# Documento CONPES

0000

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

## POLITICA NACIONAL DE SEGURIDAD DIGITAL



Ministerio de Tecnologías de la Información y las Comunicaciones
Ministerio de Defensa Nacional
Ministerio de Justicia y del Derecho
Ministerio de Relaciones Exteriores
Ministerio de Comercio, Industria y Turismo
Ministerio del Interior
Ministerio de Hacienda y Crédito Público
Ministerio de Ambiente y Desarrollo Sostenible
Ministerio de Agricultura y Desarrollo Rural
Ministerio de Educación Nacional
Ministerio de Salud y de la Protección Social
Ministerio de Trabajo
Ministerio de Minas y Energía
Ministerio de Cultura
Ministerio de Transporte
Ministerio de Vivienda, Ciudad y Territorio
Departamento Nacional de Planeación
Departamento Administrativo de la Presidencia
Departamento Administrativo de la Función Pública
Departamento Administrativo Nacional de Estadística
Departamento Administrativo Nacional de la Economía Solidaria

Borrador 2 – 22/01/2016

Bogotá, D.C., fecha de aprobación

## 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

**Tomás González Estrada**
Ministro de Minas y Energía

**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**
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 y
Secretario Técnico del CONPES

**Manuel Fernando Castro Quiroz**
Subdirector Territorial y
de Inversión Pública

**Resumen ejecutivo**

El crecimiento del uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, así como el incremento de los servicios disponibles en línea y la creciente participación de la sociedad en actividades económicas y sociales en el entorno digital han transformado la vida de todos y cada uno de los Colombianos, sin embargo el uso del entorno digital acarrea riesgos inherentes de seguridad digital que deben ser gestionados. En tan sólo un día (7 de enero de 2016), la empresa de servicios de consultoría para la respuesta a incidentes Intel Security Foundstone monitoreó un total de 8.128 incidentes de seguridad digital en Colombia.

Como resultado de la expedición del documento CONPES 3701 del año 2011, *Lineamientos de Política para Ciberseguridad y Ciberdefensa*, se implementó en el país una institucionalidad que ha adelantado sus funciones y actividades de manera eficiente, en cabeza del Ministerio de Defensa Nacional. Si bien este esfuerzo ha permitido un posicionamiento importante a nivel internacional en torno al tema, se considera fundamental robustecer el liderazgo del Gobierno nacional y construir una nueva visión general clara bajo un enfoque integral, de acuerdo con las mejores prácticas internacionales para abordar los riesgos de seguridad digital. Esta situación genera que los lineamientos de política a la fecha vigentes deban ser modificados.

El presente documento CONPES plantea una Política Nacional de Seguridad Digital que articula una visión general clara, soportada por el alto nivel del Gobierno, bajo un modelo institucional eficiente y de vinculación integral de todos y cada uno de los actores de interés, siendo éstos el mismo Gobierno nacional, las organizaciones públicas y privadas, la academia y la sociedad civil. Esta política claramente distingue los objetivos de prosperidad económica y social con los objetivos de defensa del país y de lucha contra el crimen y la delincuencia en el entorno digital, y se centra en la implementación de un conjunto de principios fundamentales, adelantando un conjunto de acciones específicas bajo unas dimensiones estratégicas, en torno a la gestión de riesgos de seguridad digital.

Con respecto al objetivo de prosperidad económica y social, esta política aborda el riesgo de seguridad digital como un reto económico y social, creando condiciones para que todos los actores de interés gestionen el riesgo de seguridad digital en sus actividades económicas y sociales, fomentando la confianza en el entorno digital como medio para alcanzar los objetivos tanto del Plan Nacional de Desarrollo 2014-2018 "*Todos por un nuevo país – Paz, Equidad y Educación*" como del Plan Vive Digital 2014-2018. Para poner en marcha esta política, se ha construido un plan de acción con una inversión total de $xxxx.

Como resultados esperados de la adopción e implementación de la Política Nacional de Seguridad Digital, se espera que Colombia: i) fortalezca la capacidad institucional,

normativa, administrativa y de gestión con el fin de abordar los temas de seguridad digital desde el más alto nivel, concientizando y capacitando a todos los actores de interés, ii) construya una estrategia nacional de seguridad digital que genere confianza y fomente el uso del entorno digital, en línea con sus valores fundamentales, y desarrolle un modelo de cooperación eficiente involucrando a todos los actores de interés en el marco de la gestión de riesgos de seguridad digital, con el objetivo de maximizar los beneficios económicos y sociales en todos los sectores económicos, iii) proteja los derechos fundamentales y las actividades económicas y sociales que realicen sus ciudadanos en el entorno digital, incremente el combate al crimen y la delincuencia en el entorno digital e implemente mecanismos de asistencia a víctimas de delitos en ese entorno, iv) asegure la defensa de sus intereses fundamentales y refuerce la seguridad digital de sus Infraestructuras Críticas Nacionales con un enfoque de gestión de riesgos, y v) participe activamente a nivel nacional e internacional en la promoción de un entorno digital abierto, estable y confiable, y en la cooperación, colaboración y asistencia respecto de la gestión de riesgos de seguridad digital.

Finalmente, se estima que la implementación de la Política Nacional de Seguridad Digital al año 2020 impactaría positivamente la economía de Colombia, generándose durante los años 2016 a 2020 aproximadamente 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:

**Palabras clave:** Seguridad Digital, Ciberdefensa, Ciberseguridad, Gestión de Riegos, Entorno Digital, Economía Digital, Prosperidad Económica y Social, Amenazas Informáticas, Capacidades, Coordinación, Fortalecimiento, Liderazgo, Infraestructura Crítica, Ciberespacio, Criptología, Diplomacia.

TABLA DE CONTENIDO

PÁGINA

# ÍNDICE DE TABLAS

PÁGINA

## ÍNDICE DE FIGURAS

PÁGINA

## SIGLAS Y ABREVIACIONES

| | |
|---|---|
| CAI VIRTUAL: | Comando de Acción Inmediata virtual de la Policía Nacional de Colombia |
| CCOC: | Comando Conjunto Cibernético del CGFM de Colombia |
| CCP: | Centro Cibernético Policial de la Policía Nacional de Colombia |
| CGFM: | Comando General de las Fuerzas Militares de Colombia |
| CICTE: | Comité Interamericano Contra el Terrorismo |
| 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 Incidencias de Seguridad (en inglés, Computer Security Incident Response Team) |
| DANE: | Departamento Administrativo Nacional de Estadística de Colombia |
| DIJIN: | Dirección de Investigación Criminal de Colombia |
| DNP: | Departamento Nacional de Planeación de Colombia |
| EUROPOL: | Oficina Europea de Policía |
| IC: | Infraestructura Crítica |
| INTERPOL: | Organización Internacional de Policía Criminal |
| MEGC: | Modelo de Equilibrio General Computable |
| MINISTERIO TIC: | Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia |
| OCDE: | Organización para la Cooperación y Desarrollo Económico |
| OEA: | Organización de Estados Americanos |
| OTAN: | Organización del Tratado del Atlántico Norte |
| PAS: | Plan de Acción y Seguimiento |
| PIB: | Producto Interno Bruto |
| TIC: | Tecnologías de la Información y las Comunicaciones |
| UIT: | Unión Internacional de las Comunicaciones |

# 1. INTRODUCCIÓN

El crecimiento del uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado por el aumento de 2,2 millones de conexiones a Internet en 2010 a 12,2 millones en 2015[1], por la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica[2] y el incremento en la oferta de servicios disponibles en línea[3] evidencian un aumento significativo en la participación digital de los ciudadanos lo que, a su vez, se traduce en la existencia de una vida digital para los Colombianos.

El uso masivo de las TIC para adelantar cualquier actividad socioeconómica ha generado el desarrollo de una economía digital creciente en el país, generando así la necesidad de establecer mecanismos para garantizar la seguridad de los individuos y sus actividades en el entorno digital, al corto, mediano y largo plazo. Por ejemplo, los incidentes de seguridad digital en plataformas tecnológicas de las entidades del sector defensa gestionados por el CCOC de Colombia aumentaron un 73% entre el 2014 y el 2015, mientras que el CCP del país ha realizado en promedio 330 capturas al año durante 2014 y 2015, lo que muestra una relación fuerte entre el crecimiento de esta economía y el aumento de los riesgos e incertidumbres[4] a los que están expuestas las personas en el entorno digital.

El desarrollo de una economía digital sólida, que contribuya positivamente a la generación de prosperidad económica y social al país, requiere la construcción de un entorno digital abierto y, al mismo tiempo, seguro y confiable, acorde con el aumento y dinamismo



[1] Según COLOMBIATIC (2015), se refiere a conexiones de banda ancha (Vive Digital) con corte a 30 de septiembre de 2015. La meta establecida en el Plan Nacional de Desarrollo 2014 – 2018, para el año 2018 es de 27 millones de conexiones a Internet.

[2] Según la SFC (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).

[3] Según el Programa Gobierno en Línea del MINISTERIO TIC, 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. Igual situación sucedió con las empresas Colombianas pasando del 24% en 2009 al 81% en 2014 (http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7654.html). Adicionalmente, el Portal del Estado Colombiano cuenta en 2015 con 1.038 trámites en línea (http://vive.gobiernoenlinea.gov.co/)

[4] Según Intel Security (2014), el costo estimado de la actividad maliciosa en el entorno digital mundial equivale entre un 0,4% y un 1,3% del PIB global. Este costo para Colombia fue aproximadamente del 0,14% del PIB en 2014.

de las actividades digitales de los individuos. Para ello, se debe contar con una visión integral y clara, respecto a la seguridad digital y a la gestión de los riesgos asociados a las amenazas e incidentes, que puedan atentar contra la integridad de los ciudadanos, el Estado Social de Derecho, el ejercicio de los derechos fundamentales, la seguridad y la defensa nacional, la soberanía y, por tanto, contra la prosperidad económica y social del país.

Así, se genera la necesidad de establecer nuevos lineamientos de política y directrices de seguridad digital, teniendo en cuenta componentes como la gobernanza, la educación, la regulación, la cooperación, la investigación y desarrollo, la innovación, la seguridad y defensa de infraestructuras críticas, la protección de la soberanía, entre otros, y enfocados en la ciudadanía, la sociedad en general, las Fuerzas Militares y los sectores público y privado, para que el país pueda contar con una estructura social y económica, que facilite el logro de los fines del Estado.

Teniendo en cuenta la problemática mencionada anteriormente, y las necesidades asociadas a la misma, en el presente documento se describen los lineamientos para el desarrollo de la Política Nacional de Seguridad Digital, la cual pretende lograr que el Gobierno Nacional, las organizaciones públicas y privadas, la academia y la sociedad civil en Colombia, hagan un uso masivo y responsable de un entorno digital abierto, seguro y confiable, a través del fortalecimiento de sus capacidades para identificar, gestionar y mitigar los riesgos asociados a las actividades digitales.

Para el desarrollo de la Política Nacional de Seguridad Digital se establecen unos principios fundamentales, que deben ser inquebrantables, y unas dimensiones y objetivos estratégicos que, mapeados, resultan en un conjunto de metas y acciones concretas que materializan dicha política (ver sección 5).

Para la elaboración de este documento, se tuvo en cuenta, principalmente, los siguientes insumos:

- Recomendaciones expedidas en el mes de septiembre de 2015, por la Organización para la Cooperación y Desarrollo Económico (OCDE), respecto a la gestión del riesgo de la seguridad digital.
- Recomendaciones concertadas en las misiones de asistencia técnica internacional y expedidas en los meses de abril de 2014 y de julio de 2015, las cuales fueron auspiciadas por el Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), con expertos de los gobiernos de Canadá, España, Estados Unidos de América, Estonia, Corea del Sur, Israel, Reino Unido, República Dominicana y Uruguay, así como representantes de organizaciones internacionales como el Foro Económico Mundial, la OCDE, la OTAN y la INTERPOL.

- Declaraciones y documentos oficiales de la Organización del Tratado del Atlántico Norte (OTAN) respecto de las buenas prácticas en el diseño de estrategias nacionales de seguridad digital.
- Recomendaciones provistas en 2014 y 2015, por expertos nacionales convocados por los Ministerios de Defensa, de Justicia y del Derecho y de Tecnologías de la Información de las Comunicaciones.
- Recomendaciones originadas de mesas de trabajo en 2014 y 2015, ampliadas con actores clave del sector público, sector privado, organizaciones de la sociedad civil, academia, industria del sector TIC y empresas especializadas en seguridad digital en Colombia.
- Recomendaciones originadas de mesas de trabajo entre el Departamento Nacional de Planeación, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional y otras entidades relacionadas con la seguridad digital en Colombia, así como con otros actores de interés, durante los meses comprendidos entre noviembre de 2015 y febrero de 2016.

El presente documento está organizado de la siguiente manera, siendo esta sección la introducción. La segunda sección describe los antecedentes, la descripción y dimensionamiento de la problemática actual en torno a la seguridad digital, lo cual permite establecer la justificación. La tercera sección contiene el marco conceptual, mientras que la cuarta presenta el diagnóstico de la problemática identificada. La quinta sección describe la Política Nacional de Seguridad Digital para Colombia, describiendo los principios fundamentales, las dimensiones estratégicas, los objetivos estratégicos y las principales metas con las acciones para alcanzar el objetivo central. De igual manera, en esta sección se presenta el calendario de seguimiento a la implementación de esta política y el esquema para su financiamiento. Por su parte, en la sexta sección se presenta una serie de recomendaciones para la implementación de la política. Finalmente, de la sección séptima a la novena se presentan el glosario, la bibliografía empleada y los anexos, que incluye el Plan de Acción y Seguimiento (PAS) detallado.

## 2. ANTECEDENTES Y JUSTIFICACIÓN

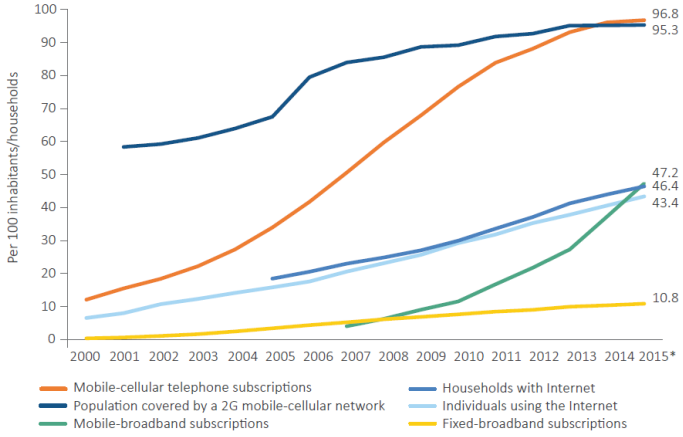
Esta sección presenta los panoramas internacional y nacional sobre las tendencias en el uso de las TIC como base para cualquier actividad socioeconómica, la dinámica consecuente que han tenido las incertidumbres en la seguridad digital durante los últimos años, y la importancia que estos aspectos tienen para el desarrollo de una economía digital. Así mismo, se presentan también consideraciones para la formulación de la Política Nacional de Seguridad Digital.

- **Panorama internacional**

La rápida evolución y adopción de las tecnologías para cualquier actividad socioeconómica, el creciente uso de las mismas por todos los niveles socioeconómicos, la expansión de las redes de telecomunicaciones, y el fenómeno de convergencia en la prestación de servicios de comunicaciones, han marcado la dinámica de este sector a nivel internacional durante los últimos años.

La Figura 2.1 presenta la evolución de los indicadores globales sobre servicios TIC. Para cada uno de estos se aprecia una evolución creciente a lo largo del tiempo, mostrando que los servicios TIC hacen parte cada día de más personas. Según UIT (2015), se ha presentado un fuerte crecimiento en la penetración de la banda ancha móvil, pasando de 12,6 suscriptores por cada cien habitantes en 2010, a un estimado de 47,2 en 2015, lo que refleja la mayor oferta de este tipo de servicios, una consecuente caída de precios, permitiendo el acceso a más personas, y la creciente masificación y uso de los dispositivos inteligentes (teléfonos y tabletas). Los individuos usando Internet y los hogares con acceso a Internet han mantenido sus tasas de crecimiento anual estables a nivel mundial. Se pasó de 29,2 individuos usando Internet por cada cien en 2010 a un estimado de 43,4 en 2015, y de 29,9 hogares con acceso a Internet por cada cien a un estimado de 46,6 en 2015.

**Figura 2.1. Desarrollo global de los indicadores de servicios TIC**




Fuente: UIT (2015)

Así mismo, las tendencias internacionales muestran que el entorno digital es dinámico y crece continuamente. En la Tabla 2.1 se muestran las proyecciones de este crecimiento a nivel global. Se estima que en los próximos cinco años, los usuarios de banda ancha móvil crecerán un 33%, los terminales conectados a Internet un 49%, los datos generados un 400%, el tráfico en las redes un 132%, los dispositivos de Internet de las cosas un 1200% y el mercado de la nube pública un 63%, aspectos que evidencian la creciente relación entre las actividades socioeconómicas y el entorno digital.

Tabla 2.1. 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 billones | 24,4 billones | 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 * | 1200% |
| Tamaño del mercado de la nube pública global | USD$97 mil millones | USD$159 mil millones | 63% |

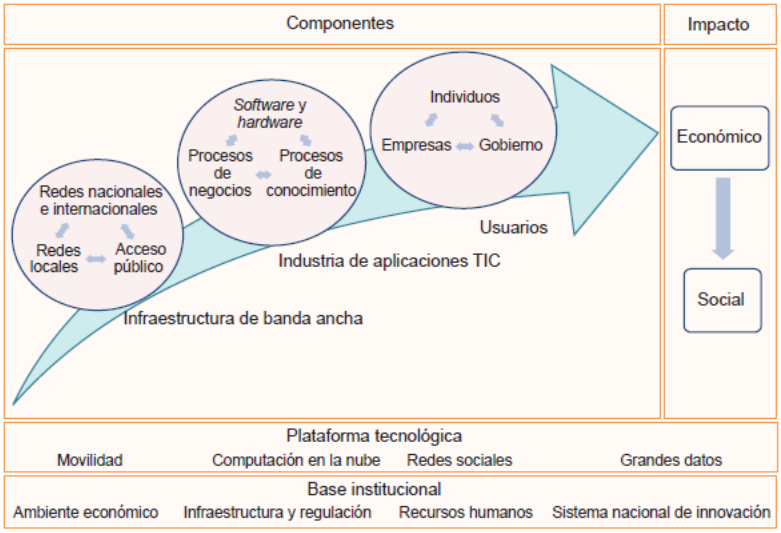
Nota: * a 2018.

Fuente: Adaptado de Intel Security Labs (2015a)

Como se ha descrito hasta el momento, a nivel global las TIC se han convertido en un factor importante en casi todos los aspectos de la vida económica y social de los individuos, proporcionando canales para la educación, la productividad laboral, la interacción social, el desarrollo de negocios más incluyentes, la democracia, las transacciones financieras, los servicios públicos al ciudadano, la seguridad y la defensa nacional, y otras interfaces entre todos los actores de interés en el entorno digital.

Según CEPAL (2014), se ha consolidado una economía basada en tecnologías (*economía digital*), la cual es un facilitador 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. La Figura 2.2 presenta un modelo de ecosistema de economía digital con tres componentes principales: la infraestructura de redes de banda ancha, la industria de aplicaciones TIC y los usuarios finales, y con unas plataformas habilitadoras y una base institucional.

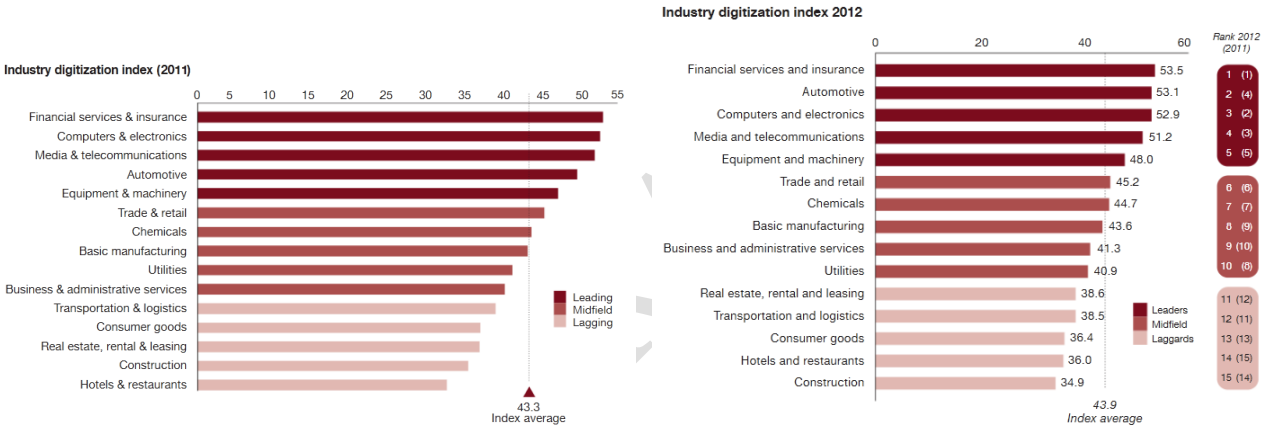
Figura 2.2. Ecosistema de Economía Digital




Fuente: CEPAL (2014)

Es ampliamente aceptado que la evolución y maduración del ecosistema de la economía digital genera impactos positivos en todos los ámbitos económico y social de la sociedad y en todos los sectores de la economía. Es así como se ha generado un proceso de digitalización a escala global, generándose así beneficios económicos para las industrias y las empresas que han estado a la vanguardia de dichas tendencias, logrando un mayor conocimiento de sus clientes y alcanzando mayor productividad y creación de nuevos modelos de negocio. PwC (2011) diseñó un índice de digitalización de industrias a partir del cual identifica industrias líderes en el proceso de digitalización como la industria de servicios financieros y seguros, la industria automotriz, la industria de computadoras y equipos electrónicos, y la industria de medios y telecomunicaciones. De igual manera, concluye que las industrias líderes en la digitalización están avanzando rápidamente, mientras que el progreso entre muchos de los rezagados se mantiene relativamente lento.

