentrará en la definición de mejores prácticas y estándares internacionales en los componentes operativos, administrativos, humanos, científicos, de infraestructura física y tecnológica para el CCOC y las Unidades Cibernéticas de las Fuerzas Militares. Se estima que el horizonte del proyecto será hasta 2019.

Los mecanismos mediante los cuales se fortalecerán las entidades responsables de la defensa nacional en el entorno digital, se definirán en el marco de la construcción del plan de fortalecimiento. Este proceso estará liderado por el CCOC con el aval del Ministerio de Defensa Nacional e incluirá dos estudios de viabilidad técnica para la conformación de un Centro de operaciones cibernéticas de las Fuerzas Militares, y de un Centro nacional de protección y defensa de infraestructura crítica cibernética nacional, por medio de los cuales se robustecerá la seguridad digital toda vez que otorga una autonomía cibernética para el Estado colombiano.

E4.2. Adecuar el marco jurídico para abordar la protección y defensa del entorno digital nacional (DE2)

El Ministerio de Justicia y del Derecho conceptuará sobre la coherencia constitucional y legal de las propuestas que presenten el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, la Superintendencia de Industria y Comercio, el DNI y la UIAF, para adecuar el marco legal y regulatorio para abordar la protección y defensa del entorno digital en Colombia.

Bajo la adecuación del mencionado marco jurídico se debe buscar que esté acorde con las definiciones internacionales en lo relacionado con la gestión de incidentes, delitos informáticos, cibercrímen, entre otros. Tema que cobra especial importancia si se tiene en cuenta la futura adhesión de Colombia al Convenio sobre Ciberdelincuencia del Consejo de Europa.

La adecuación del marco jurídico deberá buscar, además, el reporte obligatorio de incidentes cibernéticos al colCERT por parte de los propietarios u operadores de infraestructuras críticas cibernéticas nacionales y demás partes interesadas, con las previsiones respectivas de confidencialidad, privacidad, entre otros aspectos.

E4.3. Generar una estrategia de protección y defensa de la infraestructura crítica cibernética nacional (DE3)

El Ministerio de Defensa Nacional, a partir de la Guía para la identificación de infraestructura crítica cibernética (2015), llevará a cabo la actualización periódica del catálogo de infraestructuras críticas cibernéticas nacionales. A partir de esto, establecerá los contenidos de los planes de protección de la infraestructura crítica cibernética nacional, y los socializará en el marco de la agenda nacional de seguridad digital.

El catálogo de infraestructura crítica se construye de forma conjunta entre el Ministerio de Defensa Nacional y las múltiples partes interesadas. Para esto, en una primera instancia, cada sector levantará su información con base en los siguientes criterios transversales: identificación de la infraestructura crítica digital, interdependencia con otras infraestructuras, y evaluación de la continuidad de negocio dependiendo de las amenazas latentes de sus servicios esenciales. Los avances en el levantamiento de la información se verificarán mensualmente por medio de reuniones convocadas por el CCOC. En una segunda instancia, las múltiples partes interesadas entregarán la información mencionada al Ministerio de Defensa Nacional para identificar, priorizar y definir el grado de criticidad de cada sector y entidad (catálogo de infraestructuras críticas cibernéticas nacionales).

El grado de criticidad de las infraestructuras cibernéticas definido por el catálogo, será el insumo principal para diseñar la estrategia de protección y defensa de la infraestructura

crítica cibernética nacional. Esta estrategia será construida por el Ministerio de Defensa Nacional en coordinación con los sectores, los subsectores y las entidades que participaron en el levantamiento de la información.

El proceso descrito tendrá que realizarse periódicamente con el fin de contar con un catálogo y una estrategia actualizados en todo momento. Característica esencial en lo relacionado con seguridad digital, teniendo en cuenta la evolución permanente de las amenazas en el ciberespacio. En cada actualización se buscará vincular a los sectores y entidades que aún no hayan decidido participar en el catálogo, reiterando la invitación a hacer parte del grupo de trabajo de la primera instancia. Esto permitirá robustecer el catálogo, y en consecuencia, la estrategia de protección y defensa.

E4.4. Fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, con la participación activa de las múltiples partes interesadas (DE4)

El coordinador nacional de seguridad digital apoyará la creación de CSIRT sectoriales, los cuales permitirán la adecuada gestión de incidentes digitales en los diversos sectores de la economía. El apoyo consistirá en identificar los sectores que no cuenten con dicho equipo de respuestas, motivarlos a participar de la comunidad CERT de Colombia, y pedirle al CSIRT que considere pertinente que actúe como garante en el proceso de creación de estas instancias[39].

Los CSIRT tendrán la capacidad de reacción ante incidentes especializados por sector y con capacidad real de interacción con los diferentes fabricantes, agencias de ley y otras agencias del gobierno. Adicionalmente, definirán prácticas adecuadas de gestión de seguridad en cada sector, asesorarán y acompañarán a las diferentes empresas.

Para mejorar continuamente la capacidad de respuesta a incidentes, anualmente, el coordinador nacional convocará a los CSIRT nacionales (existentes y a los que se constituirán en el marco de esta política) a una jornada de socialización. En estas jornadas cada equipo presentará las tipologías comunes de ataques cibernéticos en su sector o entidad, que atenten contra la defensa nacional en el entorno digital, y la manera eficiente de gestionar sus riesgos. Producto de estas jornadas de socialización el Ministerio de Defensa Nacional realizará un informe anual que será entregado al coordinador nacional de seguridad digital.

Finalmente, el Ministerio de Defensa Nacional, a través del colCERT, gestionará convenios y acuerdos de cooperación e intercambio de información con las múltiples

[39] Figura exigida por las metodologías internacionales para la creación de equipos de respuesta a incidentes cibernéticos.

interesadas. Lo anterior, con el fin de que la información de interés para la prevención de incidentes digitales sea conocida por los diferentes equipos de respuesta.

E4.5. Fortalecer las capacidades de los responsables de garantizar la defensa nacional en el entorno digital (DE5)

El Ministerio de Defensa Nacional diseñará contenidos educativos especializados y capacitará a las múltiples partes interesadas responsables de garantizar la defensa nacional en el entorno digital. El mismo ministerio realizará y participará en ejercicios de simulación y entrenamiento, nacionales e internacionales, que permitan desarrollar habilidades y destrezas para las múltiples partes interesadas responsables de las infraestructuras críticas cibernéticas nacionales y la defensa nacional en el entorno digital. En estas actividades participarían las múltiples partes interesadas responsables de las infraestructuras críticas cibernéticas nacionales y la defensa nacional en el entorno digital.

El desarrollo y fortalecimiento de las capacidades de ciberdefensa permiten afrontar las amenazas cibernéticas transnacionales, los desafíos y los retos que imponen los desarrollos tecnológicos y la convergencia de las telecomunicaciones en un mundo más globalizado e interconectado. Así mismo, mediante operaciones cibernéticas, se contribuye al desarrollo de las operaciones militares de tierra, mar, aire y espacio a fin de garantizar la superioridad militar en todo tiempo.

5.3.5. Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional

Este objetivo busca dinamizar la cooperación nacional entre las múltiples partes interesadas y la cooperación internacional en materia de seguridad digital. Para cumplir lo anterior se ejecutarán dos estrategias.