**Figura 2.3. Índice de digitalización de industrias en 2011 y 2012**

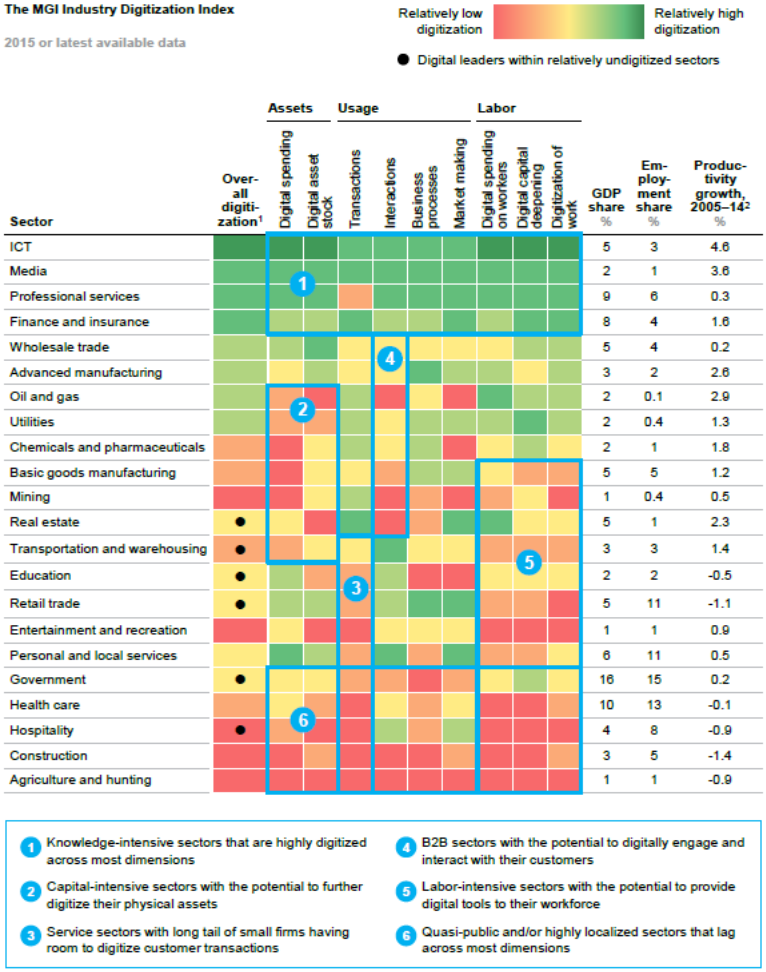



Fuente: PwC (2011) y PwC (2012)

McKinsey Global Institute (2015) también diseñó el *Índice de Digitalización de Industrias* en los Estados Unidos en donde se examinan todos los sectores en la economía a través de la lente de activos digitales, el uso digital y trabajadores digitales. El índice muestra 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, y en correspondencia con las mediciones en PwC (2011) y PwC (2012), los sectores de la economía más altamente digitalizados son los medios de comunicación, los servicios profesionales, y los servicios financieros. El índice también pone de relieve donde hay espacio para el crecimiento de las capacidades digitales. Los servicios públicos, la minería y la manufactura, por ejemplo, se encuentran en las primeras etapas de la digitalización y podrían estar a la vanguardia de la próxima ola de digitalización. Adicionalmente, las industrias intensivas en capital de trabajo como el comercio minorista y la atención de la salud están expandiendo el uso digital, pero una parte considerable de sus grandes fuerzas laborales no utilizan la tecnología ampliamente. Industrias que dependen

intensamente de mano de obra y localizada, como la construcción, el entretenimiento y la agricultura, tienden a estar menos digitalizadas.

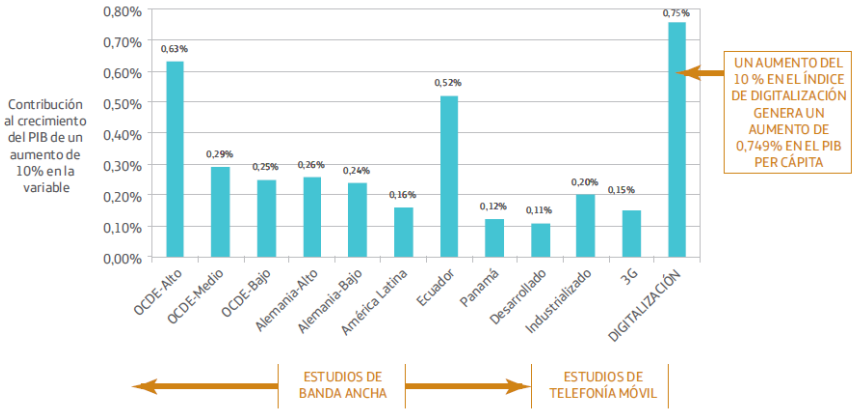
Figura 2.4. Índice de digitalización de industrias en Estados Unidos en 2015




Fuente: McKinsey (2015)

En este proceso de digitalización, el Internet es considerado como una plataforma sobre la cual se soporta cada sector de la economía y es un eje impulsor para alcanzar ganancias en productividad, competitividad y crecimiento económico. Katz (2015) concluye que tanto la digitalización de un país como el aumento en la penetración de las TIC como la banda ancha o la telefonía móvil contribuyen positivamente al crecimiento del PIB de los países. Por ejemplo, un incremento anual en 10% en la penetración de banda ancha en un país medio de la OCDE contribuiría al crecimiento anual del PIB del país en un 0,29%, o un incremento del 10% del índice de digitalización de un país generaría un aumento de 0,75% en su PIB per cápita.

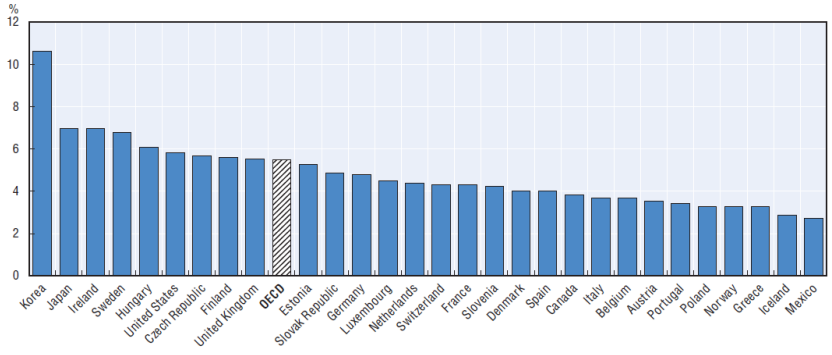
Figura 2.5. Impacto económico comparado de la digitalización de un país y de la penetración de la banda ancha y de la telefonía móvil




Fuente: Katz (2015a)

Adicionalmente, la participación de las TIC en el valor agregado total de la economía es significativo y se ha mantenido estable a nivel global. En la Figura 2.6, OCDE (2015b) estimó que el sector TIC representó el 5,5% del valor agregado total de los países de la OCDE (es decir, alrededor de USD$ 2,4 billones de dólares) en 2013. Este porcentaje muestra grandes variaciones entre los países, que van desde el 10,7% del valor agregado en Corea a menos del 3% en Islandia y México.

Figura 2.6. Participación del sector TIC en el valor agregado total en países OCDE en 2013

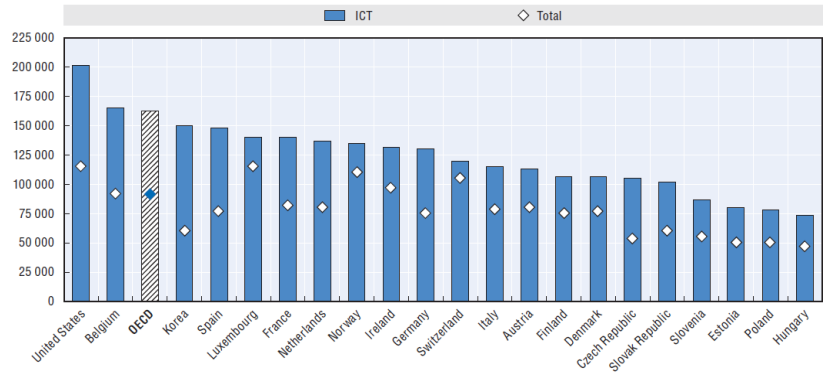



Fuente: OCDE (2015b)

Igualmente, OCDE (2015b) estimó que la productividad laboral (valor agregado por persona empleada) en el sector TIC para los países de la OCDE fue aproximadamente de

USD$ 162.000 PPP[5], siendo ésta un 79% más alta que la del resto de la economía. La Figura 2.7 presenta las estimaciones de productividad laboral para dicho grupo de países en donde se aprecia que la misma varía de un valor de USD$ 200.000 PPP en Estados Unidos a USD$ 74.000 PPP en Hungría.

**Figura 2.7. Productividad laboral en el sector TIC y en la economía en países OCDE en 2013**




Fuente: OCDE (2015b)

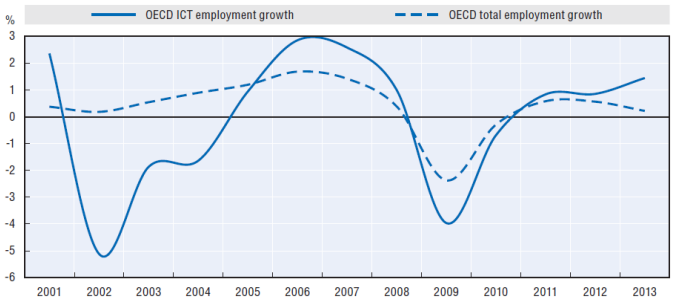
El empleo en el sector de las TIC representa más de 14 millones de personas en los países de la OCDE, casi el 3% del empleo total en dichos países. La Figura 2.8 presenta las tasas de crecimiento anual de empleos en el sector TIC entre 2001 y 2013, así como la comparación del porcentaje de empleos del sector TIC frente al empleo total en dichos países entre 2011 y 2014. OCDE (2015b) concluye que la contribución del sector TIC al crecimiento del empleo total ha variado significativamente en los últimos quince años. En 2013, el sector TIC representó el 22% del crecimiento total del empleo. De igual forma, concluye que mientras que el empleo en el sector TIC es estable, el empleo de especialistas TIC en todos los sectores de la economía ha aumentado, alcanzando al menos el 3% del empleo total en la mayoría de los países de la OCDE.



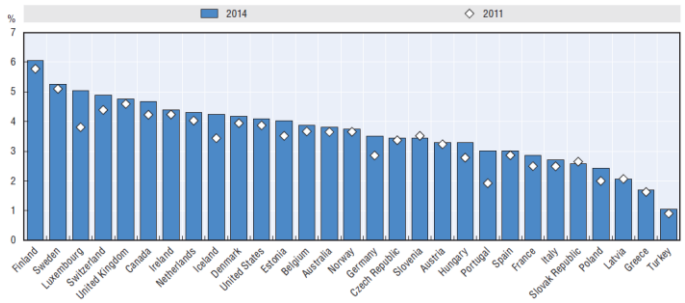
[5] Según la OCDE, la Paridad del Poder Adquisitivo (PPP) (en inglés, *Purchasing Power Parities*) es una tasa de conversión de moneda que iguala el poder adquisitivo de las distintas monedas eliminando las diferencias en los niveles de precios entre países.

Figura 2.8. Mercado laboral del sector TIC en países de la OCDE

Crecimiento anual de empleos TIC




% Empleos TIC frente al total 2011 y 2014




Fuente: OCDE (2015b)

Teniendo en cuenta lo anterior, la creciente relevancia del entorno digital sobre las actividades socioeconómicas, y su alto dinamismo, ha traído consigo en los últimos años un conjunto de riesgos, amenazas, vulnerabilidades e incidentes de diversos tipos, a los que han estado expuestos los individuos y las organizaciones públicas y privadas. La Tabla 2.2 resume algunos casos relevantes sobre incidentes de seguridad digital en el mundo durante el 2014, en donde se puede apreciar que éstos afectan a cualquier sector de la economía, con consecuencias que pueden impactar de manera negativa a millones, e incluso miles de millones, de personas en el mundo.

Tabla 2.2. Grandes casos de incidentes de seguridad digital en el mundo durante 2014

| Mes de 2014 | Organización | Sector | Impacto |
|---|---|---|---|
| Enero | SNAPCHAT | Red social | 4,5 millones de nombres y números móviles comprometidos |
| Febrero | KICKSTARTER | Crowd funding | 5,6 millones de víctimas |
| Marzo | KOREAN TELECOM | Telecomunicaciones | 12 millones de suscriptores comprometidos |
| Abril | HEARTBLEED | Software | Primera de tres vulnerabilidades de fuente abierta |
| Mayo | EBAY | Compras | Base de datos de 145 millones de compradores comprometida |
| Junio | PF CHANG´S | Comidas | Más alta violación de información de alto nivel del mes |
| Julio | ENERGETIC BEAR | Energía | Operación de ciber espionaje a la industria de energía |
| Agosto | CYBERVOR | Tecnología | 1,2 billones de credenciales comprometidas |
| Septiembre | iCLOUD | Entretenimiento | Cuentas de celebridades comprometidas |
| Octubre | SANDWORM | Tecnología | Ataque a la vulnerabilidad de Windows |
| Noviembre | SONY PICTURES | Entretenimiento | Más alta violación de alto nivel del año |
| Diciembre | INCEPTION FRAMEWORK | Sector público | Operación de ciber espionaje a sector público |

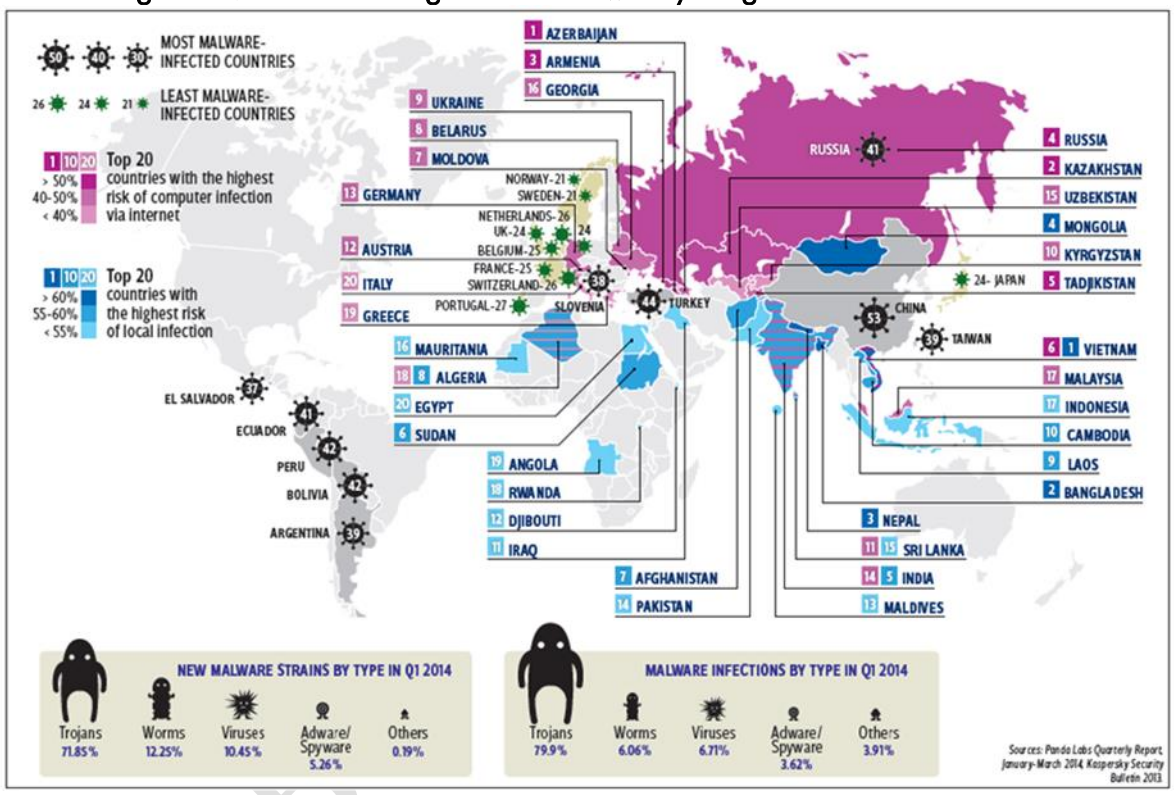
Fuente: Adaptado de Verizon (2015)

Los incidentes de seguridad digital 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*[6] 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.

[6] Término compuesto en inglés para llamar a cualquier software malicioso (*malicious software*).

Las Figuras 2.9 y 2.10 presentan los tipos de incidentes de seguridad digital más comunes alrededor del mundo en 2014 y 2015, respectivamente, en donde se destacan los troyanos (en inglés, *trojans*), los gusanos (en inglés, *worms*) y los virus (en inglés, *viruses*)[7]. También se destacan incidentes de suplantación de identidad (en inglés, *phishing*) caracterizado por intentar adquirir información confidencial de forma fraudulenta.

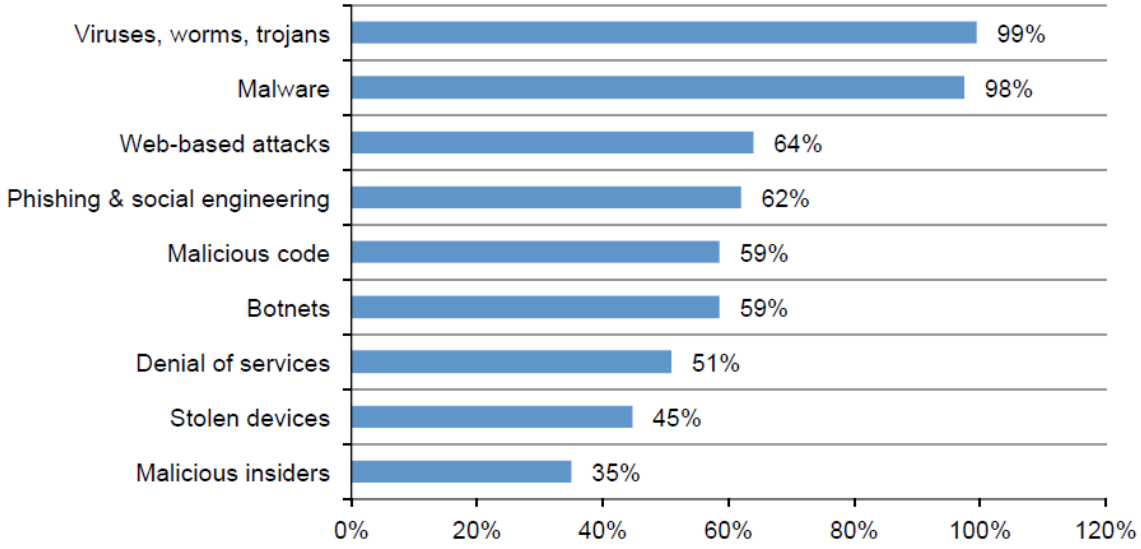
Figura 2.9. Distribución global de malware y riesgo de infección en 2014




Fuente: ISS (2014)

[7] El troyano (en inglés, *trojan*) es un *malware* que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al terminal infectado. El gusano (en inglés, *worm*) es un *malware* que tiene la propiedad de duplicarse a sí mismo. El virus (en inglés, *virus*) es un *malware* que tiene por objetivo alterar el normal funcionamiento del terminal, sin el permiso o el conocimiento del usuario.

Figura 2.10. Tipos de incidentes de seguridad digital más comunes en 2015



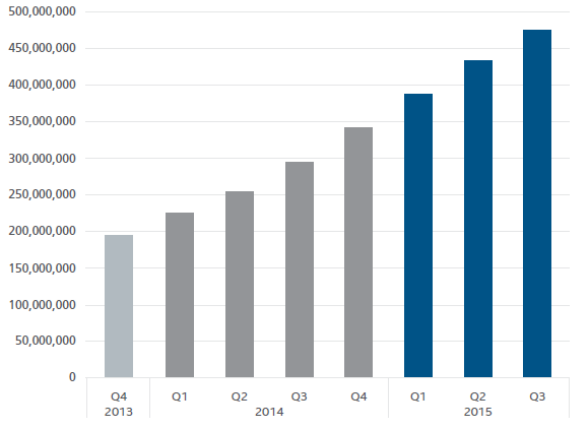

Fuente: Ponemon Institute (2015)

Hoy día, los incidentes de seguridad digital a nivel global[8], han evolucionado y son más sofisticados, al punto de poder penetrar sistemas de seguridad de entidades de gobierno, organismos internacionales, empresas del sector privado e infraestructura crítica para el Estado. Según Intel Security (2015b), los incidentes por *malware* han crecido continuamente durante los últimos años, y se espera cruzar la barrera de quinientos millones de incidentes en 2015.



[8] Según OEA (2014), "*el panorama actual en materia de amenazas cibernéticas en América Latina y el Caribe muestra que los usuarios están sufriendo el impacto de amenazas que son tendencia a nivel mundial y de otras propias de cada región. Como agravante de este desafío, América Latina y el Caribe tienen la población de usuarios de Internet de más rápido crecimiento del mundo, con un aumento del 12 por ciento durante el último año.*" Dicho informe identificó las principales tendencias que impactan a la región: 1) Las violaciones de datos están aumentando, 2) Continúan en aumento los ataques dirigidos, 3) Las estafas en medios sociales están aumentando, 4) el malware aumentó, especialmente los troyanos bancarios y robos, y 5) Los eventos de gran convocatoria son atractivos para los delincuentes.

Figura 2.11. Evolución del malware a nivel global a tercer trimestre de 2015 (acumulado)




Fuente: Intel Security Labs (2015b)

Los incidentes digitales no sólo muestran una tendencia global creciente en número, sino que también afectan a cualquier sector de la economía. Las Figuras 2.12 y 2.13, tomadas del reporte de seguridad de Internet 2015 de SYMANTEC (2015), muestran cómo diversos sectores de la economía son afectados por un tipo específico de incidente digital. En la Figura 2.12 se puede apreciar la lista de los diez sectores con más incidentes de exposición de identidades en el 2014, donde se resaltan sectores como el comercio minorista y el financiero. Por su parte, la Figura 2.13 muestra los diez sectores más afectados en el 2014 por incidentes del tipo "*spear-phishing*"[9].

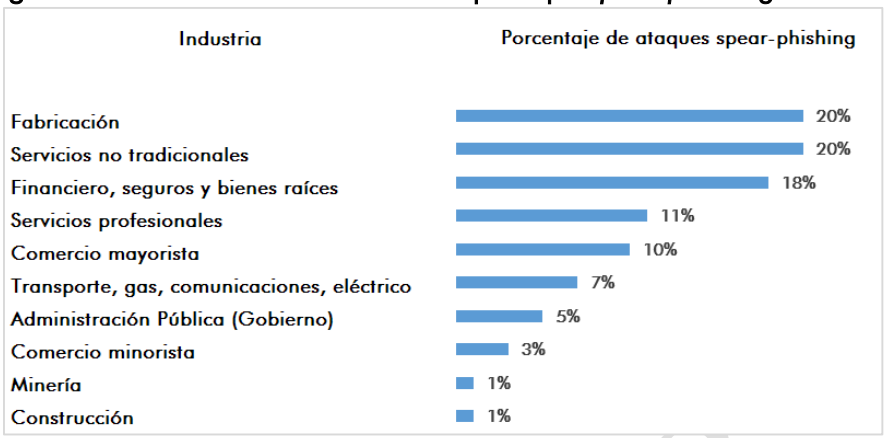
Figura 2.12. Sectores vulnerados por número de identidades expuestas

| Sector | Número de identidades expuestas | Porcentaje de identidades expuestas |
|---|---|---|
| Comerico minorista | 205.446.276 | 59,5% |
| Financiero | 79.465.597 | 23,0% |
| Software | 35.068.405 | 10,2% |
| Salud | 7.230.517 | 2,1% |
| Gobierno y sector público | 7.127.263 | 2,1% |
| Redes sociales | 4.600.000 | 1,3% |
| Telecomunicaciones | 2.124.021 | 0,6% |
| Hospitalidad | 1.818.600 | 0,5% |
| Educación | 1.359.190 | 0,4% |
| Arte y medios | 1.082.690 | 0,3% |

Fuente: Adaptado de SYMANTEC (2015)

[9] Intento de fraude por suplantación de correo electrónico dirigido contra una organización específica, buscando el acceso no autorizado a datos confidenciales, probablemente llevado a cabo por autores con ánimo de lucro, secretos comerciales o información militar.

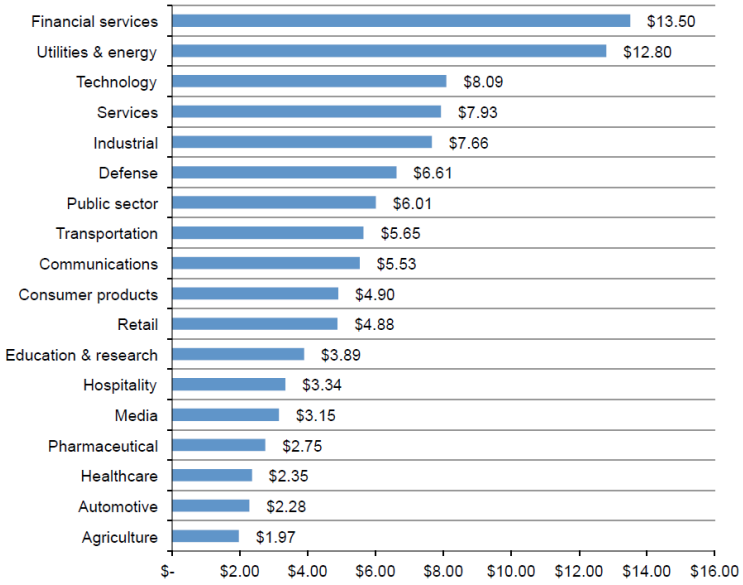
Figura 2.13. Industrias blanco de ataques tipo *spear-phishing* en 2014




Fuente: Adaptado de SYMANTEC (2015)

Por otra parte, los incidentes de seguridad digital tienen también un impacto directo sobre las finanzas de los individuos y de las organizaciones. Según el Ponemon Institute (2015), el costo estimado anual por incidentes de seguridad digital varía según el sector de la economía afectado. La Figura 2.14 muestra el costo estimado anual, para el año 2015, de incidentes de seguridad digital, donde se puede apreciar que para una organización típica del sector financiero éste es cercano a los USD $13 millones al año, o para el sector público es de aproximadamente USD $6 millones al año.

Figura 2.14. Costo estimado anual de incidentes de seguridad digital para una organización típica por industria
(millones de dólares anual)




Fuente: Ponemon Institute (2015)

Por otra parte, Intel Security (2013) estimó que el costo de las actividades maliciosas en el entorno digital para el año 2013, incluyendo las pérdidas de propiedad intelectual y de confidencialidad de la información, los crímenes en el entorno digital, la pérdida de información estratégica, los costos de oportunidad por la reducción de la confianza de las actividades en el entorno digital, los costos adicionales de aseguramiento, seguros y resiliencia, y los costos en pérdida de reputación para las compañías atacadas, equivalieron a una cifra agregada entre los USD $300 mil millones (equivalente al PIB de Singapur o Hong Kong) y USD $1 billón (del orden del PIB de México) a nivel global .

En Intel Security (2014) se estimó que el costo aproximado anual a la economía mundial, a partir de las actividades maliciosas en 2014, fue de USD $445 mil millones que equivalen a un 0,57% del PIB mundial, incluyendo las ganancias a los criminales y los costos de seguridad y recuperación para las empresas. La estimación conservadora fue de USD $375 mil millones, mientras que el máximo se estimó en USD $575 miles de millones. Dado que la economía digital generó en 2014 entre USD $2 billones y USD $3 billones, Intel Security (2014) estimó que el costo estimado de la actividad maliciosa en el entorno digital equivale entre un 15% y un 20% del valor creado por el Internet.

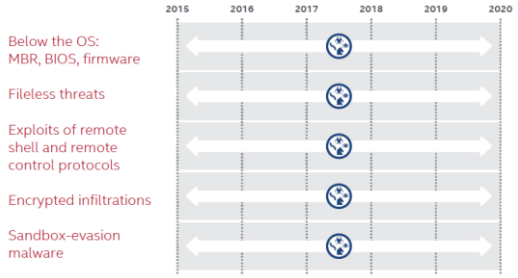
**Tabla 2.3. Costo estimado de actividad maliciosa en el entorno digital**

| ITEM | Costo Estimado | Porcentaje de PIB global |
|---|---|---|
| Piratería | USD$1 mil millones a USD$16 mil millones | 0,0012% a 0,02%* |
| Tráfico de drogas | USD$600 mil millones | 0,77%* |
| Actividad maliciosa en el entorno digital | USD$300 mil millones a USD$1 trillón | 0,4% a 1,3%* |

Nota: * se recalculó a partir de cifras de PIB del Banco Mundial.
Fuente: Adaptado de Intel Security Labs (2013)

Por otra parte, según Intel Security (2015b), el año 2015 ha marcado el inicio de un cambio significativo hacia nuevas amenazas que son más difíciles de detectar, incluyendo ataques sin archivo (*fileless threats*), infiltraciones cifrados (*encrypted infiltrations*) y el robo de credenciales, entre otros. La Figura 2.15 presenta las predicciones de nuevos tipos de amenazas en el entorno digital, lo que representa un escenario de mayor incertidumbre frente a la seguridad digital a nivel global.

**Figura 2.15. Predicciones de nuevos tipos de amenazas en el entorno digital en el futuro**




Fuente: Adaptado de Intel Security Labs (2015b)

Otro aspecto de gran relevancia en la seguridad digital es que los riesgos asociados a esta apuntan no sólo a bases de datos o sistemas de información, sino también a la infraestructura física nacional, como hidroeléctricas, redes de energía, sistemas SCADA[10], sistemas portuarios, sistemas de defensa, o armamento de guerra, entre otros. 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 un estudio desarrollado por Intel Security (2015c) sobre incidentes en infraestructuras críticas, a partir de una encuesta realizada en 2015 a profesionales de la seguridad de la información de 625 organizaciones a nivel global, se demuestra que casi nueve de cada diez encuestados han experimentado al menos un ataque en los sistemas de seguridad en 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 a su organización están aumentando y al 48% le parece probable que un ataque para poner fuera de operación la infraestructura crítica puede estar acompañado de pérdidas potenciales de vidas humanas. De igual manera, se ha demostrado que las amenazas a la infraestructura crítica son una realidad incuestionable y presentan una tendencia creciente. Por ejemplo, más del 59% de los encuestados respondió que los ataques dejaron como resultado un daño físico y más del 33% dio lugar a la interrupción del servicio.

En complemento de lo anterior, la OEA y Trend Micro (2015) realizaron una encuesta cuantitativa en línea en enero de 2015 entre los jefes de seguridad de las principales infraestructuras críticas de todos los Estados miembros. Asimismo, se incluyeron organizaciones privadas que gestionan la infraestructura crítica en sus países. Entre los principales resultados se encontró que el 53% de los encuestados ha observado un incremento de los incidentes en sus sistemas de cómputo durante al 2014 y que el 76% de los encuestados percibe que los incidentes contra las infraestructuras críticas se están volviendo más sofisticados. En este mismo sentido, concluyen también que los creadores de amenazas podrían estar apuntando a infraestructuras críticas más vulnerables en el futuro.

De esta manera, se puede concluir que, a nivel internacional, el mayor acceso y uso del entorno digital para el desarrollo de cualquier actividad socioeconómica, está generando una nueva economía digital con impactos importantes en los ámbitos económico y social de los países. No obstante, este nuevo entorno económico ha traído consigo nuevos tipos de

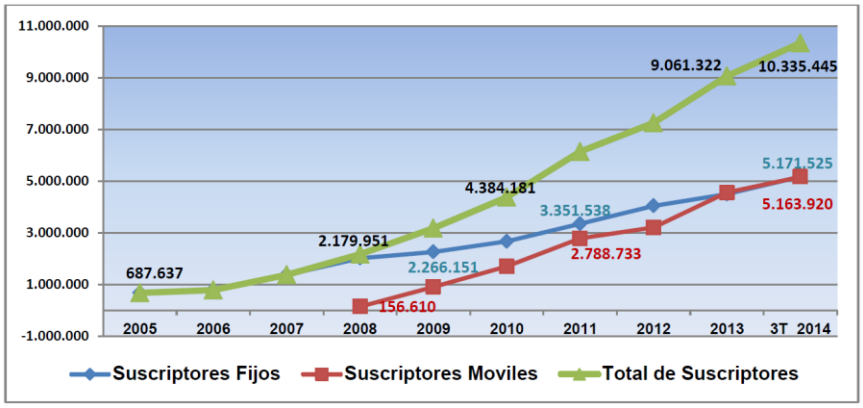
[10] Acrónimo en inglés para *Supervisory Control And Data Acquisition*. Sistema para el control y monitoreo remoto de equipos industriales, que opera con señales codificadas sobre un canal de comunicación.

amenazas y modalidades de incidentes de seguridad digital, que demandan una mayor planificación, prevención, y atención por parte de todos los actores de interés (gobiernos, organizaciones públicas y privadas, academia y sociedad civil).

- Panorama nacional

En línea con el panorama internacional, Colombia ha vivido una revolución digital durante la última década, en especial desde el año 2010, mediante la implementación del Plan Vive Digital. Según el Ministerio de Tecnologías de la Información y Comunicaciones, en el país se multiplicó por cinco el número de conexiones a Internet, pasando de 2,2 millones en 2010 a 12,2 millones en 2015[11].

Figura 2.16. Evolución de suscriptores de Internet en Colombia




Fuente: DNP (2014a)

De igual manera, según MINISTERIO TIC (2015a) en Colombia actualmente están conectados a la red troncal de fibra óptica 1.078 de los 1.123 municipios del país. También se destaca la instalación de 899 Puntos Vive Digital, centros de acceso comunitario para dar formación en el uso de internet a personas de estratos 1 y 2 en todo el país, así como de 7.621 Kioscos Vive Digital, centros de acceso comunitario, ubicados en zonas apartadas y centros poblados de más de 100 habitantes de la Colombia rural.

De igual manera, MINISTERIO TIC (2015a) establece que el Gobierno Nacional realizó la mayor inversión y donación de tecnología para escuelas y colegios oficiales de todo el país: 2 millones de tabletas y computadores. Y a través de la iniciativa Apps.co se construyó la mayor red de emprendedores de Latinoamérica (80.000 emprendedores) que están

[11] Según COLOMBIATIC (2015), se refiere a conexiones de banda ancha (Vive Digital) con corte a 30 de septiembre de 2015. La meta establecida en el Plan Nacional de Desarrollo 2014 – 2018, para el año 2018 es de 27 millones de conexiones a Internet.

haciendo realidad sus ideas de negocios basados en las TIC. Hoy en día, el 65% de los ciudadanos interactúan por medios electrónicos con agencias gubernamentales que disponen de más de cuatrocientos procedimientos totalmente en línea. Por lo tanto, los ciudadanos y las empresas son más abiertos y dispuestos a interactuar con el Estado mediante el uso de las TIC.

Así mismo, es necesario recordar que Colombia cuenta actualmente con el Plan Nacional de Desarrollo "*Todos por un nuevo país*" cuyos pilares son la paz, la equidad y la educación para el periodo 2014 – 2018. Para su ejecución, dicho plan se apoya en estrategias transversales soportadas en las TIC. Por ejemplo, DNP (2014b) dispone que respecto a la competitividad y las infraestructuras estratégicas, el plan establece el uso de las TIC como plataforma para alcanzar altos niveles de equidad y de educación mejorando la competitividad. De igual forma, las TIC se consideran un componente transversal relevante en el desarrollo de los demás sectores económicos del país[12].

En cuanto a la movilidad social, el plan tiene como objetivos cerrar aún más la brecha en el acceso a la educación y mejorar su calidad mediante el uso eficiente de las TIC. En cuanto, a la transformación del sector agricultura, el objetivo es lograr la competitividad rural mediante la adopción y promoción de dichas tecnologías. En aspectos como la justicia, la seguridad y la democracia para lograr la paz, se busca garantizar el acceso de todos los ciudadanos a todo tipo de servicios relacionados con la justicia mediante el uso de las TIC. El buen gobierno se logra mediante el uso de la información de los ciudadanos adecuadamente y asegurando su gestión oportuna y eficiente, así como construyendo un gobierno más transparente y abierto. El crecimiento verde está orientado a lograr resiliencia y reducir la vulnerabilidad ante el riesgo de desastres y el cambio climático y todo esto debe ser apoyado por mejores y más integrados sistemas de información.

En Colombia, se apuesta por los beneficios aportados por el uso de las TIC ya que son herramientas poderosas que ayudan a transformar la vida de todos y cada uno de los colombianos mediante el suministro de más y mejor infraestructura que permite el acceso a



[12] Por ejemplo, las TIC se consideran como apoyo al sector eléctrico colombiano en el cual el Sistema Interconectado Nacional (SIN) agrupa a las diferentes actividades de la cadena de prestación del servicio de energía eléctrica, las cuales se encuentran divididas en: Sistema de Generación, Sistema de Transmisión Nacional (STN), Sistema de Transmisión Regional (STR) y Sistema de Distribución Local (SDL). En el SIN se incluye el 98,9% de la generación instalada en el país. Bajo este contexto, Colombia ha venido realizado importantes avances en materia de automatización del STN y su integración con los Sistemas de Generación ubicados en diferentes zonas del territorio nacional, evidenciando la utilización de una infraestructura TIC que soporta todo el sistema eléctrico. Atendiendo la experiencia a nivel del STN, el sector eléctrico se encuentra listo para dar el siguiente paso para continuar con las automatización del SDL, el cual cuenta con una red de 200.000 km de líneas divididas en más de 5.000 circuitos con una media de casi 100 transformadores por circuito, que representan el reto de alcanzar la automatización de la red eléctrica en territorio Colombiano al año 2030.

Internet, junto con las oportunidades que se generan a lo largo de todo el país, generando una cultura de apropiación y adopción de las TIC que potencie el desarrollo económico y social del país.

Según el *Índice de Evolución Digital* de Tufts University (2013), Colombia es uno de los mercados con el potencial de desarrollar economías digitales fuertes, mostrando una consistente e impresionante mejora de su estado de preparación digital. Katz (2015b) señala que el país pasó de ser un país de "*digitalización transicional*" en 2013 a uno de "*digitalización transicional avanzada*" en 2015, al existir en el país modificaciones adecuadas en el contexto político e institucional respecto al sector de TIC.

A nivel regional, la digitalización en América Latina ha contribuido en US$ 195 mil millones al PIB de la región entre el 2005 y el 2013. Esto significa que el desarrollo de la digitalización generó aproximadamente 4,3% de crecimiento acumulado al PIB de América Latina. De la Figura 2.17, Katz (2015b) estimó que la digitalización en Colombia contribuyó en USD$ 16 mil millones al PIB del país durante el periodo 2005 a 2013, lo que representó un 6,12% de crecimiento acumulado del PIB en dicho periodo.

**Figura 2.17. Impacto económico de la digitalización en América Latina (2005-2013)**

**En US$ millones a tipo de cambio corriente**

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | Total |
|---|---|---|---|---|---|---|---|---|---|---|
| Argentina | 867 | 1.200 | 1.056 | 914 | 566 | 2.672 | 1.157 | 2.087 | 2.261 | 12.781 |
| Bolivia | 0 | 0 | 141 | 171 | 66 | 34 | 343 | 205 | 161 | 1.122 |
| Brasil | 3.606 | 2.636 | 7.854 | 9.752 | 8.159 | 16.486 | 6.619 | 23.003 | 10.365 | 88.480 |
| Chile | 460 | 498 | 382 | 540 | 1.059 | 1.422 | 1.693 | 791 | 782 | 7.626 |
| Colombia | 1.786 | 964 | 695 | 1.846 | 1.203 | 2.003 | 1.503 | 2.871 | 3.104 | 15.976 |
| Costa Rica | 14 | 65 | 9 | 126 | 25 | 248 | 412 | 499 | 240 | 1.637 |
| Cuba | 42 | 112 | 108 | 0 | 228 | 261 | 238 | 293 | 23 | 1.305 |
| Ecuador | 329 | 0 | 201 | 542 | 19 | 418 | 343 | 499 | 520 | 2.870 |
| El Salvador | 54 | 73 | 84 | 133 | 125 | 277 | 142 | 106 | 69 | 1.064 |
| Guatemala | 120 | 188 | 221 | 229 | 88 | 188 | 14 | 470 | 14 | 1.532 |
| Haití | N.D. | N.D. | N.D. | N.D. | N.D. | N.D. | 176 | 0 | 25 | 200 |
| Honduras | 44 | 49 | 256 | 85 | 76 | 200 | 0 | 52 | 33 | 795 |
| Jamaica | 4 | 0 | 22 | 0 | 46 | 300 | 21 | 51 | 23 | 467 |
| México | 2.170 | 1.992 | 1.389 | 1.725 | 3.674 | 5.207 | 8.818 | 4.968 | 5.596 | 35.540 |
| Nicaragua | NA | NA | NA | NA | NA | NA | 102 | 138 | 44 | 285 |
| Panamá | 13 | 77 | 136 | 100 | 194 | 287 | 164 | 189 | 72 | 1.231 |
| Paraguay | 11 | 174 | 96 | 174 | 167 | 75 | 60 | 198 | 100 | 1.055 |
| Perú | 302 | 305 | 756 | 275 | 533 | 941 | 2.212 | 1.174 | 811 | 7.309 |
| R. Dominicana | 345 | 112 | 1 | 140 | 98 | 349 | 249 | 0 | 472 | 1.766 |
| Trinidad & Tobago | 46 | 95 | 27 | 181 | 24 | 380 | 40 | 70 | 73 | 936 |
| Uruguay | 41 | 79 | 85 | 133 | 152 | 296 | 276 | 308 | 337 | 1.707 |
| Venezuela | 1.037 | 922 | 871 | 682 | 1.185 | 1.737 | 338 | 1.551 | 1.005 | 9.327 |
| Total | 11.292 | 9.541 | 14.389 | 17.750 | 17.688 | 33.781 | 24.917 | 39.522 | 26.128 | 195.009 |

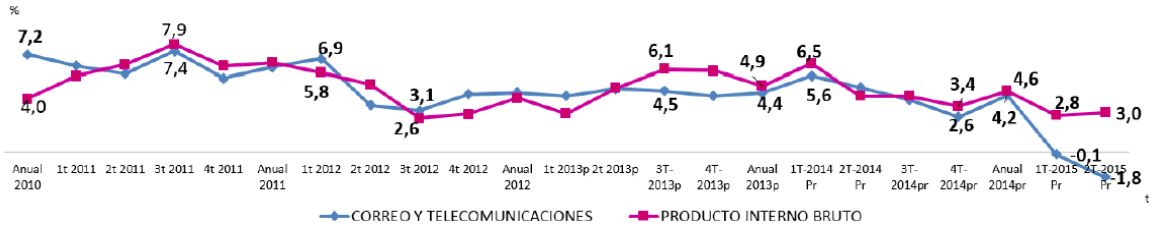
**% del PIB que representa el incremento del PIB resultante de la digitalización (en %)**

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | Total |
|---|---|---|---|---|---|---|---|---|---|---|
| Argentina | 0,47 | 0,55 | 0,40 | 0,28 | 0,18 | 0,72 | 0,26 | 0,44 | 0,45 | 3,76 |
| Bolivia | 0,00 | 0,00 | 1,11 | 1,06 | 0,40 | 0,18 | 1,50 | 0,79 | 0,58 | 5,62 |
| Brasil | 0,41 | 0,24 | 0,57 | 0,59 | 0,50 | 0,77 | 0,27 | 0,96 | 0,42 | 4,74 |
| Chile | 0,37 | 0,32 | 0,22 | 0,30 | 0,61 | 0,65 | 0,67 | 0,29 | 0,27 | 3,72 |
| Colombia | 1,21 | 0,60 | 0,33 | 0,77 | 0,51 | 0,69 | 0,45 | 0,77 | 0,78 | 6,12 |
| Costa Rica | 0,07 | 0,29 | 0,03 | 0,42 | 0,08 | 0,67 | 0,98 | 1,08 | 0,48 | 4,10 |
| Cuba | 0,08 | 0,18 | 0,16 | 0,00 | 0,31 | 0,35 | 0,32 | 0,39 | 0,03 | 1,83 |
| Ecuador | 0,81 | 0,00 | 0,40 | 0,91 | 0,03 | 0,67 | 0,48 | 0,63 | 0,61 | 4,55 |
| El Salvador | 0,32 | 0,39 | 0,42 | 0,62 | 0,61 | 1,29 | 0,61 | 0,44 | 0,28 | 4,98 |
| Guatemala | 0,44 | 0,62 | 0,65 | 0,59 | 0,23 | 0,45 | 0,03 | 0,94 | 0,03 | 3,98 |
| Haití | N.D. | N.D. | N.D. | N.D. | N.D. | N.D. | 2,35 | 0,00 | 0,29 | 2,64 |
| Honduras | 0,47 | 0,47 | 2,14 | 0,64 | 0,54 | 1,31 | 0,00 | 0,29 | 0,18 | 6,04 |
| Jamaica | 0,04 | 0,00 | 0,17 | 0,00 | 0,37 | 2,21 | 0,14 | 0,34 | 0,15 | 3,41 |
| México | 0,25 | 0,20 | 0,13 | 0,16 | 0,41 | 0,50 | 0,75 | 0,42 | 0,43 | 3,26 |
| Nicaragua | N.D. | N.D. | N.D. | N.D. | N.D. | N.D. | 1,07 | 1,32 | 0,40 | 2,79 |
| Panamá | 0,08 | 0,45 | 0,69 | 0,43 | 0,80 | 1,06 | 0,53 | 0,52 | 0,18 | 4,74 |
| Paraguay | 0,13 | 1,60 | 0,68 | 0,92 | 1,04 | 0,36 | 0,25 | 0,76 | 0,32 | 6,06 |
| Perú | 0,40 | 0,35 | 0,75 | 0,23 | 0,45 | 0,65 | 1,31 | 0,62 | 0,40 | 5,15 |
| R. Dominicana | 1,00 | 0,31 | 0,00 | 0,30 | 0,21 | 0,67 | 0,45 | 0,00 | 0,79 | 3,73 |
| Trinidad & Tobago | 0,28 | 0,51 | 0,12 | 0,64 | 0,12 | 1,81 | 0,17 | 0,27 | 0,27 | 4,19 |
| Uruguay | 0,24 | 0,40 | 0,36 | 0,44 | 0,50 | 0,75 | 0,59 | 0,62 | 0,65 | 4,54 |
| Venezuela | 0,71 | 0,50 | 0,37 | 0,21 | 0,36 | 0,44 | 0,11 | 0,40 | 0,29 | 3,38 |
| Total | 0,45 | 0,32 | 0,43 | 0,44 | 0,42 | 0,65 | 0,51 | 0,66 | 0,43 | 4,30 |

Fuente: Adaptado de Katz (2015a)

Esta situación está acorde también con el comportamiento económico del sector TIC en el país durante los últimos cinco años. La Figura 2.18 presenta el crecimiento del PIB total y del PIB asociado a la actividad económica Correo y Telecomunicaciones. No obstante, se presenta un decrecimiento del 1,8% en el segundo trimestre de 2015, durante el periodo 2010 a 2014 dicha rama tuvo tasas de crecimiento positivas, y en algunos casos superiores al de la economía.