E5.1. Generar mecanismos para impulsar la cooperación, colaboración y asistencia a nivel internacional, en materia de seguridad digital (DE1)

Bajo esta estrategia, se busca la adhesión de Colombia a convenios internacionales en torno a la seguridad digital, tales como la Convención de Budapest; la presencia activa de las instancias nacionales de seguridad digital en organismos, redes de intercambio y eventos internacionales; e impulsar los trámites de firma de acuerdos de cooperación, colaboración o asistencia a nivel internacional.

Para lograr lo anterior, el Ministerio de Relaciones Exteriores definirá una agenda estratégica internacional a más tardar en diciembre de 2017, que identifique prioridades respecto a cooperación, colaboración y asistencia a nivel internacional en temas de seguridad digital, bajo el esquema de múltiples partes interesadas. El coordinador nacional

de seguridad digital debe velar por que esta agenda esté relacionada con la agenda nacional de seguridad digital y que se cumpla. Adicionalmente, el ministerio en mención realizará seguimiento a los temas relacionados con la seguridad digital en el ámbito bilateral, subregional, regional y multilateral.

El seguimiento mencionado se hará desde cada una de las dependencias de la Cancillería en las que puedan existir temas relacionados con la seguridad digital. Posteriormente, la Dirección de asuntos políticos multilaterales, a través de la Coordinación de prevención del delito, recopilará la información con el fin de realizar informes semestrales de seguimiento. Con el fin de que haya una articulación efectiva con el coordinador nacional de seguridad digital, el Ministerio de Relaciones Exteriores entregará los informes mencionados a dicho actor.

Todo esto con el fin de adelantar la debida determinación de los temas relevantes a ser impulsados en la agenda internacional por parte de Colombia, y proceder con el seguimiento respectivo del tema promovido.

E5.2. Fortalecer la cooperación, colaboración y asistencia a nivel nacional, entre las múltiples partes interesadas en temas de seguridad digital (DE5)

El Ministerio de Tecnologías de la Información y Comunicaciones, con la participación del coordinador nacional de seguridad digital, definirá una agenda estratégica de cooperación, colaboración y asistencia nacional en temas de seguridad digital.

Dicho ministerio creará un documento que contenga la descripción completa de la agenda. Este documento será una de las herramientas que permitirá profundizar las relaciones de las múltiples partes interesadas a nivel nacional, y que contribuirá con el desarrollo e implementación de la política nacional de seguridad digital. Dicha agenda debe ser amplia, incluyente y coherente, y debe facilitar una colaboración efectiva entre actores, cumplir metas comunes e incentivar una participación activa e incluyente. Adicionalmente, en la agenda se deben (i) identificar y definir los lineamientos prioritarios de la cooperación, colaboración y asistencia; (ii) definir áreas de demanda prioritarias en torno a la cooperación, a la colaboración y a la asistencia entre las partes interesadas a nivel nacional; (iii) definir áreas de oferta prioritarias en torno a la cooperación, a la colaboración y a la asistencia entre las partes interesadas a nivel nacional; y (iv) los mecanismos de seguimiento y evaluación.

El mismo ministerio, adelantará catorce jornadas de intercambio y transferencia de conocimiento (por parte de expertos internacionales) en materia de seguridad digital con las múltiples partes interesadas, a nivel nacional y territorial. Con estas jornadas se busca promover una apropiación social del conocimiento a partir de las mejores experiencias

internacionales, entendiendo por esta un proceso de comprensión y uso de la gestión del riesgo de seguridad digital. Se adelantarán dos jornadas en 2016, tres en 2017, cuatro en 2018 y cinco en 2019.

En el marco del horizonte fijado para la implementación de la política, todas las acciones propuestas deberán cumplirse a más tardar el 31 de diciembre de 2019, bajo el liderazgo del Ministerio de Defensa Nacional y del Ministerio de Tecnologías de la Información y Comunicaciones.

5.4. Valoración de impacto económico de la política

La CRC de Colombia, con apoyo del DNP, estimó el impacto económico de la adopción e implementación de la política nacional de seguridad digital en Colombia al año 2020, mediante el uso de un Modelo de Equilibrio General Computado (MEGC) dinámico[40]. Se estima que la implementación de dicha política al año 2020 habría generado alrededor de 307.000[41] empleos, y un crecimiento aproximado de 0,09% en la tasa promedio de variación anual del PIB, sin generar presiones inflacionarias.

La Tabla 8 presenta los resultados de la valoración del impacto económico. Los supuestos del ejercicio de valoración se presentan en el Anexo E del presente documento.

Tabla 8. Impacto económico esperado de la implementación de la política nacional de seguridad digital en Colombia

Promedios anuales, 2010-2020

Resultados	Unidad de medida	Escenario base	Escenario con gestión de riesgos de seguridad digital	Diferencia
Tasa de cambio	Pesos por USD	2.619,04	2.620,46	**1,42**
	Variación %	5,44%	5,45%	**0,01%**
Inflación al consumidor (canasta 2010)	Porcentaje	5,17	5,17	**0,00**
PIB	Miles de millones de pesos	755.571	772.013	**16.442**
	Crecimiento %	4,35%	4,44%%	**0,09%**

[40] El MEGC dinámico de la CRC es un instrumento de simulación económica y de evaluación de impacto de medidas económicas, construido para el conjunto de la economía con énfasis en el sector de comunicaciones a partir de la definición de varios escenarios. Este incluye ecuaciones definidas sobre la base de la teoría económica generalmente aceptada, interactuando con aspectos fiscales, monetarios y de inversión, con presencia de diversos agentes económicos.

[41] Se estima la creación de 307.000 empleos en el periodo 2016 a 2020, los cuales se dividen en dos categorías: (i) asalariados, e (ii) independientes y trabajadores no asalariados. Este dato es la creación nacional de empleo, por ende es la cantidad de empleos que se crean en todos los sectores de la economía, bien sea directamente por la Política nacional de seguridad digital, como por sus derivaciones.

Resultados	Unidad de medida	Escenario base	Escenario con gestión de riesgos de seguridad digital	Diferencia
Empleo total	Empleos	23.540.812	23.848.034	**307.222**
	Variación %	3,55%	3,88%	**0,33%**
Asalariados	Empleos	8.397.632	8.493.358	**95.726**
	Variación %	-1,11%	-0,78%	**0,33%**
Independientes y trabajadores no asalariados	Empleos	15.143.180	15.354.676	**211.496**
	Variación %	6,19%	6,51%	**0,33%**

Fuente: CRC con apoyo el apoyo del DNP, 2016.
Nota: El análisis parte de un escenario base que refleja la situación económica reciente (año 2015), la de los últimos cinco años (2010, 2011, 2012, 2013 y 2014), las estadísticas base del año 2010, y unas previsiones de precios internacionales, de políticas monetaria y fiscal para los años de proyección (2015-2020) considerados plausibles.

5.5. Seguimiento

El seguimiento a la ejecución física y presupuestal de las acciones propuestas para el cumplimiento de los objetivos del documento CONPES se realizará a través del PAS que se encuentra en el Anexo A. En este, se señalan las entidades responsables de cada acción, los periodos de ejecución de las mismas, los recursos necesarios y disponibles para llevarlas a cabo, y la importancia de cada acción para el cumplimiento del objetivo general de la política.

Tabla 9. Cronograma de seguimiento

Corte	Fecha	Porcentaje acumulado de implementación[a]
Primer corte	31 de diciembre de 2016	11%
Segundo corte	30 de junio de 2017	
Tercer corte	31 de diciembre de 2017	54%
Cuarto corte	30 de junio de 2018	
Quinto corte	31 de diciembre de 2018	77%
Sexto corte	30 de junio de 2019	
Informe de cierre	31 de diciembre de 2019	100%

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2015.
Nota: (a) Las metas establecidas en el PAS tienen una periodicidad anual, por lo tanto este valor solo se define para los cortes correspondientes al 31 de diciembre de cada año.

El reporte periódico al PAS se realizará por todas las entidades participantes en este documento CONPES, y será consolidado por el DNP de acuerdo con el cronograma de la

Tabla 9. En cada informe de seguimiento se deberá reportar el nivel de ejecución de todas las acciones iniciadas.

5.6. Financiamiento

Para efectos del cumplimiento de los objetivos específicos de esta política, las entidades involucradas en su ejecución, en el marco de sus competencias, gestionarán y priorizarán recursos para la financiación de las acciones que se proponen. Lo anterior, acorde con el Marco de Gasto de Mediano Plazo del respectivo sector.

En la Tabla 10 se encuentran los recursos asignados y las fuentes de los mismos, los cuales se ejecutarán durante el horizonte de la política nacional de seguridad digital en Colombia.

Tabla 10. Financiamiento estimado, 2016-2019

Millones de pesos

Entidad	2016	2017	2018	2019	Total
Ministerio de Defensa Nacional	14.618	7.392	7.583	7.782	**37.375**
Ministerio de Tecnologías de la Información y las Comunicaciones	8.750	13.950	13.000	9.550	**45.250**
Dirección Nacional de Inteligencia	-	-	500	1.000	**1.500**
Ministerio de Justicia y del Derecho	-	200	250	-	**450**
Ministerio de Educación Nacional	-	75	150	120	**345**
Departamento Nacional de Planeación	75	75	-	-	**150**
Total	**23.443**	**21.692**	**21.483**	**18.452**	**85.070**

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones y Ministerio de Defensa Nacional, 2015.

6. RECOMENDACIONES

El Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, el Departamento Administrativo de la Presidencia, el Ministerio de Educación Nacional, el Ministerio del Interior, el Ministerio de Justicia y del Derecho, el Ministerio de Relaciones Exteriores, el Departamento Administrativo Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación, recomiendan al Consejo Nacional de Política Económica y Social:

1. Aprobar la política nacional de seguridad digital en Colombia, incluyendo su Plan de Acción y Seguimiento (Anexo A).
2. Solicitar al Ministerio de Defensa Nacional:
    a. Con apoyo del coordinador nacional de seguridad digital, elaborar y ejecutar los planes de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del colCERT, del CCP y del CCOC, (diciembre de 2019).
    b. Realizar la actualización periódica del catálogo de infraestructuras críticas cibernéticas nacionales (a partir de enero de 2017).
3. Solicitar al Departamento Administrativo Dirección Nacional de Inteligencia:
    a. Con el apoyo del coordinador nacional de seguridad digital, elaborar y ejecutar el plan de fortalecimiento de las capacidades institucionales, operativas, administrativas, humanas, de infraestructura física y tecnológica del sector inteligencia DNI (diciembre de 2019).
4. Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones:
    a. Con apoyo del coordinador nacional de seguridad digital, diseñar un modelo de gestión de riesgos de seguridad digital a nivel nacional (diciembre de 2018); definir una agenda estratégica de cooperación, colaboración y asistencia en el ámbito nacional en temas de seguridad digital (diciembre de 2017); y crear un tanque de pensamiento con las múltiples partes interesadas para abordar la gestión de riesgos de seguridad digital mediante la investigación, el desarrollo y la innovación (diciembre de 2018).
5. Solicitar a la Comisión de Regulación de Comunicaciones:
    a. Ajustar el marco regulatorio del sector de Tecnologías de la Información y las Comunicaciones, teniendo en cuenta aspectos necesarios para la gestión de riesgos de seguridad digital (diciembre de 2017).
6. Solicitar al Ministerio de Educación Nacional:

a. Crear contenidos educativos complementarios relacionados con la gestión de riesgos de seguridad digital, y capacitar a: (i) los estudiantes de educación básica y media, (ii) los estudiantes de educación superior, y (iii) a los docentes (a partir de enero de 2017).

7. Solicitar al Ministerio de Justicia y del Derecho:

   a. Conceptuar sobre la coherencia constitucional y legal de las propuestas que presenten las entidades para modificar el marco legal y regulatorio de la seguridad digital en Colombia (diciembre de 2019).

   b. Proponer lineamientos de ajuste al marco legal y regulatorio para adecuarlos a las necesidades actuales en materia de seguridad digital, de acuerdo con los principios fundamentales de la política nacional de seguridad digital (junio de 2019).

8. Solicitar al Ministerio de Relaciones Exteriores:

   a. Con apoyo del coordinador nacional de seguridad digital, definir una agenda estratégica internacional en temas de seguridad digital (diciembre de 2017); y presentar, a solicitud de las entidades nacionales competentes, propuestas de acuerdos en materia de seguridad digital (a partir de julio de 2016).

9. Solicitar a todas las entidades del orden nacional de la rama ejecutiva:

   a. Adoptar e implementar el modelo de gestión de riesgos de seguridad digital a nivel nacional (a partir de enero de 2018), e informar el avance periódico de la aplicación de la gestión de riesgos de seguridad digital a la instancia de máximo nivel en seguridad digital (a partir de enero de 2018).

10. Solicitar al Departamento Nacional de Planeación:

    a. Crear y mantener la figura de coordinador nacional de seguridad digital en el Departamento Nacional de Planeación (diciembre de 2016).

    b. Bajo el liderazgo del coordinador nacional de seguridad digital, definir la instancia de máximo nivel interinstitucional e intersectorial en el Gobierno nacional para la orientación superior en temas de seguridad digital en Colombia (diciembre de 2017), diseñar un modelo dinámico de coordinación entre las múltiples partes interesadas (junio de 2017), y crear una agenda nacional de seguridad digital (diciembre de 2017).

    c. 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 Tabla 9.

ANEXOS

Anexo A: Plan de Acción y Seguimiento (PAS)

Ver archivo en Excel.

Anexo B: Análisis comparativo de estrategias y políticas de seguridad digital expedidas en 2015 en cinco países

Componente	República Checa	Malta	Irlanda	Portugal	Francia
Principios fundamentales	Protección de los derechos humanos y las libertades fundamentales y del Estado del derecho democrático. Enfoque integral de ciberseguridad basado en los principios de subsidiariedad y de cooperación. Fomento de la confianza y la cooperación entre los sectores público y privado, y la sociedad civil. Fortalecimiento de capacidades de ciberseguridad.	Estado de Derecho. Enfoque colaborativo y cooperativo entre las múltiples partes interesadas. Responsabilidad compartida. Gestión del riesgo.	Estado de Derecho. Subsidiariedad. Proporcionalidad. Gestión de riesgos.	Subsidiariedad. Complementariedad. Cooperación. Proporcionalidad. Conocimiento.	Dotar de los medios necesarios para defender sus intereses fundamentales en el ciberespacio y consolidar la seguridad digital de sus infraestructuras críticas y la seguridad de sus operadores esenciales para la economía. Desarrollar un uso del ciberespacio conforme a sus valores y en el que protegerá la vida digital de sus ciudadanos e incrementar su lucha contra la ciberdelincuencia y la asistencia a las víctimas de ciberataques. Promover desde la escuela la sensibilización sobre la seguridad digital y los comportamientos responsables en el ciberespacio. Desarrollar un ecosistema favorable a la investigación y a la innovación, hacer de la seguridad digital un
Objetivos estratégicos	Garantizar la ciberseguridad. Promover la cooperación internacional activa. Proteger las infraestructuras críticas nacionales y los sistemas importantes de información.	Combatir el cibercrímen. Fortalecer la ciberdefensa nacional. Asegurar el ciberespacio. Establecer un marco de gobernanza. Promover la cooperación nacional e internacional.	Mejorar la resiliencia y robustez de la infraestructura crítica. Trabajar con socios internacionales y organizaciones internacionales para asegurar que el ciberespacio se mantenga abierto, seguro, libre y capaz de	Promover el conocimiento, uso gratuito, seguro y eficiente del ciberespacio. Proteger los derechos fundamentales, la libertad de expresión, los datos personales y la privacidad de los ciudadanos. Fortalecer y garantizar la seguridad del ciberespacio, de las infraestructuras críticas y de los servicios nacionales	