Figura 2.18. Crecimiento del Producto Interno Bruto y de la actividad de Correo y Telecomunicaciones 2010 - 2T 2015 (%)




Fuente: MINISTERIO TIC (2015b)

Durante los años 2010 a 2014, según cifras de la Encuesta Anual de Servicios (EAS) del DANE, el sector TIC[13] tuvo una participación del 24% del total del valor agregado de la economía colombiana en 2014. Esto significa que el sector TIC está posicionado como uno de los sectores que genera mayor valor agregado en el país. Se aprecia en la Tabla 2.4 que aunque el valor agregado del sector TIC crece a una tasa promedio anual del 9% su participación en el valor agregado total ha venido disminuyendo levemente desde el año 2012.

Por otra parte, en cuanto al consumo de bienes intermedios, aprovechando la producción de los demás sectores, el sector TIC creció entre el 2010 y el 2014 un 48%. Dicho crecimiento, comprueba que cada año el sector TIC se comporta como un sector transversal en la economía colombiana, por lo que tiene influencia en el crecimiento de los demás sectores. Así mismo, la participación del consumo intermedio del sector TIC en el consumo intermedio total se ha venido incrementando alcanzando un 33% en el año 2014.

Con respecto a la productividad del sector TIC, en la Tabla 2.4 se aprecia que por cada peso que se gastó en el sector TIC en 2014, se generó $1,6 pesos de ingresos o en otras palabras $0,6 pesos de rendimientos. Esto teniendo en cuenta que la EAS del DANE mide la productividad de las actividades económicas mediante la relación entre los ingresos y el consumo intermedio. Vale la pena anotar que la productividad del sector ha venido disminuyendo levemente desde el año 2012.



[13] El análisis de impacto económico del sector TIC en la economía colombiana entre 2010 y 2014 a partir de la Encuesta Anual de Servicios (EAS) del DANE presentado en la Tabla 2.4 tiene en cuenta una muestra aproximada de 5.318 empresas en Colombia (566 del sector TIC) y considera el sector TIC en Colombia como el conjunto de actividades según clasificación CIIU 3 y 4 definidas por la Organización de las Naciones Unidas (ONU) así: i) Bajo la clasificación CIIU 3 se toman las actividades: I3 Actividades de postales y correos, I4 Telecomunicaciones, O1 Actividades de radio y televisión y agencias de noticias y K2 Informática y actividades conexas, y ii) Bajo la clasificación CIIU 4 se toman las actividades: H2 Postales y correos, J3 Actividades de telecomunicaciones, J2 Programación y transmisión de radio y televisión y agencias de noticias y J4 Informática y servicios de información.

La productividad laboral en el sector TIC para Colombia en 2014 fue aproximadamente de $138.000 pesos, siendo ésta un 257% más alta que la productividad laboral total del país. Vale la pena mencionar que el DANE calcula la productividad laboral por cada persona ocupada mediante la relación entre el valor agregado de la actividad económica y la cantidad de personas ocupadas de dichas actividades. De esta manera, el sector TIC ocupa el primer lugar del ranking de actividades con mayor productividad laboral por persona ocupada en el 2014.

Finalmente, la contribución del sector TIC al crecimiento del empleo total en Colombia se ha incrementado levemente durante los últimos cinco años. Durante dicho periodo, la tasa de crecimiento anual de los empleos en el sector TIC ha sido de 2%. De igual forma, se concluye que el empleo en el sector TIC alcanzó un 7%% del empleo total en el país.

**Tabla 2.4. Impacto económico del sector TIC en la economía colombiana entre 2010 y 2014 (cifras en pesos corrientes)**

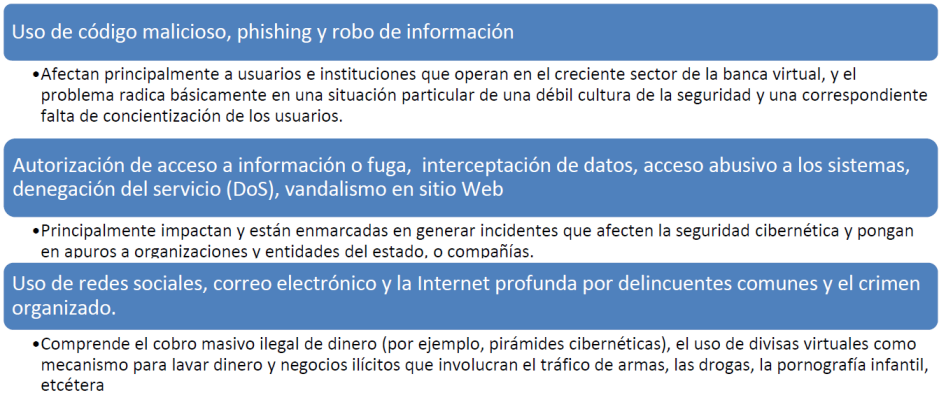
| | 2010 | 2011 | 2012 | 2013 | 2014 | Tasa de Crecimiento entre 2010 y 2014 | Tasa de crecimiento promedio anual entre los años 2010 y 2014 |
|---|---|---|---|---|---|---|---|
| Empresas Total | 5343 | 5170 | 5427 | 5301 | 5351 | 0% | 0% |
| Empresas Sector TIC | 576 | 552 | 563 | 558 | 579 | 1% | 0% |
| Empresas Sector TIC vs Empreas Total | 10,8% | 10,7% | 10,4% | 10,5% | 10,8% | | |
| Personal Ocupado Total | 1364309 | 1415763 | 1493676 | 1595485 | 1705181 | 25% | 6% |
| Personal Ocupado Sector TIC | 84576 | 85948 | 93000 | 105725 | 116221 | 37% | 8% |
| Personal Ocupado Sector TIC vs Personal Ocupado Total | 6,2% | 6,1% | 6,2% | 6,6% | 6,8% | 10% | 2% |
| Ingresos Total (miles de $corr.) | $ 82.389.436.832 | $ 91.756.810.788 | $ 103.402.734.660 | $ 115.243.624.805 | $ 126.035.184.558 | 53% | 11% |
| Ingresos Sector TIC (miles de $ corr.) | $ 25.091.681.684 | $ 28.017.099.021 | $ 30.604.072.934 | $ 34.411.551.510 | $ 37.769.880.923 | 51% | 11% |
| Ingresos Sector TIC vs Ingresos Total (%) | 30,5% | 30,5% | 29,6% | 29,9% | 30,0% | | |
| Ingresos Sector TIC por empresa (miles de $ corr.) | $ 43.561.947 | $ 50.755.614 | $ 54.358.922 | $ 61.669.447 | $ 65.232.955 | 50% | 11% |
| Valor agregado Total (miles de $corr.) | $ 43.076.868.441 | $ 48.857.194.019 | $ 55.278.004.839 | $ 61.419.292.334 | $ 65.745.558.538 | 53% | 11% |
| Valor agregado Sector TIC (miles de $ corr.) | $ 11.315.515.483 | $ 12.646.287.222 | $ 14.192.750.788 | $ 15.640.944.849 | $ 16.008.414.582 | 41% | 9% |
| VA Sector TIC vs VA Total (%) | 26,3% | 25,9% | 25,7% | 25,5% | 24,3% | | |
| Consumo Intermedio Total (miles de $corr.) | $ 37.060.840.194 | $ 40.202.277.869 | $ 44.925.214.151 | $ 49.991.809.439 | $ 55.543.342.122 | 50% | 11% |
| Consumo Intermedio Sector TIC (miles de $ corr.) | $ 12.315.349.763 | $ 13.547.743.059 | $ 14.285.044.139 | $ 16.067.664.387 | $ 18.232.907.927 | 48% | 10% |
| CI Sector TIC vs CI Total (%) | 33,2% | 33,7% | 31,8% | 32,1% | 32,8% | | |
| Gastos de Personal Total (miles de $corr.) | $ 27.989.926.902 | $ 30.521.312.413 | $ 34.889.923.521 | $ 37.879.397.772 | $ 41.487.367.815 | 48% | 10% |
| Gastos de Personal Sector TIC (miles de $ corr.) | $ 3.420.469.121 | $ 3.863.365.433 | $ 4.423.222.526 | $ 5.029.288.455 | $ 5.499.769.526 | 61% | 13% |
| Gastos de Personal Sector TIC vs Gastos de Personal Total (%) | 12,2% | 12,7% | 12,7% | 13,3% | 13,3% | | |
| Productividad Total | 1,27 | 1,30 | 1,30 | 1,31 | 1,30 | 3% | 1% |
| Productividad Total Sector TIC | 1,59 | 1,61 | 1,64 | 1,63 | 1,59 | 0% | 0% |
| Productividad Laboral | $ 31.574 | $ 34.509 | $ 37.008 | $ 38.496 | $ 38.556 | 22% | 5% |
| Productividad Laboral Sector TIC | $ 133.791 | $ 147.139 | $ 152.610 | $ 147.940 | $ 137.741 | 3% | 1% |
| Remuneración Mensual | $ 1.593 | $ 1.682 | $ 1.798 | $ 1.839 | $ 1.890 | 19% | 4% |
| Remuneración Mensual Sector TIC | $ 2.937 | $ 3.320 | $ 3.487 | $ 3.559 | $ 3.588 | 22% | 5% |

Fuente: MINISTERIO TIC a partir de DANE Encuesta Anual de Servicios (EAS) para 2010, 2011, 2012, 2013 y 2014

En adición a lo anterior, Colombia está haciendo grandes esfuerzos para reducir la brecha digital, ya que más Internet equivale a menos pobreza y más productividad, y el desarrollo de infraestructura de información y el uso activo de ella se convierten en un camino ágil para su crecimiento económico. Obviamente el país quiere aprovechar dichas oportunidades y busca convertirse en un actor relevante en la economía digital. Pero también se entiende que esto no sería posible, si los ciudadanos y las empresas no confían en el entorno digital y si no se establece una visión general clara de la seguridad digital en el país.

Si bien el incremento en la conectividad en Colombia ha traído consigo innumerables beneficios para el país también, se han incrementado las amenazas, delitos e incidentes en el entorno digital afectando la seguridad de los ciudadanos, las organizaciones públicas y privadas, e incluso infraestructuras que hacen parte de los intereses de la nación. Durante los últimos años, Colombia ha sido foco de interés para distintos tipos de atacantes. Las técnicas y vectores de ataque se han sofisticado trayendo consigo el incremento de efectividad de los mismos, teniendo como consecuencia una mayor dificultad para su oportuna detección. CRC (2015) menciona que en Colombia se han identificado tres tendencias específicas de incidentes que se muestran en la Figura 2.19. Adicionalmente, en la Tabla 2.5 se presentan las modalidades utilizadas por delincuentes en Colombia para obtener la información de los clientes financieros identificadas por ASOBANCARIA (2015).

**Figura 2.19. Tendencias de incidentes en el entorno digital en Colombia**




Fuente: CRC (2015)

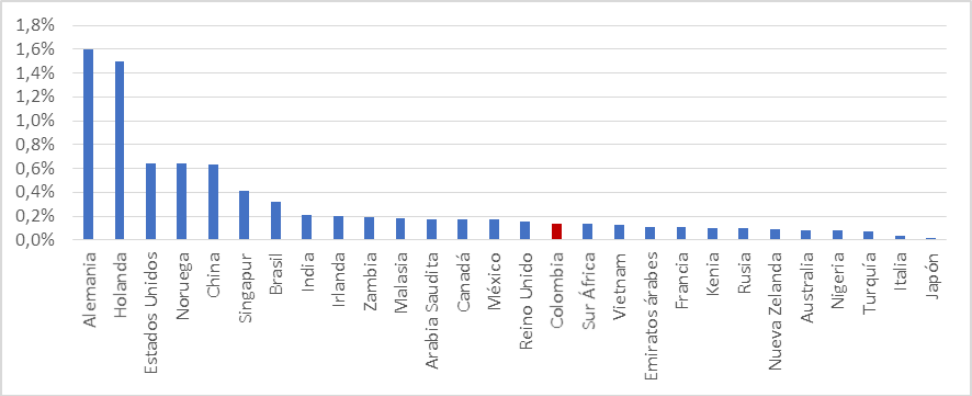
**Tabla 2.5. Modalidades utilizadas por delincuentes en Colombia para obtener la información de los clientes financieros**

| Concepto | Descripción |
|---|---|
| **Phishing** | Esta modalidad consiste en que los delincuentes suplantan el sitio web de la entidad con el fin de obtener la información personal y financiera (números de tarjetas y claves) y, mediante correo electrónico o ventanas emergentes, direccionan a los clientes a la página de internet suplantada donde le solicitan su información. |
| **Smishing** | Con esta práctica fraudulenta se hace uso de los mensajes de texto SMS y la ingeniería social para engañar a las personas con el fin de obtener la información personal y financiera. |
| **Software espía (Malware o troyanos)** | Los delincuentes instalan un software para monitorear las actividades que realiza el usuario del PC. Igualmente, tienen acceso a la información que el usuario teclea y a los contenidos de sus correos electrónicos. |
| **Key logger** | Mediante la utilización de software o hardware, los delincuentes buscan grabar el texto que escriben las personas en el teclado de sus PC. |
| **Clonación** | Corresponde al copiado no autorizado de la información contenida en la banda magnética de las tarjetas débito y crédito. |

Fuente: ASOBANCARIA (2015)

Con relación a los costos de los incidentes de seguridad digital en el país, por una parte ISS (2014) estimó que el costo de la actividad maliciosa en el entorno digital para Colombia en 2013 fue aproximadamente de USD $ 464 millones. Por otra parte, Intel Security (2014) estimó que dicho costo para Colombia en 2014, fue aproximadamente de 0,14% del PIB.

Figura 2.20. Costo de actividad maliciosa como % del PIB en algunos países en 2014




Fuente: Adaptado de Intel Security (2014)

En complemento de lo anterior, a partir de información provista por Intel Security Foundstone, empresa de servicios de consultoría para la respuesta a incidentes, el descubrimiento de vulnerabilidades y la estrategia de seguridad en colaboración con Intel Security, durante el día 7 de enero de 2016 en los Estados Unidos se reportaron un total de 604.493 incidentes y en Brasil 77.423, mientras que en Colombia se reportaron 8.128 incidentes.

Una vez analizado el panorama internacional y el panorama nacional en torno a la evolución del acceso y uso de las TIC en el entorno digital, se concluye que Colombia es cada vez más digital gracias a los esfuerzos del Gobierno nacional mediante la implementación de políticas sectoriales efectivas que permiten impulsar la participación de la sociedad en actividades económicas y sociales en el entorno digital. La digitalización del país genera crecimiento económico y mejoras en la productividad y competitividad. Sin embargo, el mayor uso del entorno digital acarrea mayores riesgos e incertidumbres. La forma de abordarlos ha sido tema de discusión a nivel internacional, ya que las condiciones para desarrollar dichas actividades económicas y sociales han venido cambiando drásticamente. Por lo tanto, el incremento de incidentes digitales en el mundo y en el país genera impactos en la economía digital que deben ser abordados bajo una visión actualizada en torno al tema.

## 3. MARCO CONCEPTUAL

Esta sección expone las nuevas tendencias respecto a la definición de estrategias o políticas de seguridad digital y al modelo de gestión de riesgos de seguridad digital, a partir de las mejores prácticas a nivel internacional en torno al tema, modelo hacia el cual debe avanzar el Gobierno nacional.

Según OCDE (2015a), durante los últimos diez años, los incidentes de seguridad digital se han incrementado generando una serie de incertidumbres y consecuencias significativas para todos y cada uno de los individuos y organizaciones. Esta situación ha generado la expedición de un marco internacional normativo, la cual se presenta en la Tabla 3.1, así como un intenso debate en torno a la manera como se deben abordar estos incidentes actualmente.

Tabla 3.1. Marco normativo internacional

| Instrumento | Materia |
|---|---|
| **Convenio sobre Ciberdelincuencia del Consejo de Europa – CCC (conocido como el convenio sobre Cibercriminalidad de Budapest16) 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. Único instrumento vinculante vigente sobre el tema en el ámbito internacional y su protocolo para la criminalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos. El Consejo considera que el delito cibernético exige una política penal común destinada a prevenir la delincuencia en el ciberespacio y en particular, hacerlo mediante la adopción de legislación apropiada y el fortalecimiento de la cooperación internacional. Cabe resaltar que si bien el CCC tuvo su origen en el ámbito regional europeo, es un instrumento abierto para su adhesión a todos los países del mundo. Es importante señalar que Colombia logró la invitación del Consejo de Europa para adherirse a la Convención de Budapest, como resultado de un proceso que inició en el año 2011 con la promulgación del Documento CONPES 3701, el cual requirió que el Ministerio de Relaciones Exteriores realizara una solicitud formal al Consejo de Europa para que Colombia fuera invitada a hacer parte de la Convención de Budapest. De esta manera, el 20 de septiembre de 2013, el Consejo de Ministros del Consejo de Europa aprobó la invitación para que Colombia adhiera a la Convención de Budapest, y sea parte del protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. A partir de esta decisión Colombia cuenta con cinco (5) años para adherir al instrumento internacional. |
| **Resolución AG /RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos** | Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética. Estipula tres vías de acción: i) Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores – CSIRT, cometido asignado al Comité Interamericano Contra el Terrorismo – CICTE; ii) Identificación y adopción de normas técnicas para una arquitectura segura de Internet, labor desarrollada por la Comisión Interamericana de Telecomunicaciones; y iii) Adopción y/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. La estrategia integral de seguridad cibernética es descrita en esta Resolución AG/RES. 2004 (XXXIV-O/04), aprobada en la cuarta sesión plenaria del trigésimo cuarto período ordinario de sesiones de la Asamblea General de la OEA, celebrada el 8 de junio de 2004. En esta medida las Resoluciones tienen un nivel de cumplimiento diferente al que genera un Tratado o una Convención, puesto que si un País miembro de la OEA ha aprobado la Resolución a través del voto se espera que el País tenga el mismo compromiso para llevar a cabo su cumplimiento. En este caso Colombia como miembro de la Asamblea General de la OEA suscribió esta Resolución, y la fuerza vinculante de las resoluciones se refleja en la obligatoriedad que tienen los países de presentar informes y exponer resultados, en relación con lo que se ha acordado en estas. Adicionalmente, Colombia como miembro del Comité Interamericano contra el Terrorismo (CICTE) y de la Comisión Interamericana de Telecomunicaciones (CITEL), debe sujetarse a las Resoluciones y recomendaciones que emitan estos organismos. Finalmente es importante tener en cuenta que las Resoluciones de la OEA, no tienen el |

| Instrumento | Materia |
|---|---|
| | carácter vinculante de un tratado, sin embargo la Asamblea General es el órgano supremo de la OEA y todas sus manifestaciones tienen un elevado nivel político diplomático. |
| 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. De acuerdo con el artículo 3 del Tratado de creación del Tribunal de Justicia de la CAN, el esquema jurídico de la CAN es supranacional, lo que se traduce en la emisión de leyes o normas comunitarias19, que tienen efectos directos y vinculantes en los países miembros desde la fecha de su publicación en la Gaceta Oficial del Acuerdo de Cartagena sin necesidad de requerir previa aprobación de los Congresos Nacionales para su entrada en vigencia en cada uno de los países miembros. |
| 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. Esta resolución continúa el seguimiento de la Asamblea, con las resoluciones emitidas hasta el 2 de diciembre de 2008. Las Resoluciones de la Asamblea General de la ONU, como las que afectan cuestiones presupuestarias, asuntos internos o instrucciones a órganos de rango inferior son vinculantes, sin embargo las recomendaciones de la Asamblea General y las Resoluciones fundadas en estas, se cumplen en la medida que el Estado pueda ejecutarlas de acuerdo a su presupuesto. |
| Directiva 2006/24 de la Unión Europea | La Directiva 2006/24 establecía 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. Esta directiva fue declarada inválida por el Tribunal de Justicia de la Unión Europea en Abril de 2014 dado que imponía a los países miembros la obligación de adoptar en las legislaciones internas la conservación de datos que se cursan en el tráfico de las comunicaciones21, por considerar que dicha medida vulnera los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal. |
| 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). |
| National Cyber Security Framework 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. |

Fuente: CRC (2015)

Adicionalmente muchas organizaciones multilaterales, tales como UIT[14], OCDE[15], OTAN[16] y OEA, así como el sector privado[17], han venido analizando los enfoques para asumir el tema de seguridad digital bajo las condiciones actuales del entorno digital, en donde se propone que las estrategias o políticas nacionales en torno al tema tengan en cuenta la gestión del riesgo, el liderazgo sistemático de los Gobiernos, el enfoque multidimensional, la responsabilidad compartida y la protección de los valores nacionales. La Figura 3.1 presenta la evolución de la implementación de estrategias de seguridad digital en varios países, algunos pertenecientes a la OCDE y otros no.



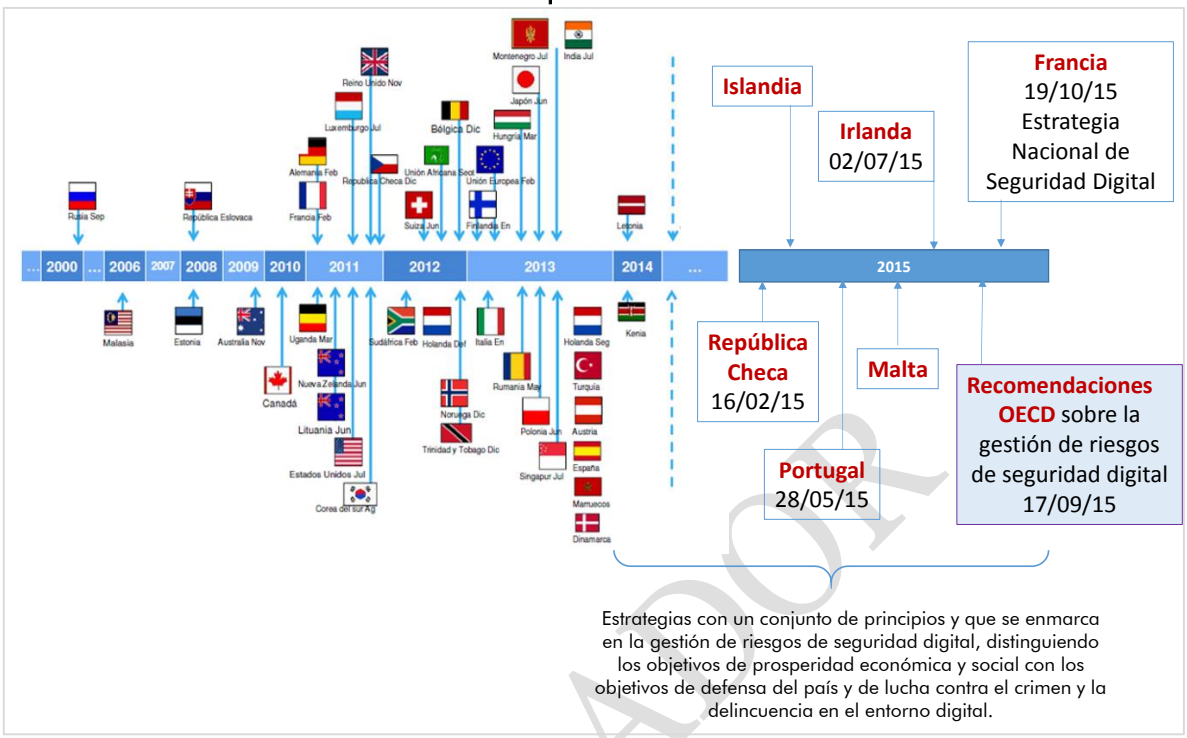
[14] La Unión Internacional de Telecomunicaciones –UIT– (International Telecommunications Union –ITU–, en inglés) es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras. UIT (2011) estableció como principios generales de una estrategia nacional de ciberseguridad la gestión del riesgo, el liderazgo sistemático de los Gobiernos, el enfoque multidimensional, la responsabilidad compartida y la protección de los valores nacionales.