Componente	República Checa	Malta	Irlanda	Portugal	Francia
	Promover la cooperación con el sector privado. Fomentar la investigación y desarrollo y la confianza de los consumidores. Proveer educación y desarrollo de conocimiento. Dar apoyo a las capacidades de la policía para la investigación y el enjuiciamiento respecto al cibercrímen. Adaptar el marco legal.		facilitar el desarrollo económico y social. Aumentar la conciencia de las responsabilidades de las empresas y de los particulares. Garantizar que el Estado cuenta con un marco legal y regulatorio integral y flexible para combatir el delito cibernético. Construir la capacidad en la administración pública y el sector privado a participar plenamente en la gestión de emergencias de incidentes cibernéticos.	vitales. Afirmar el ciberespacio como un lugar para el crecimiento económico y la innovación.	factor de competitividad, y fomentar el desarrollo de la economía y la promoción internacional de sus productos y servicios digitales. Ser, junto con los Estados miembros voluntarios, el motor de una soberanía digital europea y desempeñar un papel activo en la promoción de un ciberespacio seguro, estable y abierto.
Dimensiones estratégicas	-	Marco político Marco legal Gestión de Riesgos Cultura Educación	-	Estructura de la seguridad en el ciberespacio. Contrarrestar al cibercrímen. Protección del ciberespacio e infraestructuras nacionales. Educación, sensibilización y prevención. Investigación y desarrollo. Cooperación.	-
Enfoque integral diferenciando objetivos	Sí	Sí	Sí	Sí	Sí
Enfoque de gestión de riesgos	Sí	Sí	Sí	Sí	Sí

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2015.

Anexo C: Normativa nacional relacionada con asuntos de seguridad digital

Norma	Contenido
Constitución Política de Colombia	Artículos 11, 12, 13, 14, 17, 21, 22, 24, 29, 44, entre otros. Por ejemplo, Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
Ley 527 de 1999 (Comercio Electrónico)	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional (artículos 6º, 8º, 7º, 28º, 12º y 13º), la autenticación electrónica (artículo 17º), la firma electrónica simple (artículo 7º), la firma digital (artículo 28º), y la firma electrónica certificada (artículo 30º, modificado por el artículo 161 del Decreto Ley 019 de 2012).
Ley 594 de 2000 (Ley General de Archivos)	Habilita el uso de nuevas tecnologías de manera general, es posible establecer que para satisfacer los requerimientos establecidos en esta norma sea viable usar firmas electrónicas simples, certificadas y firmas digitales.
Ley 599 de 2000 (Código Penal)	Por la cual se expide el código penal colombiano.
Ley 600 de 2000 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal.
Ley 679 de 2001 (Pornografía y explotación sexual con menores)	Esta Ley contempla en el artículo 4, un sistema de autorregulación, en virtud del cual el Gobierno nacional, por intermedio del Ministerio de Comunicaciones – hoy Ministerio de Tecnologías de la Información y las Comunicaciones- , promoverá e incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y el aprovechamiento de redes globales de información, estos códigos se elaboraran con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información.
Ley 906 de 2004 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal (corregida de conformidad con el Decreto 2770 de 2004)
Ley 962 de 2005 (racionalización de trámites y procedimientos)	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1032 de 2006 (derechos de autor y conexos)	Por la cual se modifican los artículos 257, 271, 272 y 306 del código penal (artículo 271. violación a los derechos patrimoniales de autor y derechos conexos).

Norma	Contenido
Ley 1150 de 2007 (medidas para la eficiencia y la transparencia)	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública (SECOP).
Circular Externa SFC 052 de 2007	Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta Entidad.
Ley 1266 de 2008 (Habeas Data)	Contempla las disposiciones generales en relación al derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009 (Delitos Cibernéticos)	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las TIC".
Ley 1336 de 2009 (Explotación, pornografía y el turismo sexual con niños)	A través de esta ley se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Esta ley establece dos medidas para contrarrestar la explotación sexual y la pornografía infantil que se relacionan tangencialmente con las TIC, en primer lugar establece en el artículo 4 (autorregulación de café internet – códigos de conducta) que todo establecimiento abierto al público que preste servicios de internet o de café internet deberá colocar en un lugar visible un reglamento de uso público adecuado de la red, y deberá indicar que la violación a este genera la suspensión del servicio al usuario.
Ley 1341 de 2009 (Sector TIC)	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Decreto 1727 de 2009 (Habeas Data)	Se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.
Decreto 2952 de 2010 (Habeas Data)	Este Decreto reglamenta los artículos 12 y 13 de la Ley 1266 de 2008, en este sentido establece que con fundamento en el principio constitucional de solidaridad surgen obligaciones a cargo del Estado y de los ciudadanos, en virtud de las cuales cuando se presenten situaciones de fuerza mayor, es posible otorgar a las víctimas de secuestro, desaparición forzada y personas secuestradas, debido a su estado de debilidad manifiesta, un tratamiento diferenciado en la administración de su información financiera, crediticia y comercial.
Ley 1437 de 2011 (Uso de medios electrónicos Procedimiento Administrativo Electrónico)	Consagra la utilización de medios electrónicos en el procedimiento administrativo permitiendo adelantar los trámites y procedimientos administrativos por medios electrónicos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes electrónicos y sedes

Norma	Contenido
	electrónicas. Lo anterior, con el fin de que los ciudadanos interactúen por medios electrónicos con validez jurídica y probatoria.
Ley 1453 de 2011 (Estatuto de seguridad ciudadana)	Por medio de la cual se reforma el código penal, el código de procedimiento penal, el código de infancia y adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad.
Ley 1474 de 2011 (Uso de medios tecnológicos)	Esta norma permite la utilización de medios tecnológicos en los trámites y procedimientos judiciales, en las diligencias, práctica de pruebas y notificaciones de las decisiones.
Ley 1480 de 2011 (Estatuto del Consumidor - Comercio electrónico y publicidad)	Se incluye en la definición de las ventas a distancia, aquellas que se realizan a través del comercio electrónico. El artículo 26 de esta Ley, consagra que la SIC determinará las condiciones mínimas bajo las cuales operar la información pública de precios de los productos que se ofrezcan a través de cualquier medio electrónico.
Ley 1564 de 2011 (Uso de las TIC)	Permite el uso de las TIC en todas las actuaciones de la gestión y trámites de los procesos judiciales con el fin de facilitar el acceso a la justicia.
Resolución CRC 3066 de 2011	Se establece el régimen integral de protección de los derechos de los usuarios de los servicios de comunicaciones. En particular, se establece que los proveedores de servicios de comunicaciones deberán implementar procesos formales de tratamiento de incidentes de seguridad de la información propios de la gestión de seguridad del proveedor.
Resolución CRC 3067 de 2011 "Por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones"	Está Resolución establece en el artículo 2.3, que los proveedores que ofrezcan acceso a internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia del mismo.
Resolución CRC 3502 de 2011 (Neutralidad de Internet)	A través de la Resolución CRC 3502 de 2011, se establecen condiciones regulatorias relativas a la neutralidad en internet, en cumplimiento de lo establecido en el artículo 56 de la Ley 1450 de 2011 (PND 2010 – 2014). Se contempla en el artículo 3 los principios de libre elección, no discriminación, transparencia e información, que deben aplicar los proveedores que prestan el servicio de acceso a internet.
Ley 1581 de 2012 (Habeas Data)	Por la cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.
Ley 1712 de 2012 (Uso de las TIC)	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la

Norma	Contenido
	información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.
Decreto 1704 de 2012 (Interceptación legal de comunicaciones)	Este Decreto determina que la interceptación legal de comunicaciones, es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos de inteligencia. De esta manera, se determina que los proveedores que desarrollen su actividad comercial en el territorio nacional, deben implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de policía judicial cumplan, previa autorización del fiscal general de la nación, con todas las labores inherentes a la interceptación de las comunicaciones requeridas.
Decreto 2758 de 2012 (Modifica la Estructura del Misterio de Defensa)	Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del Viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente le encarga a la Dirección de seguridad pública y de infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.
Decreto Ley 019 de 2012 (Entidades de Certificación Digital)	Establece las siguientes actividades que las entidades de certificación acreditadas podrán realizar en el país, tales como emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas, emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles, y emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999, entre otras.
Resolución SIC No. 76434 de 2012 (Habeas Data)	Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países.
Decreto 2364 de 2012 (Firma electrónica)	Establece la reglamentación del artículo 7º de la Ley 527 de 1999, complementando el marco jurídico de los mecanismos de autenticación previstos en Colombia. Se definen algunas características que benefician el uso de los medios electrónicos, tales como la definición de los criterios de confiabilidad y apropiabilidad en el uso de los mecanismos de autenticación, la fijación de la relación de género y especie entre firmas electrónicas y firmas digitales, señalando las diferencias en su tratamiento probatorio, pues en el último mecanismo existe una inversión probatoria, y el uso de la firma electrónica mediante acuerdo de las múltiples partes de una relación jurídica, entre otras.
Resolución 3933 de 2013	Creó el Grupo colCERT y asignó funciones a la dependencia de la Dirección de seguridad pública y de infraestructura del Ministerio de Defensa Nacional respecto a promover el desarrollo de capacidades locales o sectoriales para la

Norma	Contenido
del Ministerio de Defensa Nacional (Crea y organiza grupos internos de trabajo)	gestión operativa de los incidentes de ciberseguridad y ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.
Decreto 1377 de 2013 (Habeas Data)	Se reglamenta parcialmente la Ley 1581 de 2012, facilitando la implementación y el cumplimiento de la Ley 1581 de 2012, reglamentando aspectos particulares relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, además consagra políticas de tratamiento de los responsables y encargados.
Ley 1621 de 2013 para la función de inteligencia y contrainteligencia en Colombia)	Esta ley expide normas para fortalecer el marco jurídico que permita a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal.
Decreto 0032 de 2013 (Creación de la Comisión Nacional Digital y de Información Estatal)	El Ministerio de Tecnologías de la Información y las Comunicaciones en cumplimiento de los lineamientos señalados en el Documento CONPES 3701, creo a través de este Decreto, la Comisión Nacional Digital y de Información Estatal cuyo objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado colombiano.
Decreto 333 de 2014 (Habeas Data)	Se reglamenta el artículo 160 del Decreto 019 de 2012), definiendo el régimen de acreditación de las entidades de certificación abierta, en desarrollo de lo que define el artículo 160 del Decreto 019 de 2012 y se deroga el Decreto 1747 de 2000, que reglamenta de manera parcial la Ley 527 de 1999, referente a las entidades de certificación digital, certificados y firmas digitales, de manera que las entidades que deseen seguir prestando los servicios de certificación digital, deberán iniciar la correspondiente acreditación, ya no ante la Superintendencia de Industria y Comercio, sino ante el Organismo de Acreditación en Colombia (ONAC).
Decreto 886 de 2014 (Registro Nacional de Base de Datos)	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al registro nacional de bases de datos. Se reglamenta la información mínima que debe contener dicho registro, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los responsables del tratamiento.
Decreto 2573 de 2014 (Gobierno en Línea)	Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto compilatorio 1070 de 2015	Por medio del cual se reglamenta la Ley estatutaria 1621 de 2013, que establece el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, para cumplir con su misión constitucional y legal. Adicionalmente, establece la reserva legal, los niveles de clasificación y el sistema para la designación de los niveles de acceso a la información y clasificación de documentos.
Decreto 1074 de 2015 (Decreto Único Reglamentario del Sector de Comercio, Industria y Turismo)	Por medio del cual se expide el Decreto único reglamentario del sector de comercio, industria y turismo, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector. Compilación de los Decretos 2364 de 2012, 333 de 2014, entre otros.

Norma	Contenido
Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC)	Por medio del cual se expide el Decreto único reglamentario del sector TIC, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector.
Circular Externa SIC 02 del 3 de noviembre de 2015	Por la cual la Superintendencia de Industria y Comercio impartió instrucciones a los responsables del tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las cámaras de comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el registro nacional de bases de datos a partir del 9 de noviembre de 2015.

Fuente: Adaptado de CRC, 2015

Anexo D: Normativa internacional relacionada con asuntos de seguridad digital

Instrumento	Materia
Convenio sobre Ciberdelincuencia del Consejo de Europa – CCC (conocido como el convenio sobre Cibercriminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004	El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas.
Resolución AG /RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos	Se establece una estrategia Integral para combatir las amenazas a la seguridad cibernética con un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética. Se estipulan tres vías de acción: i) Creación de una Red Hemisférica de CSIRT, cometido asignado al CICTE de la OEA; ii) Identificación y adopción de normas técnicas para una arquitectura segura de Internet, labor desarrollada por la Comisión Interamericana de Telecomunicaciones; y iii) Adopción o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas - REMJA.
Decisión 587 de la Comunidad Andina, adoptada el 10 de julio de 2004	Por la cual se establecen los lineamientos de la Política de Seguridad Externa Común Andina. Dentro de los objetivos de dicha política se encuentra el prevenir, combatir y erradicar las nuevas amenazas a la seguridad y cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.
Consenso en materia de ciberseguridad de la Unión Internacional de Telecomunicaciones - UIT, en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005	Busca la promoción del examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones. Las Resoluciones que emita la UIT son vinculantes para Colombia, puesto que a través de las Leyes 252 de 1995 y 873 de 2004, se aprobó la constitución de la UIT y el Convenio de la UIT, así como las enmiendas posteriores que se han realizado.
Resolución 64/25 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional". Asamblea General de las Naciones Unidas (UNGA). (2009)	La Asamblea General exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información.