[15] OCDE (2015b) resalta que una nueva generación de estrategias nacionales de ciberseguridad bajo políticas nacionales con el apoyo de liderazgo de alto nivel en los gobiernos, incluyendo a todos los actores de la sociedad con un enfoque holístico abarcando aspectos económicos, sociales, técnicos, legales, educacionales, diplomáticos, militares y relacionados con la inteligencia.

[16] La Organización del Tratado del Atlántico Norte –OTAN– (North Atlantic Treaty Organization –NATO–, EN INGLÉS) también denominada *Alianza del Atlántico* o *del Atlántico Norte*, es una alianza militar intergubernamental basada en el *Tratado del Atlántico Norte* o *Tratado de Washington* firmado el 4 de abril de 1949. Según el manual para la formulación de estrategias nacional de ciberseguridad presentado por el Centro de Excelencia de Cooperación para la Ciberseguridad de la OTAN en CCDCOE (2012), una de las cuatro tendencia en la formulación de estrategias nacionales, en particular las definidas por los Estados Unidos y el Reino Unido, es el reconocimiento de que un conjunto diverso de las amenazas y los desafíos requiere una enfoque de gestión del riesgo. De igual manera, resalta la importancia de que dichas estrategias deben lidiar con un conjunto de dilemas, entre otros estimular la economía versus mejorar la seguridad nacional.

[17] El Consejo de la Industria de Tecnologías de la Información (Information Technology Industry Council –ITI–, en inglés) es la voz global del sector de tecnología y reúne a las empresas y organizaciones TIC más importantes en el mundo. ITI (2011) e ITI (2012) recomiendan que una estrategia nacional de ciberseguridad debe estar basada en la gestión de riesgo y se debe enfocar en la concientización y educación de todos los actores de interés con el fin de conocer cómo reducir los riesgos de seguridad digital, entre otras.

Figura 3.1. Evolución de la implementación de estrategias de seguridad digital en algunos países




Fuente: Adaptado de Hernández (2014)

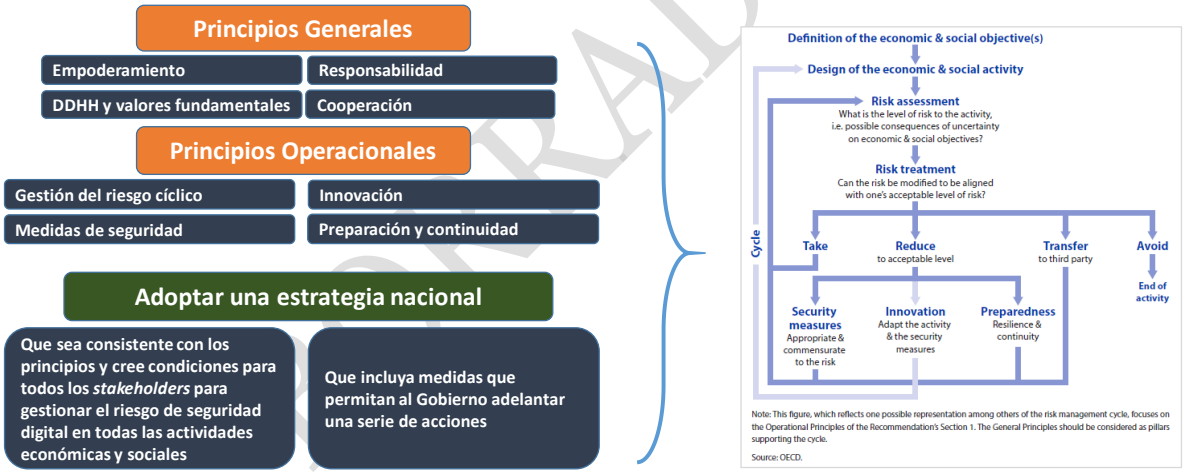
Al hacer revisión de diferentes políticas o estrategias nacionales en torno al tema, se puede concluir que las estrategias nacionales de ciberseguridad y ciberdefensa han evolucionado hacia estrategias nacionales de seguridad digital. Se pasó del diseño de estrategias de ciberseguridad y ciberdefensa que se centran principalmente en objetivos de defensa nacional y de seguridad nacional (lucha contra el crimen y la delincuencia) en el entorno digital, hacia el diseño de estrategias con un conjunto de principios y que se enmarca en la gestión de riesgos de seguridad digital, distinguiendo los objetivos de prosperidad económica y social con los objetivos de defensa del país y de lucha contra el crimen y la delincuencia en el entorno digital.

Esta es la posición de la OCDE, después de un trabajo de más de dos años de revisión y análisis de más de treinta años de experiencias respecto a la manera como se abordaron estos incidentes en el entorno digital en el pasado y respecto de los objetivos que los países habían planteado alcanzar. Como resultado de dicho trabajo, la OCDE adoptó el pasado 17 de septiembre de 2015, las *Recomendaciones sobre Gestión de Riesgos de Seguridad Digital para la Prosperidad Económica y Social*. Este documento provee guías para una 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.

La recomendación de la OCDE propone tanto a los países miembros como a los que no se han adherido, que: i) implementen un conjunto de principios en todos los niveles del Gobierno y de las organizaciones públicas, y ii) adopte una estrategia nacional para la gestión de riesgos de seguridad digital.

La Figura 3.2 presenta un resumen esquemático de las Recomendaciones de la OCDE sobre la Gestión de Riesgos de Seguridad Digital, en donde se resalta un conjunto de ocho principios; cuatro generales y cuatro operacionales; así como una serie de recomendaciones en torno a la adopción de una estrategia de gestión de riesgos digitales. En términos generales, se recomienda que la política aborde el riesgo de seguridad digital como un reto económico y social, creando condiciones para que todos los actores de interés gestionen el riesgo de seguridad digital en sus actividades económicas y sociales, fomentando la confianza en el entorno digital como medio para alcanzar los objetivos.

**Figura 3.2. Resumen esquemático de las Recomendaciones de la OCDE sobre la Gestión de Riesgos de Seguridad Digital**




Fuente: MINISTERIO TIC, 2015

De igual forma, la Recomendación es clara en aconsejar que la política que diseñen los países debe articular una visión general, soportada por el alto nivel del Gobierno, bajo un modelo institucional eficiente y de vinculación integral de todos y cada uno de los actores de interés, siendo éstos el mismo Gobierno nacional, las organizaciones públicas y privadas, la academia y la sociedad civil. Esta política nacional debe claramente distinguir los objetivos de prosperidad económica y social con los objetivos de defensa del país y de lucha contra el crimen y la delincuencia en el entorno digital.

La Figura 3.3 presenta el resumen de los principios propuestos por la OCDE para la construcción de una política de gestión de riesgos de seguridad digital. Se propone principios generales, tales como: i) conocimiento, capacidades y empoderamiento, ii) responsabilidad, iii) derechos humanos y valores fundamentales, y iv) cooperación. También propone principios operativos, tales como: i) evaluación de riesgos y ciclo de tratamiento, ii) medidas de seguridad, iii) innovación, y iv) preparación y continuidad.

**Figura 3.3. Principios propuestos por la OCDE para la construcción de una política de gestión de riesgos de seguridad digital**

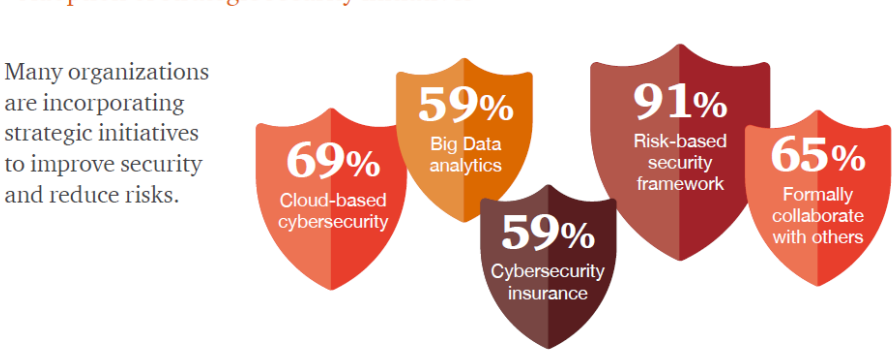

Fuente: MINISTERIO TIC, 2015

Finalmente, se resalta en la Figura 3.1 la adopción de una estrategia nacional de seguridad digital por parte de Francia, unos días después de publicada la recomendación objeto de análisis por parte de la OCDE. Dicho país definió una estrategia basada en unos principios fundamentales con cinco objetivos estratégicos, alrededor de la gestión de riesgos de seguridad digital. Este también ha sido el enfoque de los países que expidieron sus

estrategias incluso antes de la fecha de adopción de las recomendaciones. Tal es el caso de la República Checa, de Malta, de Portugal, entre otros.

Por otro lado, es importante resaltar que este cambio de enfoque se ha visto no sólo a nivel gubernamental sino a nivel de organizaciones privadas. PwC (2015) concluye, a partir de la encuesta: *The Global State of Information Security Survey 2016,* que los programa de seguridad digital eficaces han comenzado con una estrategia basada en los riesgos, encontrando que la gran mayoría de organizaciones (91%) han adoptado la gestión de riesgos de seguridad digital, bajo directrices como la ISO 27001, que permiten a las organizaciones identificar y priorizar los riesgos, y generar una mejor comunicación interna y externa. La Figura 3.4 y la Tabla 3.2 presentan los resultados de dicha encuesta.

**Figura 3.4. Adopción de estrategias de seguridad digital en organizaciones**




Fuente: PwC, 2015

**Tabla 3.2. Porcentaje de organizaciones que aplican estrategias de seguridad digital basadas en riesgos**

| Tipo de Organización encuestada | Porcentaje |
|---|---|
| Organizaciones de servicios financieros | 92% |
| Organizaciones públicas | 92% |
| Organizaciones de productos industriales | 86% |
| Organizaciones de entretenimiento, medios y comunicaciones | 94% |
| Organizaciones de consumo (minoristas) | 90% |
| Organizaciones de telecomunicaciones | 93% |
| **Total** | **91%** |

Fuente: PwC, 2015

## 4. DIAGNÓSTICO

Esta sección describe al avance que ha logrado el país en materia seguridad digital en Colombia bajo el enfoque establecido en el CONPES 3701 de 2011. También presenta el avance en el análisis de las experiencias internacionales en torno a la seguridad digital mediante el desarrollo de mesas de trabajo de alto nivel y plantea la problemática general con cinco problemas específicos los cuales se pretenden resolver mediante la implementación de una política nacional.

## 4.1. Avances de las recomendaciones establecidas en el CONPES 3701 de 2011

El Documento CONPES 3701 del año 2011, *Lineamientos de Políticas para Ciberseguridad y Ciberdefensa de Colombia*, estableció un marco de trabajo con el fin de abordar los temas de seguridad digital durante el periodo 2011 a 2015, formulando tres objetivos estratégicos: i) implementar la institucionalidad adecuada, i) brindar la capacitación especializada y ampliar las líneas de investigación en Ciberseguridad y Ciberdefensa, y iii) fortalecer la legislación y la cooperación internacional con el fin de forjar una línea base que facilite la construcción de la estrategia nacional. Respecto al cumplimiento de los indicadores establecidos para el seguimiento al mencionado CONPES, se evidencia el cumplimiento del 90% de las actividades propuestas en el plan de acción, de acuerdo a lo establecido por el Departamento Nacional de Planeación (DNP), mediante reporte realizado a corte del mes de julio de 2015.

- Institucionalidad

En lo que se refiere al cumplimiento de las actividades definidas en el documento CONPES citado, se fortaleció la institucionalidad en esta materia dado que el país cuenta hoy con el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), el Comando Conjunto Cibernético de las Fuerzas Militares (CCOC) y el Centro Cibernético Policial (CCP), además del equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT-PONAL). Además de esta institucionalidad, se han creado otras áreas en entidades existentes, tales como la Delegatura de Protección de Datos en la Superintendencia de Industria y Comercio (SIC), y la Subdirección de Seguridad y Privacidad de Tecnologías de Información adscrita a la Dirección de Estándares y Arquitectura de Tecnologías de la Información del Viceministerio Tecnologías y de Sistemas de Información del Ministerio de las Tecnologías de la Información y las Comunicaciones, así como las Unidades Cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana, entre otras organizaciones. También se creó la Comisión Nacional Digital y de Información Estatal mediante el Decreto 32 de 2013, el cual tiene como funciones, entre otras: i) asesorar al Gobierno Nacional en la posición que presentará ante los organismos encargados de asuntos relacionados con gobernanza en Internet, dominios, propiedad intelectual en la red, ciberseguridad, ciberdefensa, protección y privacidad de la información, y ii) generar lineamientos rectores para el Grupo de Respuesta a Emergencias Cibernéticas en Colombia.

- Capacitación

En lo que refiere al Ministerio de Defensa Nacional, es preciso decir que el equipo del ColCERT ha promovido la difusión de una cultura de Ciberseguridad y Ciberdefensa, así

como la gestión de incidentes en las entidades del Estado. Por su parte, el CCOC promovió el desarrollo y fortalecimiento de las capacidades de Ciberdefensa propias y de las Unidades Cibernéticas, así como 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, para dar cumplimiento a la misión institucional. Del mismo modo, en coordinación con el ColCERT, se viene adelantando el proceso para elaboración del catálogo de infraestructuras críticas, que permitirá coordinar y gestionar los planes y programas de protección y defensa de las mismas. Por su parte, el CCP está a cargo de la investigación y judicialización de delitos cibernéticos para lo cual cuentan con el personal especializado, equipos y laboratorios de última tecnología por lo que sus resultados operacionales dan muestra de las capacidades que se han desarrollado.

Así mismo, la capacitación y entrenamiento se ha fortalecido desde diferentes focos y 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. Igualmente, el país ha avanzado significativamente en la generación de oferta académica especializada en esta materia, que hoy cuenta con más de cincuenta programas académicos desde el nivel técnico hasta el de maestría, así como una amplia gama de cursos de educación no formal, que incluyen certificaciones de reconocimiento internacional.

- Legislación

Con respecto al fortalecimiento de la legislación, en Colombia existe un marco jurídico que incluye el reconocimiento de los datos e información como bien jurídico tutelado y cuenta con normas específicamente destinadas a aspectos tales como la protección de datos personales, regulación sobre protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad. Dentro de los aspectos incluidos en este marco, vale la pena resaltar que el Ministerio de las Tecnologías de la Información y las Comunicaciones estableció la implementación de la estrategia de Gobierno en Línea, la cual incorpora la adopción de *Sistemas de Gestión de Seguridad* de la Información en las entidades de la administración pública, lo cual ha contribuido a generar una dinámica que facilita la comprensión de la problemática asociada a los incidentes cibernéticos y su gestión, insumo importante para el desarrollo de capacidades institucionales del Estado en temas de ciberseguridad.

- Cooperación

Con respecto al fortalecimiento de la cooperación internacional, se han dado pasos muy significativos en materia de cooperación. Colombia, a través del Ministerio de Relaciones Exteriores, solicitó en 2013 formalmente la adhesión del país a la Convención de Europa sobré Cibercriminalidad, también conocido como Convenio de Budapest, que establece los principios de un acuerdo internacional sobre seguridad cibernética y la sanción de delitos de esta naturaleza. Con el Foro Económico Mundial, se estableció un convenio multilateral para buscar 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 de la OEA se ha logrado trabajar con grupos nacionales de "*Equipos de Respuesta a Incidentes*" (CSIRT), siendo Colombia parte de esta red de alerta hemisférica que proporciona formación técnica a personal especializado en estos temas, promueve el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética y fomenta el desarrollo de una cultura que permita su fortalecimiento en el continente. Con la OCDE, además del apoyo recibido como parte de la misión internacional, Colombia comparte plenamente las recomendaciones establecidas en el documento llamado: "Recomendaciones del Consejo sobre la gestión de riesgos de seguridad digital para la prosperidad económica y social".

En este mismo frente, el país ha suscrito acuerdos con empresas de la industria, para acceder a recursos y programas específicos en Ciberseguridad y Ciberdefensa, así como con organizaciones internacionales tales como el Antipishing Working Group, con el objeto de 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 incidentes cibernéticos. Estas alianzas también se han fortalecido en el contexto local con actores de la industria.

Otro aspecto a resaltar, es que Colombia cuenta con ocho (8) equipos de respuesta a incidentes de Seguridad Informática con membresía FIRST (por las siglas en inglés de Forum of Incident Response and Security Teams), siendo el tercer país del continente que más equipos de respuesta tiene inscritos, superado únicamente por Estados Unidos y Canadá.

En el ámbito regional, Colombia se ha posicionado como uno de los países que más ha avanzado en la región en aspectos relacionados con Ciberseguridad y Ciberdefensa, lo cual se refleja en estadísticas formales, tales como el Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT), en el cual el país se ubica actualmente 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 tales como Dinamarca, Egipto, Francia y España.

### 4.2. Mesas de trabajo de alto nivel para analizar el estado de la política vigente

No obstante los avances logrados mediante el desarrollo de las acciones establecidas en el Documento CONPES 3701 de 2011, todos estos resultados no pueden interpretarse como una capacidad suficiente y efectiva de preparación y de respuesta ante incidentes digitales, por cuanto se ha demostrado que países que están ubicados en mejores posiciones que Colombia han experimentado graves efectos por cuenta de la materialización de ataques en el ciberespacio, cada vez más frecuentes, así como sofisticados y motivados por intereses de diferente índole.

Sin lugar a dudas el Documento CONPES 3701 de 2011, dio lugar a una nueva dinámica en estos ámbitos, sin embargo, desde el año 2014, se ha buscado generar un renovado impulso mediante la formulación y desarrollo de nuevas políticas para el fortalecimiento de las habilidades adquiridas, así como el desarrollo de mayores capacidades para contrarrestar las amenazas en el ciberespacio, fortalecer la institucionalidad, actualizar y armonizar el marco normativo existente y fortalecer la relación y cooperación con actores e interesados a nivel nacional e internacional, entre otros frentes.

Es por esto que en el mes de febrero de 2014, el Presidente Juan Manuel Santos, consciente del incremento de incidentes relacionados con esta materia, solicitó la creación de una Comisión de Expertos nacionales de alto nivel liderada por los Ministros de Defensa Nacional, de Justicia y de Tecnologías de la Información y las Comunicaciones, que fueran apoyados por una comisión internacional, con el fin de trabajar en el fortalecimiento de la las políticas de Ciberseguridad y Ciberdefensa para el país, que permita brindar garantías de un ciberespacio seguro para el ciudadano y para el propio Estado, a fin de promover y fortalecer el desarrollo político, económico y social observando respeto por los derechos constitucionales, así como evaluando las vulnerabilidades a las que se encuentra expuesta Colombia en este campo y por lo tanto, la necesidad de adecuarse a los retos impuestos por los avances tecnológicos y las amenazas en el ciberespacio.

A partir del establecimiento de esta Comisión, los Ministerios a cargo convocaron la realización de mesas de trabajo con expertos nacionales e internacionales con el fin de adelantar un diagnóstico y contar con recomendaciones a partir de las cuales se construyan las bases de una nueva dirección de política para Colombia, teniendo como plataforma la finalización de la vigencia del Documento CONPES 3701 de 2011. El equipo de expertos nacionales contó con la participación de miembros de los Ministerios que conforman la Comisión, así mismo del ColCERT, del CCOC, del CCP y del sector público y privado, entre otros. El equipo de expertos internacionales 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 miembros del Foro Económico Mundial, de OCDE, del Consejo de Europa y de la INTERPOL.

En el marco de estas mesas de trabajo, se obtuvieron importantes insumos, evaluando las condiciones actuales de la política, con el fin de llevarla a un estado avanzado y equiparable a políticas en Ciberseguridad y Ciberdefensa a nivel mundial. En el caso de la mesa de expertos nacionales se orientó la revisión a los aspectos ya existentes de la política, como a los que aún se encuentran ausentes, girando en torno a cinco (5) 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.

Por su parte, la mesa internacional emitió recomendaciones enfocadas en la necesidad de: i) desarrollar una visión 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 política para la protección y defensa de la infraestructura crítica, siendo conscientes de la necesidad de fortalecer las capacidades del personal, así como también las físicas, lógicas, legales y de cooperación de las instituciones.

En conclusión, podría afirmarse que existe coincidencia en la necesidad de incorporar nuevos elementos a las estructuras institucionales, legislación y acciones existentes, y de incorporar lineamientos y directrices en lo relacionado con el respeto de los Derechos Humanos y aspectos de aplicación del Derecho Internacional Humanitario en el ciberespacio, de forma que pueda lograrse un entorno armónico sobre estos temas en el país y una adecuada articulación a nivel internacional.

Es así que a partir de las propuestas formuladas, se dio paso a la incorporación en las mesas de trabajo a otras entidades del orden gubernamental y privado, a representantes de la academia, organizaciones de la sociedad, empresas especializadas y autoridades en la materia, con el propósito de enriquecer la propuesta de plan de acción y verificar que las recomendaciones estratégicas que se recibieron estuvieran consideradas.

### 4.3. Problemática general

A partir del análisis que ha adelantado el Gobierno nacional y los cinco problemas que se describen a continuación, se concluye que Colombia no se cuenta con una visión general clara en torno a la seguridad digital y se hace necesario adelantar una gestión de riesgos de seguridad digital, situación que permite concluir que el país no cuenta con un entorno digital confiable y seguro, lo que conlleva a la materialización de riesgos asociados a amenazas e

incidentes que atenten contra la integridad de los ciudadanos, el Estado Social de Derecho, el ejercicio de los derechos fundamentales, la seguridad y la defensa nacional y, por tanto, contra la prosperidad económica y social del país.

Así, se genera la necesidad de establecer nuevos lineamientos de política y directrices de seguridad digital, teniendo en cuenta componentes como la gobernanza, la educación, la cooperación, la regulación, la investigación, la innovación, la diplomacia, el desarrollo, la protección, la seguridad y defensa de infraestructuras críticas, los intereses nacionales del Estado, entre otros, y enfocados en la ciudadanía, la sociedad en general, las Fuerzas Militares y los sectores públicos y privados, para que el país pueda contar con una estructura social y económica, que facilite el logro de los fines del Estado.