Instrumento	Materia
Directiva 2006/24 de la Unión Europea	Se establece la conservación de datos en la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y fue el referente aplicado por los países miembros hasta el año 2014.
Pronunciamientos de Principios	Resoluciones UNGA: 55/63 y 56/121 sobre la lucha contra el uso delictivo de tecnologías de información; 57/239, 58/199 y 64/211 sobre la creación de una cultura mundial de seguridad cibernética y la protección de infraestructuras críticas de información; Cumbre Mundial sobre la Sociedad de la Información (CMSI), Declaración de Principios y Orden del Día de la Fase de Túnez (en particular la línea de acción C5). Estas son normas o principios generales, que no constituyen reglas y no son vinculantes, sin embargo estos actos o instrumentos jurídicos sin carácter obligatorio, son incardinados de una forma u otra, en el sistema de fuentes del Derecho Internacional (Soft Law).
Marco de trabajo de estrategias nacionales de ciberseguridad. Manual de la OTAN	LA OTAN publica en el año 2012 en colaboración con la NATO Cooperative Cyber Defence Centre of Excellence el manual para la formulación de estrategias nacional de ciberseguridad para sus países miembros.
Declaración de la Cumbre de Gales de la OTAN en 2014	Documento oficial de los resultados de la Cumbre de la OTAN celebrada en Cardiff (Gales) los días 4 y 5 de septiembre de 2014, en donde se resaltan acuerdos para abordar la ciberseguridad en los países de dicha alianza.
Declaración sobre la protección de infraestructura crítica ante las amenazas emergentes (Aprobado durante la quinta sesión plenaria, celebrada el 20 de marzo de 2015)	Declaración en donde, entre otros, la Secretaría Ejecutiva del CICTE de la OEA desarrolla un proyecto de asistencia técnica que, permita a estos la elaboración de un listado de su infraestructura crítica y su clasificación, basados en sus respectivos activos, sistemas, redes y funciones esenciales, para hacer posible la mejor evaluación de vulnerabilidades, brechas, amenazas, riesgos e interdependencia.
Declaración sobre Seguridad en las Américas de la OEA (México, 2003)	Identifica como relevantes, entre otras nuevas amenazas, el terrorismo y los ataques a la seguridad cibernética, y comprometió a los Estados miembros a desarrollar una cultura de seguridad cibernética en las Américas con la adopción de medidas de prevención eficaces para prever, enfrentar y responder a los ataques cibernéticos, cualquiera fuera su origen, luchando contra las amenazas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas.

Fuente: Adaptado de CRC, 2015

Anexo E: Estimación del impacto económico de la adopción e implementación de la política nacional de seguridad digital para Colombia

La CRC, con apoyo de la Dirección de Estudios Económicos del DNP, estimó de manera preliminar el impacto económico de la adopción e implementación de la política nacional de seguridad digital en Colombia desde el año 2015 al año 2020, mediante el uso de un Modelo de Equilibrio General Computado (MEGC) dinámico.

El MEGC dinámico de la CRC es un instrumento de simulación económica y de evaluación de impacto de medidas económicas construido para el conjunto de la economía con énfasis en el sector de comunicaciones a partir de la definición de varios escenarios. Este incluye ecuaciones definidas sobre la base de la teoría económica generalmente aceptada, interactuando con aspectos fiscales, monetarios, y de inversión, con presencia de diversos agentes económicos.

Los escenarios se identificaron a partir de la especificación de diversas variables que definen los dos contextos en los que se desenvuelve y a los que responde la economía colombiana: el internacional, reflejado en el comportamiento de los precios internacionales, y el nacional, concretado en las políticas monetarias, fiscales y regulatorias que aplica el Estado.

Los escenarios incluyeron también un conjunto de instrumentos de política específicos para el sector de Comunicaciones que el Ministerio de Tecnologías de la Información y las Comunicaciones y la CRC consideraron apropiados para el desarrollo del modelamiento. Los instrumentos a usar son, por supuesto, una decisión política, más allá del resultado de cualquier simulación realizada con el MEGC, cuyo único propósito es ofrecer una información sustentada para una mejor decisión.

Varios de estos instrumentos ya son aplicados en la economía colombiana y se incluyen en el escenario base que se describe más adelante. Tales son, por ejemplo, los precios administrados existentes en los servicios públicos e inmobiliario (los cuales son ajustados, por regla general, con la inflación del periodo anterior) y los subsidios al sector agropecuario y a la construcción de vivienda.

Escenario base

El análisis parte de un escenario base que refleja la situación económica reciente (año 2015), la de los últimos cinco años (2010, 2011, 2012, 2013 y 2014), las estadísticas base del año 2010 y unas previsiones de precios internacionales, de políticas monetaria y fiscal para los años de proyección (2015-2020) considerados plausibles. Los demás escenarios son comparados con el escenario base para identificar los cambios en las variables económicas derivados de la política o políticas aplicadas en el escenario respectivo. Los resultados se comparan en particular con relación al crecimiento del PIB nacional, valor

agregado, inflación al consumidor, inversión nacional privada y pública, y variables de empleo nacional.

A continuación, se presentan a modo de ilustración las características y los resultados del escenario base de la política nacional de seguridad digital.

Supuestos

Desde el año 2012, los precios de las materias primas han venido disminuyendo, en gran parte por la desaceleración de la economía de China, la recesión europea, y las dificultades económicas en Estados Unidos y Japón, como consecuencia de diversas circunstancias y de problemas económicos aún no resueltos derivados de la Gran recesión 2008-2009. Para los fines de la definición del escenario base, se consideró esa reducción progresiva en los precios de las materias primas y un bajo crecimiento en los precios de los bienes de capital, de las manufacturas intermedias y de consumo. Así mismo, se consideró que la inversión extrajera (petróleo, minería, portafolio y otros), al igual que la remisión de utilidades de las empresas multinacionales, disminuirán en el año 2015 y, posteriormente, se estabilizaran en los niveles alcanzados en el 2015.

En cuanto a las condiciones locales del escenario base, se supuso que la inversión colombiana en el exterior se mantendrá estable a partir del 2014, el préstamo neto privado presentará un comportamiento estable, y la tasa de distribución de utilidades de las empresas locales se mantendrá alrededor del 45,7. Por su lado, se consideró que el sector financiero continuará manteniendo un comportamiento de "competencia monopolística" como encuentra el Banco de la República.

Con relación a la política tributaria, se consideró que las tasas de los impuestos (efectivas, es decir descontando las exenciones) se mantendrían estables al nivel actual, durante todos los años de la proyección: 10% a los salarios, 25% al capital, 25% a las utilidades de las empresas, 16% al valor agregado y 1% al patrimonio (o impuesto a la riqueza). Los aranceles a las importaciones se mantendría en su nivel actual según los sectores: agricultura 4,1%, hidrocarburos 5,0%, minerales 5,0%, químicos 7,5%, manufacturas intermedias 5,3%, manufacturas de consumo 6,9% y bienes de capital 5,6%.

En cuanto al gasto fiscal, se consideró un crecimiento anual del orden de 9%, con el fin de suplir las pérdidas por inflación y un ajuste real cada año. Adicionalmente, a partir de 2014, se consideraron subsidios a la agricultura por un valor de 1,5 billones de pesos anuales, y a partir de 2013, subsidios a la construcción de vivienda por 1,1 billones de pesos. Para la inversión pública, se consideró un crecimiento anual de 10%. El modelo incorpora también en el escenario base precios administrados para los sectores de servicios públicos y servicios inmobiliarios, una práctica antigua en la economía colombiana, además de permitir modelar cambios en los cargos de acceso de la telefonía móvil.

Por el lado monetario, se supuso que el Banco de la Republica tendrá su tasa de referencia en 4% en el 2014 y la mantendrá en 4,75% para los años siguientes. Así mismo, se consideró que acumularía reservas internacionales en montos que fluctuarían entre USD 3.000 y USD 6.000 millones de dólares.

Resultados

Para el escenario base, la tasa de crecimiento promedio anual entre 2010 y 2020, del PIB que proyecta el modelo es de 4,35%. El resultado es acorde con la tendencia mostrada por la economía colombiana durante los últimos años. Vale la pena aclarar que dada la alta volatilidad de la economía internacional en los últimos años, la caída del precio del petróleo y el aumento de la tasa de cambio, este crecimiento puede ser sobreestimado por el modelo, ya que el periodo de pronóstico es bastante amplio y podría ocurrir algún choque externo, generando una alteración en la tendencia de crecimiento que hasta el momento el MEGC no tiene incorporado.

Para la inflación de precios al consumidor (IPC), el modelo proyecta una tasa promedio de 5,17%, teniendo en cuenta las presiones inflacionarias a las que está expuesta la economía nacional, superando las metas establecidas por Banco de la Republica (entre 2% y 3% anual). Es importante mencionar que una inflación de alrededor del 5% no representa una amenaza latente para la economía colombiana.

En el escenario base, la inversión pública proyectada promedio para el periodo 2010-2020, como porcentaje del PIB es 3,81% y la inversión privada de 15,30%, sumando un total nacional del 23,48% promedio en el periodo. Dicha tasa representa un incremento respecto a la tasa registrada para el año base (2010) que fue de 23,17% del PIB. Esta expansión se explica fundamentalmente por los crecimientos registrados de la inversión pública en los años 2011 y 2012 y el supuesto de un incremento anual de 10% en los años siguientes hasta el 2020. En el año 2010, la inversión pública representó 2,60% del PIB.

En términos de ocupación, el modelo proyecta un promedio anual entre 2010 y 2020 de 25.255.330 personas; de estos 8.879.240 son asalariados y 16.376,090 son no asalariados. En el año 2010, los registros del DANE indican que la ocupación total era de 20.350.818, de los cuales 8.794.140 eran asalariados y 11.556.678 no asalariados.

Escenario: Colombia implementando la gestión de riesgos de seguridad digital

El escenario se refiere a la implementación de la gestión de riesgos para la seguridad digital por parte de las múltiples partes interesadas en Colombia. El escenario contempla las políticas aplicadas durante 2015 y una proyección hipotética de las mismas hasta el año 2020. Este escenario propone un crecimiento de la inversión y gasto del gobierno equivalente a un punto porcentual a partir del 2016. Adicionalmente, se contempla un aumento en la

competencia bancaria, mediante la reducción de la variable denominada *ganancias monopólicas* en 0,50 puntos porcentuales a partir del 2016, y por último un incremento en la inversión privada de la misma magnitud del incremento del Gobierno nacional: un punto porcentual a partir del 2016.

Supuestos

Para simular el impacto de la política nacional propuesta, es necesario tener presentes los posibles actores que serían afectados por la misma. A continuación se presenta una breve descripción de los sectores y su posible afectación, tanto directa como indirecta.

- El sector comercial sería el primer afectado (positivamente) por la política nacional de seguridad digital. El efecto se vería representado por la disminución en los costos de transacción en lo que se considera comercio electrónico. Al tener mayor seguridad, las personas podrían estar exentas de pagar primas de seguro (posiblemente incluidas en el precio del bien o adquiridas adicionalmente por el cliente) por los pedidos que realizan. Este efecto va a ser modelado mediante una disminución en los costos de los servicios, transferidos a los precios de los bienes (dada la construcción teórica de los precios en el MEGC). Ahora bien, este efecto no genera necesariamente un aumento de la demanda agregada, ya que es posible que exista un efecto sustitución entre el comercio tradicional (almacenes físicos, tiendas, centros comerciales, etc.) y el mercado virtual, en el cual simplemente el agente prefiere hacer las transferencias virtualmente y no presencialmente como se ha venido manejando.
- El segundo efecto en orden de magnitud sería sobre el sector bancario. Al tener una mayor seguridad sobre las transacciones bancarias virtuales, se posibilita la disminución de costos de transacción, tanto para el banco como para el agente que realiza la transacción. Estos menores costos podrían incentivar la competencia bancaria (vale la pena aclarar que este supuesto es válido para países que tengan altos niveles de bancarización). El modelamiento de este fenómeno se verá reflejado en el modelo mediante la reducción de la variable *competencia monopolística* bancaria.
- El sector Gobierno sería otro de los agentes directamente implicados. En su misión de manejo web (Gobierno en línea) y sus líneas de atención al cliente, es de vital importancia que exista seguridad de los datos personales de los usuarios del servicio. El Gobierno nacional debe realizar un gasto adicional en la protección de la infraestructura crítica cibernética nacional, mediante la implementación de programas efectivos que permitan la gestión de riesgos óptima en temas de seguridad digital. Se debe tener en cuenta que el efecto sobre el crecimiento económico podría ser neutral, ya que este tipo de políticas generan inversión y gasto público, pero son enfocadas a mitigar riesgos y por ende no se ve reflejado su beneficio en la economía, a menos de

que se vea materializado el riesgo. El modelamiento de este efecto será visto mediante incrementos en la inversión pública y gasto del Gobierno nacional, es posible que esto genere un efecto de multiplicador del gasto transmitido al crecimiento económico por medio del aumento del consumo. Por otro lado, se debe tener en cuenta que el incremento de la inversión pública, conlleva un efecto *crowding out*[42] de la inversión privada y podría opacar el efecto inicial.

- El último grupo de agentes implicados son las empresas. En un entorno internacional enfocado en el desarrollo industrial, se debe tener en cuenta el factor de investigación y desarrollo e innovación como motor del crecimiento económico. Mediante innovación y creación de nuevas tecnologías, las empresas aseguran permanecer en el mercado con mejores productos o servicios para sus clientes. Gran parte de los desarrollos realizados por las mismas son protegidos por las leyes de propiedad intelectual y los acuerdos de confidencialidad de las empresas. Mediante la gestión de riesgos de seguridad digital, es posible que se incentive la inversión en innovación y desarrollo, al haber una mayor protección a la propiedad intelectual que puede evitar el plagio o copia de los desarrollos realizados por las empresas. Esto se refleja en un aumento en el crecimiento económico. El modelamiento de este efecto será a través de un aumento en la inversión privada.

Se estimaron los dos escenarios posibles con cada uno de los agentes, y se procede a realizar las comparaciones relativas de los mismos.

Resultados

Los resultados del escenario muestran mayores tasas de crecimiento del PIB nacional, pasando de 4,35% en el escenario base a 4,44%, un incremento de 0,09 puntos porcentuales en términos de crecimiento económico.

En cuanto a la inflación de precios al consumidor (IPC), se concluye que no existe cambio alguno entre lo esperado para el escenario base (5,17%) y lo resultante en el escenario bajo la gestión de riesgos para la seguridad digital. Se debe tener en cuenta que el modelo presenta una tasa de inflación superior a la establecida por el Banco de la Republica (entre 2% y 3% anual).