#### 4.3.1. Colombia realiza esfuerzos limitados para abordar los temas de seguridad digital, ya que no cuenta con una visión general clara del tema y no se basa en la gestión de riesgos.

El marco de trabajo establecido en el CONPES 3701 de 2011 se centró en la creación de un marco institucional que ha adelantado sus funciones y actividades de manera eficiente, en cabeza del Ministerio de Defensa Nacional. Si bien este esfuerzo ha permitido un posicionamiento importante a nivel internacional en torno al tema, se considera fundamental robustecer el liderazgo del Gobierno nacional y construir una nueva visión general clara bajo un enfoque integral, de acuerdo con las mejores prácticas internacionales para abordar los riesgos de seguridad digital. Esta situación genera que los lineamientos de política a la fecha vigentes deban ser modificados.

Actualmente, se presentan las siguientes evidencias respecto de esta problemática:

- *Colombia no cuenta con un organismo o un responsable de coordinación nacional en materia de seguridad digital.*

- *No se ha diseñado una Agenda Nacional de Seguridad Digital en la cual se vincule a todas las entidades del sector público así como al resto de actores de interés.*

- *Actualmente existe un marco legal y regulatorio disperso respecto de los temas de seguridad digital que dificultan la coordinación, el direccionamiento, la homogenización y articulación de procesos, planes y programas que permitan la coordinación y la respuesta inmediata a la gestión de incidentes en el entorno digital de tipo nacional, ocasionando por una parte, innumerables riesgos a todos los actores de interés*. La Tabla 4.1 presenta un marco normativo nacional disperso respecto de aspectos vinculados con la seguridad digital que deben ser revisados teniendo en cuenta las nuevas condiciones del entorno digital en el país.

## Tabla 4.1. Marco normativo nacional

| Norma | Contenido |
|---|---|
| Constitución Nacional | 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. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley. |
| 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. |
| 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 TIC-, 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. Por otra parte, esta Ley contempla en el artículo 7, para los proveedores o servidores, administradores y usuarios de redes globales de información, determinadas prohibiciones como: alojar en su propio sitio imágenes, textos o archivos que impliquen actividades sexuales con menores; alojar en su propio sitio material pornográfico que contenga imágenes o videos, en los cuales las personas filmadas o fotografiadas sean menores de edad; alojar en sitio links sobre páginas que remitan a temáticas de pornografía infantil. Finalmente, la Ley en el artículo 8 contempla que los proveedores, administradores y usuarios de redes globales de información deberán: denunciar la difusión de material pornográfico con menores de edad. |
| 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) | En el año 2009 se expide la Ley 1273 "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". Se crean los siguientes tipos penales: Capítulo I – "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", este capítulo tipifica las siguientes conductas penales: Acceso Abusivo a un sistema informático, obstaculización ilegítima de sistema informático o de red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales. Capítulo II – "De los atentados informáticos y otras infracciones", este capítulo tipifica las siguientes conductas: hurto por medios informáticos y semejantes, transferencia no consentida de activos. |
| 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 Tecnologías de la Información y las Comunicaciones, 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. Finalmente, en el artículo 19 se establece que el documento de criterios de clasificación de páginas en internet con contenidos de pornografía infantil y de recomendaciones al gobierno será actualizado cada dos años, a fin de revisar la vigencia doctrinal de sus definiciones, actualizar los criterios sobre tipos y efectos de la pornografía infantil, con el fin de asegurar la actualidad de los marcos tecnológicos de acción. |
| 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 1453 de 2011 (Estatuto de seguridad ciudadana) | El Art. 236 establece que cuando el fiscal tenga motivos razonables, para inferir que el indicado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a la policía la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado. La aprehensión que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados, de ser el caso. |

| Norma | Contenido |
|---|---|
| **Ley 1480 de 2011 (Estatuto del Consumidor - Comercio electrónico y publicidad)** | La Ley 1480 en el artículo 5, 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. Adicionalmente, el artículo 27 establece que el consumidor tiene derecho a exigir a costa del productor o proveedor constancia de toda operación de consumo que realice. La factura o su equivalente, expedida por cualquier medio físico, electrónico o similar podrán hacer las veces de constancia. |
| **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 PRST 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. Para lo cual, deben informar en su página web las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls. Filtros antivirus y la prevención del spam, phishing, malware entre otros; no obstante la responsabilidad de los PRST no cubre los equipos del cliente, puesto que los mismos son controlados directamente por el usuario del servicio. Adicionalmente, los PRST que ofrezcan acceso a internet deberán implementar modelos de seguridad, de acuerdos con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, en línea con los marcos de seguridad definidos por la UIT, en lo relativo a las recomendaciones pertenecientes a las series X.800, y en relación con los siguientes aspectos: autenticación (UIT X.805 y UIT X.811), acceso (UIT X.805 y UIT X.812), no repudio (UIT X.805 y UIT X.813), confidencialidad de datos (UIT X.805 y UIT X.814), integridad de datos (UIT X.805 y UIT X.815) y disponibilidad (UIT X.805). Finalmente se establece, los PRST a través de redes móviles, deberán implementar modelos de seguridad que eviten el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada de la comunicación, utilizando modelos de cifrados, firmas digitales y controles de acceso descritos en las recomendaciones UIT X.1121 y X.1122. |
| **Resolución CRC 3502 de 2011 (Neutralidad de Internet)** | A través de la Resolución 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 (Plan Nacional de Desarrollo 2010 – 2014). Esta resolución, contempla en el artículo 3 los principios de libre elección, no discriminación, transparencia e información, que deben aplicar los PRST 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. |
| **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 PRST 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.<br>Adicionalmente, el Decreto establece que una vez cumplido los requisitos legales, los PRST deben suministrar a la Fiscalía General de la Nación de forma inmediata, los datos del suscriptor, tales como identidad, dirección de facturación y tipo de conexión, los cuales deben estar actualizados y deben ser conservados por 5 años. En el año 2012 se interpuso una demanda de Nulidad contra la expresión "o demás autoridades competentes" contenida en el artículo 4 del Decreto 1704/2012. En escrito separado se solicitó la suspensión provisional de la expresión mencionada, la cual fue concedida mediante Auto del 31 de julio de 2013, y confirmada en el resuelve del recurso de súplica interpuesto por el MINISTERIO TIC, el 3 de abril de 2014. Por lo anterior, actualmente se encuentra suspendida únicamente la expresión" o demás autoridades competentes" contenida en el artículo 4 del Decreto 1704. No obstante, es de notar que la Ley 1453 de 2011 (Reforma al Código Penal) fue declarada exequible, y el artículo 52 que modifica el art. 235 de la Ley 906 de 2004, dispone la interceptación de comunicaciones que se cursen por cualquier red, según orden de |
| **Decreto 2758 de 2012 (Modifica la Estructura del Misterio de Defensa)** | Se reestructura la organización del Ministerio de Defensa, 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. |
| **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. En efecto, el Decreto expedido tiene algunas características que benefician el uso de los medios electrónicos: 1. Se definen los criterios de confiabilidad y apropiabilidad en el uso de los mecanismos de autenticación. 2. Se fija 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. 3. Se instaura el uso de la firma electrónica mediante acuerdo de las partes de una relación jurídica, pero se establece también de manera clara que estos mecanismos deben garantizar las condiciones de confiabilidad, y en ese orden de ideas, quien predisponga métodos de autenticación, como bancos o entidades financieras, deberán garantizar las condiciones de autenticidad e integridad definidas como alcance del concepto de confiabilidad. Esto redunda en la seguridad de consumidores y de usuarios finales. 4. Se destaca la neutralidad tecnológica de los diferentes mecanismos de |

| Norma | Contenido |
|---|---|
| | autenticación, lo que posibilitará el uso de cualquier tipo de tecnología para estos efectos, con plenas consecuencias jurídicas, y de igual forma se reitera que la firma digital es un mecanismo neutro tecnológicamente. 5. Se definen criterios para determinar la seguridad de la firma electrónica, haciendo alusión a la necesidad de contar con auditorías técnicas o la intervención de terceros especializados para definir las condiciones de confiabilidad y apropiabilidad. 6. Los mecanismos de autenticación deben ser confiables y seguros independiente de quién los provea, y deberán probarse en cualquier momento esas condiciones. 7. Cuando la firma electrónica sea por un acuerdo de voluntades, este método de autenticación será aplicable interpartes, con lo cual no podrá hacerse oponible a terceros, por ejemplo en la circulación de títulos valores electrónicos, donde ya hay un régimen definido para el uso de documentos electrónicos transferibles. |
| Resolución 3933 de 2013 Del Ministerio de Defensa (Crea y organiza grupos internos de trabajo) | 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/sectoriales para la 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) | "A través de este Decreto se reglamenta parcialmente la Ley 1581 de 2012". El decreto tiene como objetivo facilitar 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 (Marco jurídico que para desempeño de funciones de los organismos de inteligencia y contrainteligencia– Protección a las bases de datos) | Esta Ley tiene por objeto fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal, así mismo esta Ley establece los límites y fines de las actividades de inteligencia y contrainteligencia, los mecanismos de control y supervisión y la regulación de la protección a las bases de datos. En el marco de la Ley hay diversas autoridades que manejan inteligencia tales como UIAF, POLFA, DIPOL son organismos con función de policía judicial. El Art. 17 establece obligaciones en relación al monitoreo del espectro y la interceptación de comunicaciones. El Art. 44 consagra el deber de colaboración de los operadores de comunicaciones para entregar a los organismos de inteligencia determinados datos como: el historial de comunicaciones, los datos técnicos de identificación de los usuarios, así como la localización de las celdas en que se encuentran las terminales. Adicionalmente, los operadores se encuentran obligados a informar al MINISTERIO TIC cualquier modificación en la tecnología de sus redes que impida la interceptación de comunicaciones. |
| Decreto 0032 de 2013 (Creación de la Comisión Nacional Digital y de Información Estatal) | El MINISTERIO TIC en cumplimiento de los lineamientos señalados en el Documento CONPES 3701 DE 2011 , 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. Adicionalmente, dicha Comisión debe emitir los lineamientos rectores del Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Defensa Nacional y asesorar al Gobierno Nacional en materia de políticas para el sector de ciberseguridad. |
| Decreto 333 de 2014 (Habeas Data) | Este Decreto define el régimen de acreditación de las entidades de certificación en desarrollo de lo que consagra el Articulo 16022 del Decreto Ley 19 de 2012. |
| Decreto 857 de 2014 | 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. |

Fuente: Adaptado de CRC (2015)



- *Los lineamientos de política a la fecha vigentes están orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país y no distingue suficientemente los objetivos de prosperidad económica y social con los objetivos de defensa del país y de lucha contra el crimen y la delincuencia en el entorno digital.*

- *Los lineamientos de política a la fecha vigente no incorporan el enfoque de gestión de riesgos y deben actualizarse con los nuevos conceptos asociados a la seguridad digital, de acuerdo con la dinámica que se ha presentado a nivel internacional en torno al tema.*

### 4.3.2. Colombia no ha vinculado integralmente a todos los actores de interés para gestionar de manera sistemática los riesgos de seguridad digital con el fin de

### maximizar las oportunidades en el desarrollo de todas las actividades socioeconómicas en el entorno digital

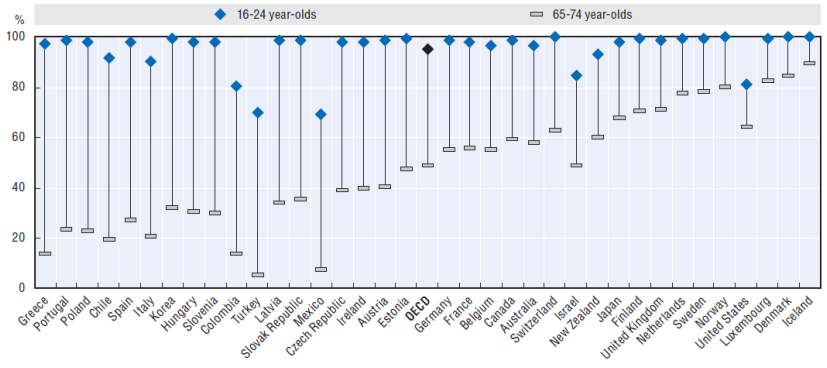
Como ya se mencionó, el marco de trabajo establecido en el CONPES 3701 de 2011 sólo se centra en los objetivos de defensa nacional y de seguridad nacional (lucha contra el crimen y la delincuencia) en el entorno digital y no distingue el objetivo de prosperidad económica y social. Con respecto al objetivo de prosperidad económica y social, se debe abordar el riesgo de seguridad digital como un reto económico y social, creando condiciones para que todos los actores de interés gestionen el riesgo de seguridad digital en sus actividades económicas y sociales, fomentando la confianza en el entorno digital como medio para alcanzar los objetivos tanto del Plan Nacional de Desarrollo 2014-2018 "*Todos por un nuevo país – Paz, Equidad y Educación*" como del Plan Vive Digital 2014-2018.

Actualmente, se presentan las siguientes evidencias respecto de esta problemática:

- *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*

Según OCDE (2015b), la difusión de Internet entre los adultos en los países OCDE en 2014 fue generalizada con un 82% de la población adulta accediendo a Internet y más del 75% usándolo diariamente. En la Figura 4.1 se aprecia que existen brechas entre los distintos grupos de edad y niveles de educación respecto al uso de Internet en dichos países. En la mayoría de ellos, el uso de los jóvenes es casi universal, pero hay grandes diferencias con las generaciones mayores. Más del 95% de los individuos entre los 16 y 24 años de edad en el área OCDE usaron Internet en 2014, frente a menos del 49% entre los 65 y 74 años de edad.

**Figura 4.1. Brecha en el uso de Internet por edades en 2014 (%)**




Fuente: OCDE (2015b)

En contraste con la situación en dichos países OCDE, tanto en la Figura 4.1 como en la Tabla 4.2, se aprecia que el 79,4% de los jóvenes entre 12 y 24 años usaron Internet en 2014 en Colombia. De igual forma, se aprecia que la brecha en el uso de Internet entre los individuos jóvenes y las generaciones mayores en Colombia (65 puntos porcentuales) es considerablemente mayor que la brecha promedio para los países OCDE. Se aprecia que en promedio tan sólo el 52,6% de los ciudadanos colombianos usaron Internet en cualquier lugar durante el año 2014.

**Tabla. 4.2. Personas por rango de edad que usaron Internet en cualquier lugar en Colombia entre 2010 y 2014 (%)**

| | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| **Total personas** | **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 Encuesta de Calidad de Vida (ECV) para los años 2010, 2011, 2012, 2013 y 2014

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

**Tabla. 4.3. Frecuencia de uso del Internet y del Teléfono Móvil**

| | Internet | | | | | Móvil | |
|---|---|---|---|---|---|---|---|
| | 2010 | 2011 | 2012 | 2013 | 2014 | 2013 | 2014 |
| Todos los días de la semana | 47,0 | 47,1 | 46,0 | 48,3 | 51,1 | 63,9 | 64,6 |
| Al menos una vez a la semana pero no cada día | 40,8 | 41,9 | 42,6 | 41,6 | 41,8 | 30,6 | 31,0 |
| Al menos una vez al mes pero no cada semana | 9,8 | 9,2 | 11,3 | 8,8 | 6,2 | 5,2 | 4,0 |
| Al menos una vez al año pero no cada mes | 2,5 | 1,8 | - | 1,3 | 0,9 | 0,3 | 0,3 |

Fuente: DANE Encuesta de Calidad de Vida (ECV) para los años 2010, 2011, 2012, 2013 y 2014

Por su parte, en la Tabla 4.4 se aprecia que según datos de la Encuesta de Calidad de Vida del DANE tan sólo el 38% de los hogares posee conexión a Internet en Colombia a 2014. Según EURACTIV (2015), el 81% de los hogares en Europa tienen acceso a Internet.

**Tabla. 4.4. Proporción de hogares que poseen conexión a Internet y por tipo de conexión**

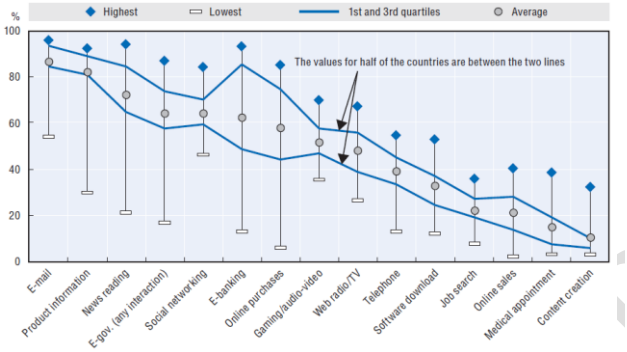
| | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| Hogares con conexión a Internet | 19,2 | 23,4 | 32,1 | 35,7 | 38,0 |
| Hogares con conexión a Internet fijo | - | - | 25,1 | 29,1 | 31,7 |
| Hogares con conexión a Internet móvil | - | - | 9,9 | 10,9 | 16,0 |
| Hogares con conexión a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

Fuente: DANE Encuesta de Calidad de Vida (ECV) para los años 2010, 2011, 2012, 2013 y 2014

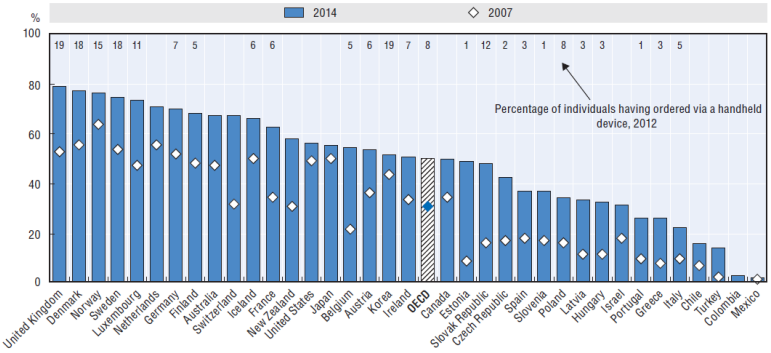
Según OCDE (2015b), en promedio el 87% de los usuarios de Internet en los países OCDE envío correos electrónicos durante los años 2013 y 2014. En la Figura 4.2 se aprecia que el 82% utilizó el Internet para obtener información sobre bienes y productos y el 72% consultó noticias en línea. Adicionalmente, la mitad de los individuos en los países OCDE (58%) compró / ordenó productos en línea y sólo el 21% vendió productos a través de Internet. De igual manera, actividades como el envío de mensajes de correo electrónico, la búsqueda de información de productos o las redes sociales mostraron poca variación entre todos los países.

**Figura 4.2. Actividades en línea por individuos en países OCDE en 2013-2014 (%)**

**Porcentaje de usuarios de Internet desarrollando cada actividad**




**% de individuos que compran / ordenan productos o servicios online**




Fuente: OCDE (2015b)

En Colombia, la situación fue muy diferente respecto de aquella reflejada en los países OCDE para el 2014. En dicho año, el 62% de los individuos utilizó el Internet para obtener información, sólo el 10% consultó noticias en línea y el 5,6% compró / ordenó productos en línea. Mientras que en los países OCDE más del 60% de los individuos usaron la banca electrónica, según los datos de la ECV del DANE tan sólo el 6,4% de los individuos en Colombia lo hicieron.

**Tabla 4.5. Proporción de personas en Colombia que usaron Internet según actividad de uso (%)**

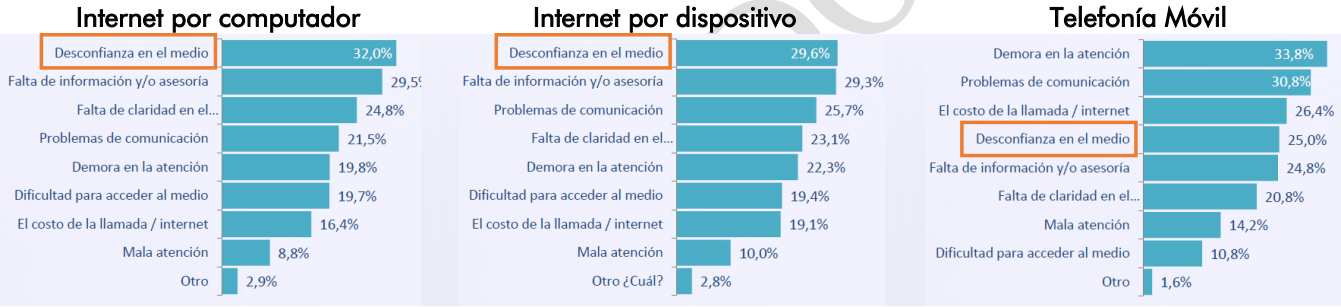
| Actividad en línea | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| Redes Sociales | | | 55,6 | 62,4 | 63,2 |
| Obtener información | 74,3 | 74,3 | 56,5 | 52,9 | 61,7 |
| Correo y mensajería | 76,2 | 78,7 | 62,4 | 58,5 | 57,6 |
| Educación y aprendizaje | 64,1 | 62,1 | 42,0 | 44,1 | 36,7 |
| Actividades de entretenimiento | 62,6 | 65,7 | 39,5 | 40,6 | 28,7 |
| Consulta de medios de comunicación | | | | 17,2 | 9,9 |
| Banca electrónica | 10,1 | 9,4 | 5,8 | 6,5 | 6,4 |

| Actividad en línea | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| Comprar / 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 Encuesta de Calidad de Vida (ECV) para los años 2010, 2011, 2012, 2013 y 2014

El bajo uso del entorno digital y por ende de la digitalización por parte de los ciudadanos se debe a la existencia de barreras en cuento al uso de medios electrónicos. INFOMETRIKA (2014) adelantó una encuesta para el MINISTERIO TIC 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 en Colombia durante 2014. Se encontró que la principal barrera de los ciudadanos para realizar trámites mediante internet por computador o por cualquier otro dispositivo, así como por la telefonía móvil, es la desconfianza en el medio.

**Figura 4.3. Percepción de uso de medios electrónicos por parte de los ciudadanos para realizar trámites y servicios en línea en Colombia durante 2014**

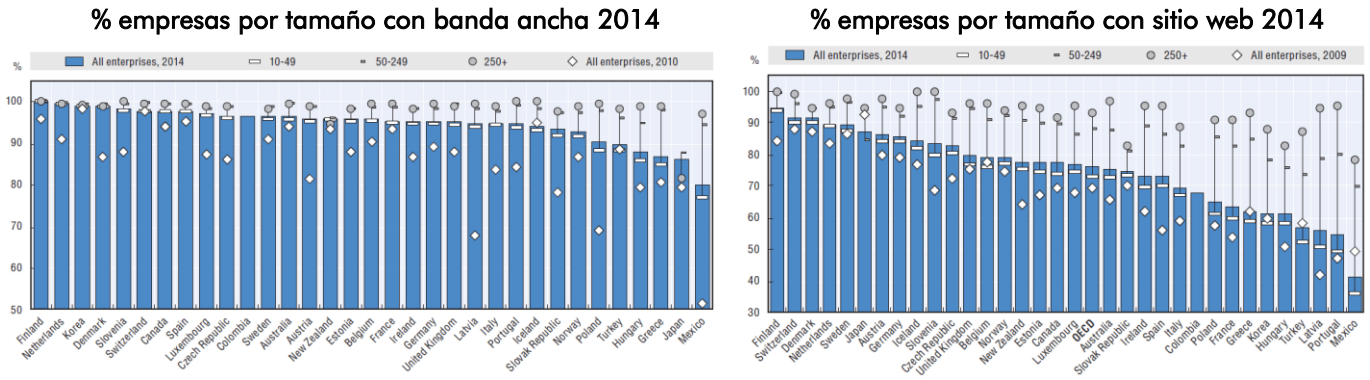



Fuente: INFOMETRIKA (2014)

- *Aunque hoy los empresas colombianas están más digitalizadas, actualmente no están maximizando los beneficios económicos y las oportunidades potenciales que brinda la economía digital*

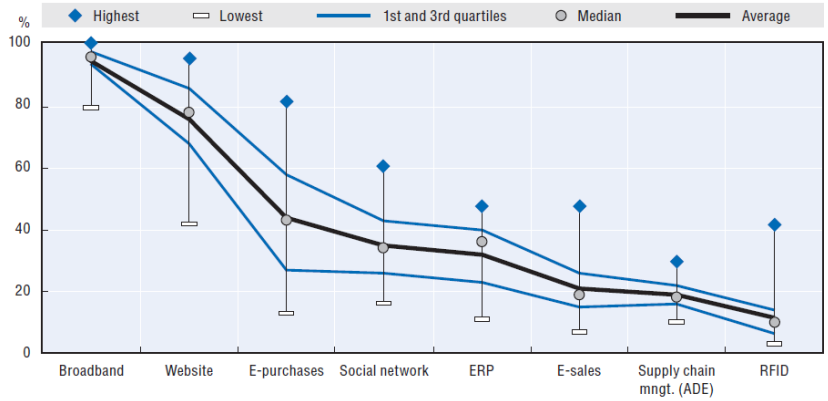
Según OCDE (2015b), la gran mayoría de las empresas hoy en día hacen uso de las TIC. En 2014, en promedio el 95% de empresas de los países de la OCDE tenían una conexión de banda ancha (esto incluye tanto conexiones de Internet fijo y móvil con una velocidad de descarga de al menos 256 Kbps), por encima del 86% en 2010. De igual manera, más del 76% de todas las empresas de la OCDE tenía un sitio web o página de inicio en el 2014, frente al 70% en el 2009. La proporción de empresas con una presencia en la web va desde más del 90% en Dinamarca, Finlandia y Suiza hasta el 54% en Portugal y el 42% en México.

Figura 4.4. Adopción y uso TIC por empresas en países OCDE 2014




Fuente: OCDE (2015b)

Figura 4.5. Actividades en línea por empresas en países OCDE en 2014 (%)




Fuente: OCDE (2015b)

Según la Encuesta Anual Manufacturera (EAM), la Encuesta Anual de Comercio (EAC) y la Encuesta Anual de Servicios (EAS) del DANE, en Colombia casi todas las empresas del sector Industria, del sector Comercio y del sector Servicios usaron internet en 2014. En las empresas de los sectores Industrial y Comercio, se aprecia que cerca de la mitad del personal ocupado utilizó Internet en su trabajo mientras que la gran mayoría del personal en las empresas del sector Servicios lo hizo durante el 2014. En contraste con la situación presentada en los países OCDE, el 67% de las empresas del sector Industria y el 60% de las empresas del sector Comercio tenían un sitio web o página de inicio en el 2014. Respecto a los usos de Internet por parte de las empresas, se destacan proporciones similares a las reportadas para los países OCDE. Por ejemplo, en Colombia

## Tabla 4.6. Adopción y uso TIC por empresas del sector industria, comercio y servicios en Colombia 2010 a 2014

| | Sector Industria | | | | | Sector Comercio | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 2010 | 2011 | 2012 | 2013 | 2014 | 2010 | 2011 | 2012 | 2013 | 2014 |
| Número de empresas encuestadas | 9.452 | 9.105 | 8.916 | 8.659 | 8.357 | 6.061 | 5.981 | 5.913 | 6.763 | 7.846 |
| Número de empresas usando Internet (%) | 98,0 | 99,7 | 98,8 | 99,0 | 99,2 | 98,6 | 98,9 | 99,2 | 99,6 | 99,5 |
| Número de empresas con página o sitio web (%) | 52,0 | 60,7 | 62,9 | 65,8 | 67,3 | 45,2 | 46,8 | 56,8 | 60,2 | 61,7 |
| % de personal ocupado que utilizó internet para su trabajo | 31,5 | 32,8 | 36,3 | 41,0 | 44,7 | 40,0 | 45,4 | 56,0 | 58,3 | 60,4 |
| % usando Internet mediante modem de cable / FO - Canal dedi | 46,3 | 47,3 | 49,1 | 50,7 | 54,0 | 29,4 | 36,0 | 37,9 | 39,3 | 34,5 |
| % con velocidad de conexión superior a 2048 Kbps | 27,4 | 33,6 | 36,1 | 46,6 | 54,7 | 35,3 | 40,6 | 41,3 | 55,3 | 62,1 |
| % que usaron plataforma electrónica para comprar insumos | - | - | 25,4 | 28,6 | 29,3 | - | - | 34,5 | 34,9 | 38,2 |
| % que usaron plataforma electrónica para vender productos | - | - | 24,5 | 27,1 | 26,9 | - | - | 20,3 | 17,8 | 20,3 |
| Compras a través de comercio electrónico vs compras totales | - | - | 8,0 | 6,7 | 24,8 | - | - | 16,4 | 13,7 | 14,7 |
| Ventas a través de comercio electrónico vs ventas totales | - | - | 10,8 | 9,0 | 19,8 | - | - | 6,4 | 5,2 | 5,8 |

| | Sector Servicios | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Número de empresas encuestadas | | Número de empresas usando Internet (%) | | % de empresas con página o sitio web | | % de personal ocupado que utilizó internet para su | | % que usaron plataforma electrónica para comprar | | % que usaron plataforma electrónica para vender productos | | Compras a través de comercio electrónico vs compras totales | | Ventas a través de comercio electrónico vs ventas totales | |
| | 2013 | 2014 | 2013 | 2014 | 2013 | 2014 | 2013 | 2014 | 2013 | 2014 | 2013 | 2014 | 2013 | 2014 | 2013 | 2014 |
| Correo y almacenamiento | 431 | 430 | 99,8 | 99,8 | 84,9 | 85,8 | 58,4 | 61,2 | 39,8 | 43,4 | 30,9 | 30,3 | 8,7 | 9,0 | 6,5 | 6,3 |
| Alojamiento y servicios de comida | 675 | 708 | 100 | 99,7 | 81,3 | 84,2 | 41,3 | 45,9 | 48,1 | 52,3 | 54,8 | 59,3 | 13,0 | 13,4 | 11,1 | 12,5 |
| Actividades de edición | 211 | 216 | 99,1 | 99,5 | 79,1 | 81,5 | 71,8 | 77,6 | 34,9 | 36,7 | 37,3 | 37,2 | 5,2 | 5,3 | 7,9 | 6,5 |
| Producción de películas | 19 | 19 | 100 | 100 | 100,0 | 100,0 | 60,5 | 79,5 | 52,6 | 57,9 | 52,6 | 57,9 | 7,8 | 11,6 | 4,9 | 5,7 |
| Programación, transmisión y agencias de no | 46 | 47 | 100 | 100 | 97,8 | 95,7 | 70,4 | 92,6 | 41,3 | 51,1 | 28,3 | 34,0 | 1,9 | 5,1 | 5,1 | 5,6 |
| Telecomunicaciones | 174 | 184 | 100 | 100 | 83,9 | 82,1 | 80,9 | 85,1 | 55,2 | 57,6 | 29,9 | 29,9 | 13,0 | 13,2 | 16,8 | 15,6 |
| Sistemas informáticos y procesamiento de da | 263 | 273 | 100 | 100 | 95,4 | 95,6 | 89,2 | 91,2 | 57,8 | 64,8 | 37,3 | 40,7 | 21,0 | 23,9 | 18,1 | 20,0 |
| Actividades inmobiliarias | 141 | 220 | 100 | 100 | 66,7 | 75,0 | 60,9 | 65,1 | 31,2 | 41,8 | 24,1 | 30,0 | 8,1 | 9,1 | 4,4 | 8,0 |
| Profesionales, científicas y técnicas | 841 | 831 | 99,8 | 100 | 84,2 | 87,7 | 70,3 | 73,7 | 49,3 | 53,1 | 26,5 | 29,2 | 9,8 | 11,3 | 4,0 | 3,8 |
| Alquiler y arrendamiento | 73 | - | 98,6 | - | 94,5 | - | 60,5 | - | 44,4 | - | 38,9 | - | 7,1 | | 9,8 | - |
| Agencias de viaje | 91 | 88 | 100 | 100 | 94,5 | 97,7 | 95,3 | 95,8 | 59,3 | 76,1 | 73,6 | 81,8 | 21,7 | 22,8 | 31,8 | 36,3 |
| Empleo, seguridad y aseo de edificios | 1140 | 1122 | 99,5 | 99,6 | 65,0 | 68,5 | 20,2 | 24,2 | 32,8 | 35,7 | 25,3 | 29,5 | 6,2 | 7,7 | 6,6 | 6,3 |
| Administrativas y de apoyo a oficina | 176 | 179 | 99,4 | 100 | 80,1 | 83,2 | 70,8 | 73,0 | 38,9 | 47,5 | 27,4 | 30,2 | 6,4 | 8,9 | 3,4 | 3,7 |
| Educación superior privada | 168 | 168 | 100 | 100 | 99,4 | 98,8 | 94,0 | 96,4 | 54,2 | 62,5 | 54,8 | 58,9 | 15,5 | 18,0 | 19,8 | 19,6 |
| Salud humana privada | 797 | 800 | 100 | 100 | 75,5 | 80,6 | 65,7 | 72,2 | 35,4 | 50,1 | 19,9 | 25,5 | 10,6 | 13,0 | 4,6 | 5,1 |
| Otras actividades de servicios personales | 113 | 112 | 100 | 100 | 81,4 | 83,9 | 60,2 | 64,9 | 46,0 | 56,3 | 31,0 | 36,6 | 17,5 | 16,7 | 7,5 | 8,4 |
| | 5359 | 5397 | | | | | | | | | | | | | | |

Fuente: DANE Encuesta Anual Manufacturera (EAM), Encuesta Anual de Comercio (EAC) y Encuesta Anual de Servicios (EAS) para los años 2010, 2011, 2012, 2013 y 2014

Según OCDE (2015b), al igual que con el acceso de banda ancha, la presencia en la web es menor entre las pequeñas empresas (MIPYMES). En 27 de los 32 países de la OCDE el 90% o más de las empresas grandes tienen un sitio web, mientras que la presencia en la web en las MIPYME oscila entre el 90% o más en Dinamarca, Finlandia y Suiza, y el 50% o menos en Letonia, Portugal y México. En la Tabla 4.7 se aprecia que tan sólo el 25% de las MIPYMES de los sectores industrial, comercial y de servicios, tuvieron acceso o usaron Internet en 2014 y tan sólo el 6% tienen presencia en la web, según los datos de la Encuesta de Microestablecimientos del DANE. También se aprecia que los usos principales de Internet fue enviar o recibir correo electrónico o el servicio al cliente. Tan sólo el 13,5% compró a proveedores por Internet mediante una plataforma electrónica y el 9% vendió productos a clientes por Internet mediante una plataforma electrónica, panorama que no difiere de aquel en Europa. Según EURACTIV (2015), el 15% de las MIPYMES en Europa vendió productos en línea en comparación con el 35% de las empresas más grandes, mientras que el 7% de las MIPYMES en dicha región compró productos en línea en comparación con el 21% de aquellas más grandes.

**Tabla 4.7. Adopción y uso TIC por Micro, Medianas y Pequeñas empresas (MIPYMES) del sector industria, comercio y servicios en Colombia 2012 a 2014**

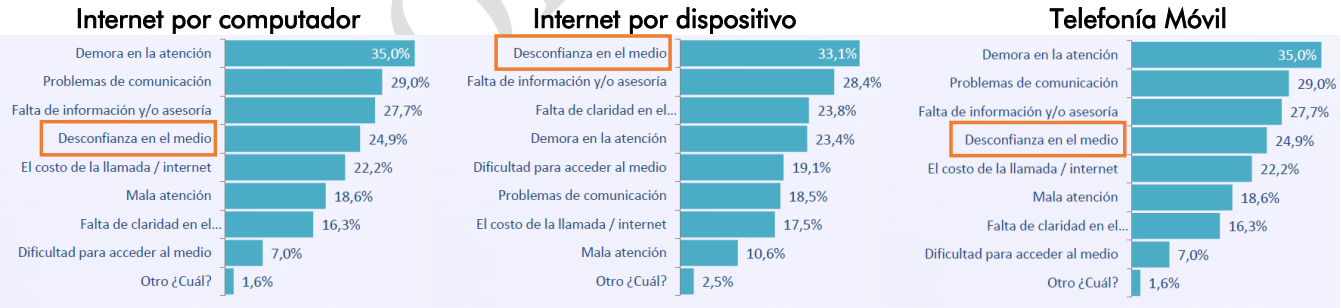
| | Total | | | Comercio | | | Industria | | | Servicios | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2012 | 2013 | 2014 | 2012 | 2013 | 2014 | 2012 | 2013 | 2014 | 2012 | 2013 | 2014 |
| Número de MIPYMES encuestadas | 36.954 | 36.841 | 37.030 | 22.968 | 23.017 | 22.123 | 3.936 | 3.838 | 3.822 | 10.050 | 9.986 | 11.085 |
| Proporción de microestablecimientos que tenían acceso o usaron Internet | 20,4 | 22,0 | 25,1 | 12,1 | 13,5 | 17,8 | 29,2 | 31,3 | 31,8 | 35,9 | 38,0 | 37,6 |
| Proporción de microestablecimientos con página o sitio web | 3,1 | 3,6 | 6,0 | 2,0 | 2,4 | 4,8 | 5,0 | 5,6 | 8,1 | 4,9 | 5,7 | 7,8 |
| Proporción de microestablecimientos con precencia en redes sociales | - | - | 3,9 | - | - | 3,0 | - | - | 5,6 | - | - | 5,3 |
| Porcentaje del personal ocupado de microestablecimientos que usaba Internet | 17,0 | 18,8 | 21,7 | 10,7 | 12,2 | 16,7 | 18,0 | 20,3 | 20,4 | 27,6 | 29,9 | 30,6 |
| % con velocidad de conexión ancho de banda fija superior a 4 MB | - | 17,6 | 39,0 | - | 16,1 | 34,6 | - | 17,5 | 41,1 | - | 18,9 | 42,5 |
| % con velocidad de conexión ancho de banda móvil 4G | 0,6 | 1,6 | 2,1 | | | | | | | | | |

| | Total | | Comercio | | Industria | | Servicios | |
|---|---|---|---|---|---|---|---|---|
| | 2013 | 2014 | 2013 | 2014 | 2013 | 2014 | 2013 | 2014 |
| Enviar o recibir correo electrónico | 94,4 | 92,2 | 92,8 | 91,3 | 97,3 | 96,0 | 94,9 | 91,8 |
| Servicio al cliente | 51,0 | 53,8 | 49,5 | 52,6 | 58,8 | 56,5 | 49,7 | 54,2 |
| Busqueda de información sobre bienes y servicios | 62,1 | 50,9 | 59,7 | 49,1 | 64,1 | 49,4 | 63,4 | 53,0 |
| Uso de aplicaciones | 50,1 | 47,3 | 50,5 | 46,2 | 50,1 | 52,0 | 49,7 | 47,0 |
| Banca electrónica y otros servicios financieros | 30,8 | 36,8 | 30,4 | 39,1 | 31,3 | 33,5 | 30,9 | 35,6 |
| Búsqueda de información de dependencias oficiales y autoridades | 30,8 | 30,5 | 24,4 | 25,2 | 24,6 | 21,2 | 38,0 | 38,3 |
| Llamadas telefónicas por internet/VoIP o uso de videoconferencias | 13,4 | 14,7 | 11,2 | 13,7 | 7,8 | 11,3 | 17,0 | 16,7 |
| Comprar a proveedores por Internet mediante una plataforma electrónica | 10,1 | 13,5 | 14,0 | 17,7 | 10,1 | 14,3 | 6,9 | 9,2 |
| Transacciones con organismos gubernamentales | 12,1 | 12,1 | 9,4 | 10,9 | 10,0 | 9,1 | 15,0 | 14,1 |
| Distribuir productos en línea | 9,1 | 10,3 | 11,6 | 13,0 | 9,9 | 11,9 | 6,9 | 7,2 |
| Vender productos a clientes por Internet mediante una plataforma electrónica | 7,3 | 8,9 | 9,3 | 10,6 | 9,0 | 11,2 | 5,2 | 6,7 |
| Capacitación de personal | - | 9,9 | - | 8,4 | - | 9,1 | - | 11,5 |

Fuente: DANE Encuesta de Microestablecimientos 2012, 2013 y 2014

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 lo encontrado para los ciudadanos, se encontró que una de las principales barreras de las empresas para realizar trámites mediante internet por computador o por cualquier otro dispositivo, así como por la telefonía móvil es la desconfianza en el medio.

**Figura 4.6. Percepción de uso de medios electrónicos por parte de las empresas para realizar trámites y servicios en línea en Colombia durante 2014**

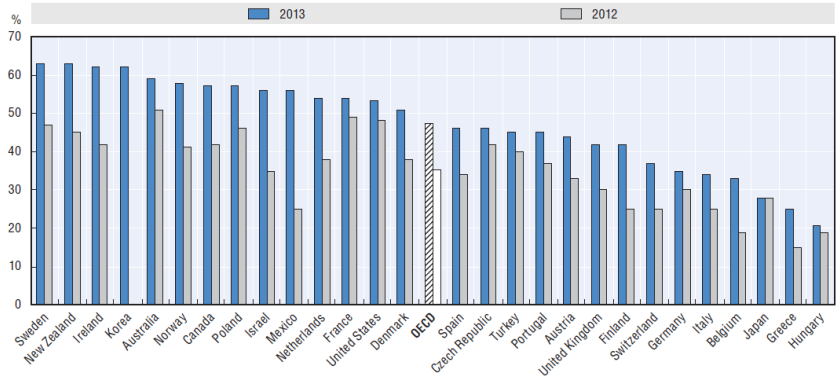



Fuente: INFOMETRIKA (2014)

- *Persiste la desconfianza en la realización de transacciones electrónicas en Colombia, incluso en sectores altamente digitalizados como el financiero.*

En línea con lo demostrado respecto de la percepción del uso de medios electrónicos por parte de los individuos y las empresas para realizar trámites en línea, en Colombia persisten barreras respecto del uso de la tecnología para realizar transacciones bancarias.

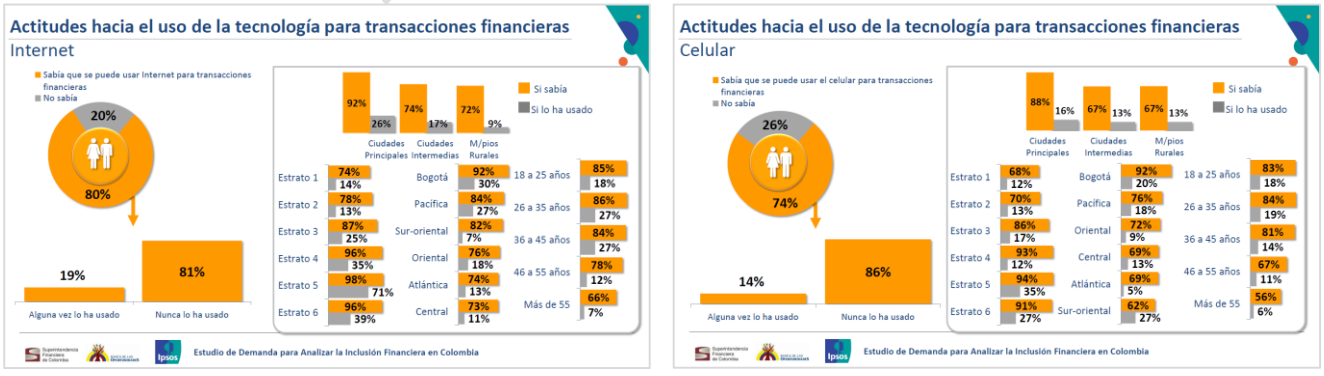
Figura 4.7. Porcentaje de usuarios de teléfonos inteligentes que utilizan Internet y realizan operaciones bancarias en línea u otras actividades relacionadas con las finanzas en su teléfono inteligente




Según SUPERFINANCIERA (2015) y lo expuesto en la Figura 4.8, la mayoría de la población colombiana sabe que el teléfono móvil y el Internet se pueden utilizar para realizar transacciones financieras. El porcentaje de personas que sabe que el móvil puede utilizarse para este propósito es un poco menor al del internet (74% verses 80%) puesto que en Colombia la utilización del móvil para realizar transacciones financieras empezó en 2007. El conocimiento del uso de estos canales para realizar transacciones financieras aumenta con el nivel socioeconómico y disminuye con la edad.

Sin embargo, la utilización de estos canales para realizar transacciones financieras es baja, puesto que menos de dos personas por cada diez los han utilizado. La utilización se concentra en los estratos altos por lo que se trata de personas con productos transaccionales tradicionales y no con cuentas gestionadas únicamente a través del celular.

Figura 4.8. Actitudes hacia el uso de la tecnología para transacciones financieras en Colombia en 2015




Fuente: SUPERFINANCIERA (2015)

SUPERFINANCIERA (2015) también resalta que entre quienes no sabían o no han utilizado el móvil y el internet para realizar transacciones financieras, a una de cada tres personas sí le gustaría utilizarlas y a dos de cada tres no les gustaría. El principal determinante es la edad, pues a la población joven es a la que más le gustaría utilizar la tecnología; seguida del género, pues los hombres tienen mayor disposición que las mujeres. Por nivel socioeconómico, los estratos 5 y 6 son los de mayor disposición, seguido de los estratos 1 y 2. La disposición también es mayor en ciudades intermedias.

Según la Tabla 4.8, SUPERFINANCIERA (2015) concluye que las principales motivaciones para el uso son la facilidad/comodidad, el ahorro de tiempo y la posibilidad de realizar las transacciones a cualquier hora. La facilidad/comodidad es lo que más valoran los jóvenes; el ahorro de tiempo lo valoran más las mujeres y las personas en ciudades principales; y la posibilidad de realizar las transacciones a cualquier hora la valoran más los hombres y las personas en ciudades intermedias.

La barrera determinante para el uso de las nuevas tecnologías es la desconfianza, pues de cada dos personas que no les gustaría utilizarlas, una no lo hace por esta razón. A las personas les parece inseguro realizar transacciones financieras por móvil e internet, principalmente a las de los estratos altos, a los jóvenes, a quienes viven en ciudades principales y a los hombres. En el caso del móvil, la inseguridad se refiere a que, en caso de pérdida o robo, personas indeseadas puedan acceder a las claves y recursos de las cuentas. En el caso del Internet, al riesgo de tener la información financiera en esta red y que otras personas puedan hackear las cuentas.