En términos de ocupación, la política nacional de seguridad digital en Colombia habría creado 307.222 puestos de trabajo adicionales en la economía nacional. Esta cifra debe tomarse con cautela, ya que el crecimiento del empleo en los últimos años fue significativo por lo que al ser un promedio de ese periodo, se puede pensar que esté sobre estimado. El

[42] Efecto desplazamiento. Es una situación en la que la capacidad de inversión de las empresas se reduce debido a la deuda pública.

mayor gasto público y la mayor inversión pública que el plan implica, son los responsables del mayor crecimiento y ocupación.

Aspectos relevantes respecto al ejercicio de valoración del impacto económico de la implementación de la política nacional.

La política nacional de seguridad digital tiene un impacto positivo sobre muchos sectores de la economía que no son medibles, o que por el diseño de la política, se ven diluidos en los diferentes canales de trasmisión de la misma. Por ende evaluar esta política teniendo en cuenta solo los datos macroeconómicos no sería prudente.

Aunque el país ha tenido presiones inflacionarias por temas relacionados con tasa de cambio y fenómenos naturales que impactan directamente a la economía, el tener una política nacional de seguridad digital parece no tener efecto alguno sobre la canasta familiar.

Por último vale la pena destacar, que todos los resultados aquí contenidos son válidos mientras se cumplan los supuestos anteriormente expuestos. Con el cambio de cualquier supuesto los resultados del modelo podrían cambiar drásticamente.

GLOSARIO

Bajo el enfoque de la política nacional de seguridad digital

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Entorno digital abierto: entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica.

Incidente digital: evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Resiliencia: es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido

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.

Desde la perspectiva de la seguridad nacional

Cibercrímen (delito cibernético): conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio.

Ciberlavado: es el uso del Ciberespacio, en cualquiera de sus formas, para dar apariencia de legalidad a bienes obtenidos ilícitamente o para ocultar dicha ilicitud ante las autoridades.

Ciberseguridad: es 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 buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

Desde la perspectiva de la defensa nacional

Amenaza cibernética: aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

Ataque cibernético: acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio.

Ciberdefensa: as el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales.

Ciberespionaje: es el acto o práctica de obtener secretos sin el permiso del dueño de la información (personal, sensible, propietaria o de naturaleza clasificada) para ventaja personal, económica, política o militar en el Ciberespacio, a través del uso de técnicas malintencionadas.

Ciberterrorismo: es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo como consecuencia una violación a la voluntad de las personas.

BIBLIOGRAFÍA

BID&OEA. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016. Recuperado de: https://publications.iadb.org/handle/11319/7449?locale-attribute=en&locale-attribute=pt&locale-attribute=es&

COLOMBIA TIC. (2015). *Boletín trimestral de las TIC – Cifras Tercer Trimestre de 2015*.

Departamento Nacional de Planeación. (2011). *Lineamientos de política para Ciberseguridad y Ciberdefensa*. Documento CONPES 3701, Bogotá D.C., Colombia: DNP. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación. (2014). Plan Nacional de Desarrollo 2014-2018, *Todos por un Nuevo País,* Bogotá D.C., Colombia: DNP. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Prensa/Bases%20PND%202014-2018F.pdf

EURACTIV. (2015). *How digital is the EU in 2015?.* Recuperado de: http://www.euractiv.com/sections/digital/infographic-how-digital-eu-2015-312828

INTEL SECURITY. (2015a). *McAfee Labs Report 2016 Threats Predictions*. Recuperado de: www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

INTEL SECURITY. (2015b). McAfee Labs Threats Report November 2015. Recuperado de: http://www.mcafee.com/de/resources/reports/rp-quarterly-threats-nov-2015.pdf

INTEL SECURITY. (2015c). *Critical Infrastructure Readiness Report - Holding the Line Against Cyberthreats*. McAfee Labs http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf

ITI. (2011). *Cybersecurity Principles for Industry and Government*. Recuperado de: https://www.itic.org/dotAsset/0e3b41c2-587a-48a8-b376-9cb493be36ec.pdf

ITI (2012). *Recommended Government Approaches to Cybersecurity*. Recuperado de: https://www.itic.org/dotAsset/6235994d-6f2a-428d-bd11-66d84a9cf2e9.pdf

Katz, Raúl. (2015a). *El Ecosistema y la Economía Digital en América Latina*. Telefónica, CEPAL, CAF, Cet.la y Ariel. Recuperado de: http://repositorio.cepal.org/bitstream/11362/38916/1/ecosistema_digital_AL.pdf

Katz, Raúl; Callorda, Fernando (2015b). *Impacto de arreglos institucionales en la digitalización y el desarrollo económico de América Latina*. Proceedings of the 9th CPR LATAM Conference, Cancun, Mexico, July 14-15st, 2015. Recuperado de: http://www.teleadvs.com/wp-content/uploads/Katz-Callorda-2015-version-final.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015a). *Informe de gestión al Congreso de la República de Colombia 2015*.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015b). *Panorama TIC – Comportamiento macroeconómico del sector TIC en Colombia*. Diciembre de 2015. Recuperado de: http://colombiatic.mintic.gov.co/602/articles-14305_panoranatic.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015c). *Estudio sobre el estado de apropiación de la seguridad de la información en entidades del Estado*.

OCDE. (2015a). *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity* in Digital Security Risk Management for Economic and Social Prosperity, OCDE Recommendation and Companion Document, OCDE Publishing, Paris, Francia. Recuperado de: http://www.OCDE.org/sti/ieconomy/digital-security-risk-management.pdf

OCDE. (2015b). OCDE Digital Economy Outlook 2015, OCDE Publishing, Paris, Francia. Recuperado de: http://www.keepeek.com/Digital-Asset-Management/OCDE/science-and-technology/OCDE-digital-economy-outlook-2015_9789264232440-en#page1

OEA. (2014a). *Recomendaciones y Observaciones - Misión Internacional de Asistencia Técnica en Seguridad Cibernética Colombia – Abril de 2014*, Publicaciones de la OEA, Washington D.C., Estados Unidos de América.

OEA. (2014b). *Tendencias de Seguridad Cibernética en América Latina y el Caribe*. Recuperado de: https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

OEA. (2015). *Recomendaciones y Observaciones - Misión Internacional de Asistencia Técnica en Seguridad Cibernética Colombia – Agosto de 2015*, Publicaciones de la OEA, Washington D.C., Estados Unidos de América.

OTAN. (2012). *National Cyber Security Framework Manual*. Publicación para la OTAN. Recuperado de: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

SFC. (2015). *Informe de Operaciones – Primer Semestre de 2015*. Delegatura para Riesgos Operativos. Recuperado de:

https://www.superfinanciera.gov.co/descargas?com=institucional&name=pubFile1014571&downloadname=informetransacciones0615.docx

SYMANTEC. (2015). *Internet Security Threat Report – ISTR 20*. Volumen 20 de abril de 2015. Recuperado de:

https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

Trend Micro Incorporated. (2015). *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*. Reporte preparado para la OEA. Recuperado de: https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

UIT. (2011). *ITU National Cibersecurity Strategy Guide*. Recuperado de: http://www.itu.int/ITU-D/cyb/cybersecurity/docs//ITUNationalCybersecurityStrategyGuide.pdf

UIT. (2015). Measuring the Information Society Report 2015. Recuperado de: http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf

VERIZON. (2015). 2015 Data Breach Investigations Report. Recuperado de: http://www.verizonenterprise.com/DBIR/2015/