**Tabla 4.8. Barreras al uso de la tecnología para transacciones financieras en Colombia en 2015**

| | Internet | Móvil |
|---|---|---|
| **NO LE GUSTARÍA** | **67%** | **68%** |
| **LE PARECE INSEGURO** | 50% | 53% |
| No sabe hacerlo | 24% | 26% |
| Prefiere otros medios | 17% | 18% |
| Rechaza la tecnología | 16% | 18% |
| No tiene internet | 14% | - |
| Redes no confiables | - | 14% |

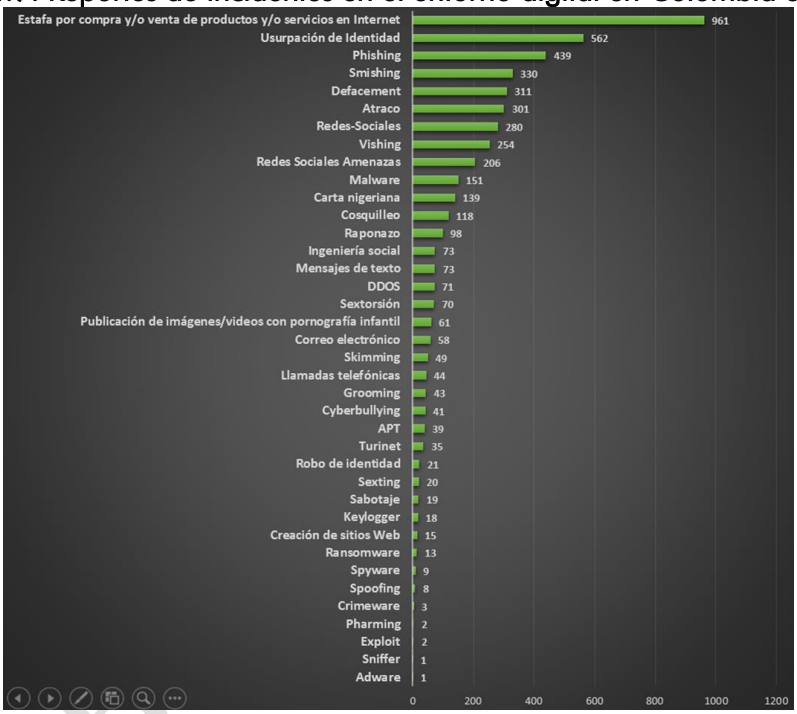
| | Internet | Móvil |
|---|---|---|
| **SI LE GUSTARÍA** | **33%** | **32%** |
| Facilidad, comodidad | 50% | 62% |
| Ahorro de tiempo | 44% | 38% |
| Transacciones a cualquier hora | 31% | 29% |
| Transacciones desde cualquier lugar | 23% | 21% |
| Seguridad | 18% | 19% |
| Economía | 13% | 15% |
| Gusta de internet | 12% | - |
| Guata de nuevas tecnologías | - | 11% |

Fuente: Adaptado de SUPERFINANCIERA (2015)

### 4.3.3. Colombia necesita reforzar sus capacidades para enfrentar nuevos tipos de crimen y delincuencia, a nivel nacional y transnacional, con un enfoque de gestión de riesgos de seguridad digital

En lo que se refiere a estadísticas de incidentes a nivel nacional, según OEA (2014), el CCP de Colombia tuvo un total de 2.652 reportes en 2013. En la Figura 4.9 se aprecia que CCP ha tenido un total de 4.960 reportes durante el año 2015, en donde se destacan los reportes por i) estafa de compra y/o venta de productos y/o servicios de internet con 961 casos, ii) la usurpación de identidad con 562 casos, y iii) el pishing[18] con 439 casos. Estos incidentes fueron reportados mediante el CAI VIRTUAL, el cual se considera como mecanismo de consulta y respuesta inmediata a las inquietudes que surgen ante las manifestaciones delictivas que utilizan las nuevas tecnologías como medio y fin.

Figura 4.9. Reportes de incidentes en el entorno digital en Colombia en 2015

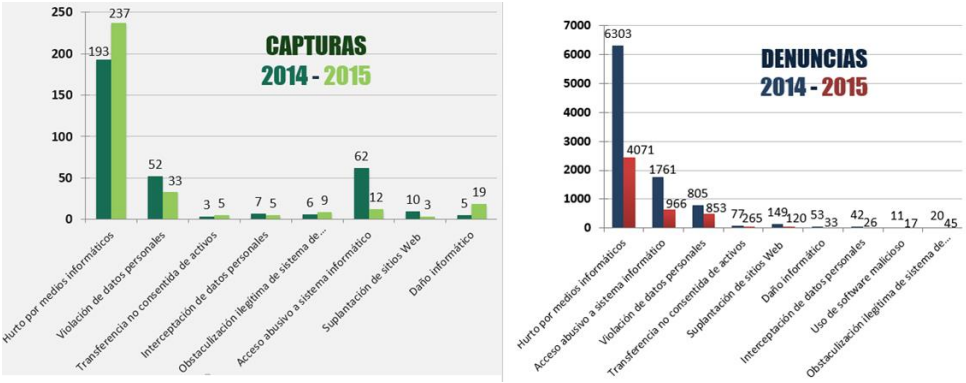



Fuente: CCP, 2015

El CCP del país ha realizado en promedio 330 capturas al año durante 2014 y 2015, La Figura 4.10 demuestra que la problemática es creciente en el país al observar la evolución de capturas debido a incidentes en el entorno digital.

[18] ISS (2014) menciona que Brasil, Colombia y Argentina fueron las tres principales fuentes de ataques mediante *phishing* en la región Latinoamérica y el Caribe durante el año 2013.

Figura 4.10. Capturas y denuncias de incidentes en el entorno digital en Colombia en 2015




Fuente: CCP, 2015

También, las denuncias por delitos asociados al entorno digital en Colombia se han incrementado fuertemente. 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, la explotación sexual comercial y la pornografía infantil y adolescente en Colombia, se aprecia un crecimiento anual promedio del 59% en la presentación de este tipo de denuncias en el país. Adicionalmente, gracias a esta iniciativa del 11 al 18 de diciembre de 2015, la DIJIN ha dado orden de bloqueo a 34 sitios web con pornografía infantil para un total de 3.373 URLs desde la puesta en marcha de Te Protejo.

Tabla 4.9. Denuncias procesadas por la iniciativa *Te Protejo* en Colombia entre 2012 y 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

Teniendo en cuenta las estadísticas que evidencia incrementos considerables de incidencias digitales, las entidades del Estado en temas de seguridad digital evidencian una brecha ante 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. Adicionalmente, los esfuerzos de las Entidades en el desarrollo de temas relacionados con Investigación, Desarrollo e Innovación no son suficientes con relación en las necesidades y avances que se tienen de forma cotidiana en esta materia, repercutiendo así, en la capacidad

y competitividad que tiene el gobierno para afrontar las amenazas a las que está constantemente expuesto.

Por otra parte, en atención al rol que cumplen los jueces y fiscales en el proceso judicial y que en el sentido del dominio y su contextualización del cibercrímen, no son suficientes las competencias de estos órganos, por lo tanto, se debe encaminar a que se dicten políticas claras que apoyen los procesos judiciales y juzguen conductas de manera efectiva que genere disuasión frente a la conducta y apoye en procesos de investigación estructural. El incremento continuo de la comisión de las conductas delictivas cibernéticas y su reincidencia se debe en gran medida al desconocimiento por parte de los administradores de justicia de la conducta criminal informática, así por parte de fiscales para entender la comisión de las conductas que pueden ser o no un delito informático y la debilidad de las herramientas jurídicas que existen actualmente para encuadrar la conducta del delito informático dentro del Código Penal. A pesar de los desarrollos normativos en la materia, se requiere la revisión y mejoramiento de cada una de las instancias judiciales, así como las sanciones administrativas y disciplinarias sobre la comisión o prevención de un delito informático.

Por otro lado, y vistas las nuevas formas de criminalidad, se debe entender que hoy por hoy las grandes redes criminales y el crimen organizado han adquirido, lamentablemente, una especial pericia 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 que en esa medida crimen e internet y/o crimen y mundo digital se funden en una amalgama que vista desde la perspectiva del riesgo país constituye una amenaza contra la defensa y la seguridad nacionales.

Es por esto que la estrategia del Estado para crear un entorno digital seguro y para luchar contra la delincuencia que se mueve en el mundo cibernético, debe tener dentro de sus objetivos entender fenómenos tales como el de ciberlavado de activos, el ciberterrorismo, o la ciberdelincuencia. Entendiendo la amenaza se hace más fácil luchar contra ella.

De igual forma, es fundamental fortalecer las capacidades de los fiscales y asistentes judiciales para entender los diferentes elementos provenientes de los medios digitales o del internet, así como los canales de cooperación interinstitucional para atender cualquier conducta que se derive de un delito informático entre el sector gobierno y el sector privado.

El CCP no cuenta con los recursos humanos, técnicos y financieros suficientes para enfrentar nuevos tipos de crimen y delincuencia, a nivel nacional y transnacional, con un enfoque de gestión de riesgos de seguridad digital, lo que ocasiona, mayor oportunidad para la materialización de amenazas.

### 4.3.4. Colombia necesita reforzar sus capacidades para proteger sus infraestructuras críticas nacionales y asegurar la defensa nacional en el entorno digital, con un enfoque de gestión de riesgos de seguridad digital

Colombia a diciembre de 2015, aún no cuenta con un catálogo de infraestructuras críticas, lo que incrementa el índice de riesgos de materialización de amenazas sobre las mismas, así como su inadecuada gestión de riesgos, protección y defensa. Además, trae consigo, la inadecuada planeación de recursos y esfuerzos en materia de seguridad digital, de los diferentes sectores económicos y productivos del país.

Por esto, es preciso advertir que la afectación o destrucción de una infraestructura critica nacional que soporte los procesos de servicios esenciales a la población traería consigo efectos y consecuencias devastadoras para el país e incluso ocasionar la pérdida de gobernabilidad en tan solo pocos minutos.

Las capacidades de las entidades responsables de Ciberseguridad y Ciberdefensa en lo que se refiere a: prevención, detección, contención, respuesta, recuperación y defensa ante las amenazas cibernéticas a los intereses nacionales, son limitadas, por lo que el país sufre mayores índices de probabilidad en la materialización de los riesgos digitales a los que se encuentra expuesto, ocasionando una preocupación por la Ciberseguridad y Ciberdefensa del Estado.

Así mismo, el CCOC, las Unidades Cibernéticas de las Fuerzas y los organismos de inteligencia del Estado no cuentan con los recursos humanos, técnicos y financieros suficientes para asegurar la defensa nacional en el entorno digital. Por otra parte, los roles en la seguridad digital del Estado, entre éstos la ciberseguridad, no se encuentran definidos para la protección de la infraestructura crítica nacional, lo que ocasiona mayor oportunidad para la materialización de amenazas.

### 4.3.5. Los esfuerzos de cooperación y colaboración nacional e internacional relacionados con la seguridad digital no son suficientes y requieren ser articulados

Se evidencia que existen esfuerzos aislados de cooperación nacional e internacional por parte de los responsables de Ciberseguridad y Ciberdefensa, con lo cual se presenta una gran brecha en el intercambio de conocimiento, experiencias, investigación, desarrollo de nuevas tecnologías, e información relacionada con los incidentes de seguridad digital. De igual forma se evidencia que no se han establecido canales de comunicación soportados en una efectiva estrategia de comunicación entre el Gobierno, el sector privado y la academia, para temas de Ciberseguridad y Ciberdefensa, lo cual genera duplicidad de esfuerzos y falta de efectividad en la formalización de convenios bilaterales y multilaterales.

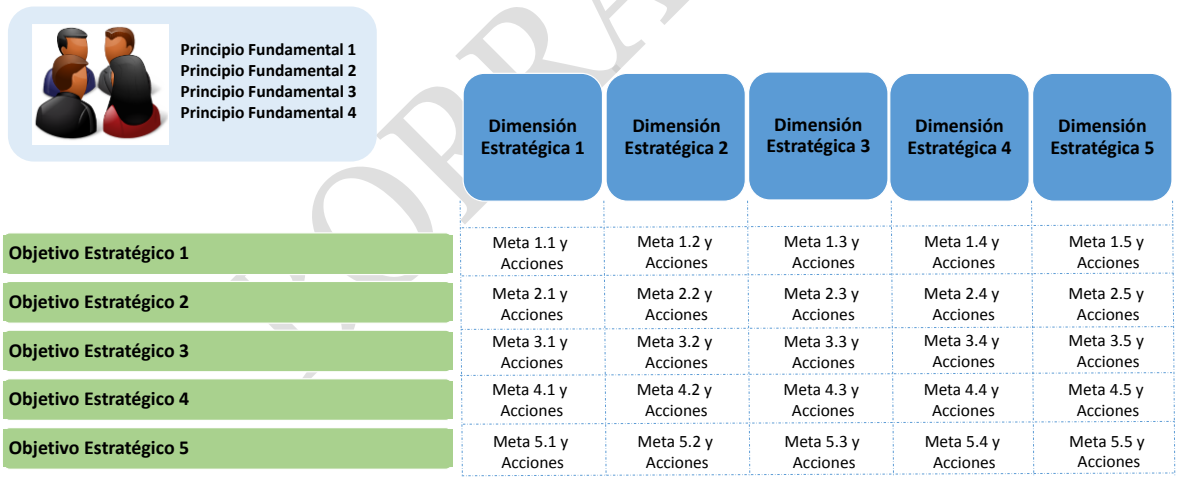
### 4.4. Población objetivo

La Política Nacional de Seguridad Digital, pretende lograr que todos los actores de interés en Colombia, siendo éstos el Gobierno Nacional, las organizaciones públicas y privadas, la academia y la sociedad civil, hagan un uso responsable y seguro del entorno digital abierto, a través del fortalecimiento de sus capacidades para identificar y gestionar los riesgos de las actividades digitales, maximizando así los beneficios obtenidos de una mayor prosperidad económica, política y social del país. Por tal razón, la población objetivo es el total de habitantes de Colombia.

## 5. DEFINICIÓN DE LA POLÍTICA

En esta sección se describe la política nacional de seguridad digital en Colombia, a partir de la siguiente estructura: i) Objetivo General, ii) cuatro principios fundamentales, iii) cinco dimensiones estratégicas, iv) cinco objetivos estratégicos, v) veinticinco metas, y vi) cien acciones a implementar.

Figura 5.1. Estructura Básica de la Política Nacional de Seguridad Digital en Colombia




Fuente: MINISTERIO TIC, 2015

### 5.1. Objetivo General

La política nacional de seguridad digital tiene como objetivo lograr que el Gobierno Nacional y los territoriales, las organizaciones públicas y privadas, la academia y la sociedad civil en Colombia, hagan un uso responsable de un entorno digital abierto, seguro y confiable, a través del fortalecimiento de sus capacidades para identificar, gestionar y mitigar los riesgos de las actividades digitales, contribuyendo al crecimiento de la economía digital

nacional, y maximizando de esta manera los beneficios obtenidos de una mayor prosperidad económica, política y social del país.

### 5.1.1. Principios Fundamentales

La política nacional de seguridad digital se basa en los siguientes Principios Fundamentales (PF):

PF1. Salvaguardar los derechos humanos y los valores fundamentales de los individuos, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de los datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia.

PF2. Adoptar un enfoque incluyente y colaborativo que involucre activamente a todos los actores de interés, siendo éstos el Gobierno Nacional y los territoriales, las organizaciones públicas y privadas, la academia y la sociedad civil, y que permita establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital en el país.

PF3. Asegurar una responsabilidad compartida entre todos los actores de interés promoviendo la máxima colaboración y cooperación en la gestión del 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, y así fomentar la prosperidad económica y social, buscando la generación de riqueza, innovación, productividad, competitividad, y empleo en todos los sectores de la economía.

### 5.1.2. Dimensiones Estratégicas

La política nacional de seguridad digital atenderá las necesidades y expectativas de todos los actores de interés en Colombia, con el fin de garantizar la seguridad digital, en torno a cinco Dimensiones Estratégicas (DE), que permiten articular el objetivo de la política bajo un enfoque de gestión de riesgos:

DE1. Marco legal y regulatorio de la seguridad digital: marco legal y regulatorio que soporta todos los aspectos necesarios para adelantar la política.

DE2. Gobernanza del entorno digital: articulación y armonización de todos los actores de interés, con el fin de gestionar la seguridad digital, bajo el liderazgo del Gobierno Nacional.

DE3. Gestión sistemática del riesgo de seguridad digital: conjunto de iniciativas, procedimientos y/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 todos los actores de interés, para 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 todos los actores de interés, para adelantar la gestión de riesgos de la seguridad digital.

### 5.2. Objetivos Estratégicos

Con el fin de alcanzar el objetivo general, bajo los principios fundamentales establecidos y asegurando un direccionamiento estratégico de la política, alrededor de las dimensiones estratégicas mencionadas, se establecen los siguientes cinco Objetivos Estratégicos (OE), que serán alcanzados mediante el establecimiento de un conjunto de metas y acciones concretas:

OE1. Fortalecer la capacidad institucional, normativa, administrativa y de gestión en materia de seguridad digital para Colombia, desde el más alto nivel: se requiere fortalecer el marco institucional, con el fin de desarrollar la política nacional de seguridad digital de manera coordinada, definiendo roles, responsabilidades y funciones específicas a todos los actores.

OE2. Fomentar la prosperidad económica y social del país, con la promoción de un entorno que permita desarrollar actividades digitales de manera abierta, segura y confiable: es de gran importancia para el futuro del país, maximizar los beneficios y oportunidades que puede ofrecer a los actores la naturaleza global, abierta, interconectada y altamente dinámica de las TIC.

OE3. Garantizar la integridad y seguridad de los individuos y del Estado, a nivel nacional y trasnacional, bajo un entorno digital creciente y dinámico: se requiere asegurar y consolidar las capacidades del país para hacer frente al crimen y la delincuencia en un mundo digital.

OE4. Fortalecer la defensa y soberanía nacional bajo un entorno digital: se requiere desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y defensa para garantizar los fines del Estado, así como también, mejorar la protección, preservar la integridad y la resiliencia de la infraestructura crítica nacional.

OE5. Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional: se requiere dinamizar la cooperación nacional entre sectores y la cooperación internacional en materia de seguridad digital.

El cruce de estos objetivos con las dimensiones estratégicas, descritas anteriormente, resulta en la definición de un conjunto de metas y acciones, las cuales se describen en el Plan de Acción y Seguimiento (PAS), cuya ejecución materializa la política nacional de seguridad digital.

## 5.3. Plan de Acción

A continuación se describe el plan de acción para alcanzar los objetivos estratégicos enunciados en la sección 5.2 del presente documento. Para cada uno de ellos se presentan las metas y acciones a desarrollarse. El detalle de las acciones aquí expuestas se puede consultar en el Plan de Acción y Seguimiento (PAS) contenido en la sección 9 (Anexo A), donde se señala a 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 nacional de seguridad digital.

### 5.3.1. Fortalecer la capacidad institucional, normativa, administrativa y de gestión en materia de seguridad digital para Colombia, desde el más alto nivel

Con el fin de alcanzar este objetivo estratégico, se propone alcanzar las siguientes metas para cada una de las dimensiones estratégicas:

- M1.1. Marco de trabajo institucional para la implementación de la Política Nacional de Seguridad Digital.

El Gobierno nacional, debe crear la figura de Consejero Presidencial para la Seguridad Digital en la Presidencia de la República, como autoridad y coordinador nacional de la Política Nacional de Seguridad Digital, así como modificar la Comisión Nacional Digital y de Información Pública, con el fin de convertirla en la instancia de máximo nivel en el Gobierno para la orientación superior de la ejecución de la Política Nacional de Seguridad Digital en Colombia. De igual manera, debe convertir al Grupo de Respuestas a Incidentes Cibernéticos de Colombia (ColCERT) en el órgano articulador y coordinador del desarrollo de medidas preventivas y reactivas de Seguridad Digital en Colombia, el cual responderá ante las instancias de máximo nivel en el Gobierno. Así mismo, debe crear en cada ministerio y departamento administrativo de orden nacional la figura de enlace sectorial en términos de Seguridad Digital con las instancias de máximo nivel en el Gobierno y con otras entidades. Finalmente, debe crear el Centro Criptológico Nacional y el Centro de Excelencia Nacional de Seguridad Digital.

- M1.2. Estructura y mecanismos de coordinación efectivas para abordar los temas de seguridad digital, entre todos los actores de interés, fortaleciendo la institucionalidad desde el más alto nivel.

El Gobierno nacional, debe diseñar un modelo dinámico de coordinación y cooperación que defina roles, responsabilidades y funciones, así como una matriz de comunicación y seguimiento entre las instancias de máximo nivel del Gobierno: i) con los ministerios y departamentos administrativos de orden nacional y ii) con el sector privado y la sociedad civil; con el fin de abordar los temas de Seguridad Digital en Colombia. De igual forma, debe crear una Agenda Nacional de Seguridad Digital con el fin de priorizar los intereses nacionales y las temáticas en torno al tema, involucrando a todos los actores de interés y una metodología única y unos estándares mínimos para el registro, manejo, control, detección temprana y reporte de incidentes en el entorno digital con un enfoque de gestión de riesgos de seguridad digital. Así mismo, debe fortalecer la capacidad administrativa del Grupo de Respuestas a Incidentes Cibernéticos de Colombia (ColCERT), adecuando la estructura orgánica del MINDEFENSA.

- M1.3. Metodología para la gestión de riesgos de seguridad digital.

El Gobierno nacional, debe diseñar una metodología para la gestión sistemática de riesgos de seguridad digital a nivel nacional con el fin de fomentar la prosperidad económica y social en el país. De igual manera debe generar los mecanismos administrativos de adopción de la gestión sistemática de riesgos de seguridad digital, bajo la metodología establecida, en todos los ministerios y departamentos administrativos de orden nacional. Finalmente, debe crear: i) una guía metodológica para la identificación de riesgos de seguridad digital, dirigida a todos los actores de interés, siendo éstos el Gobierno Nacional, las organizaciones públicas y privadas, academia y la sociedad civil, y ii) una guía metodológica para la evaluación del impacto socio económico de la gestión sistemática de riesgos de seguridad digital, dirigida a todos los actores de interés.

- M1.4. Programas, proyectos y campañas de socialización y concientización a todos los actores de interés debidamente diseñados, respecto de los aspectos relevantes de la economía digital y de la política de seguridad digital, con un enfoque de gestión de riesgos.

El Gobierno nacional, debe crear campañas nacionales de concientización destinada a aumentar la confianza en el uso del entorno digital, con enfoque en la salvaguarda de los derechos humanos y los valores fundamentales y diseñar programas y proyectos de concientización de todos los actores de interés respecto de la Seguridad Digital. De igual manera, debe diseñar un plan de socialización de la guía metodológica para la identificación de riesgos de seguridad digital, dirigida a todos los actores de interés y un plan de

socialización de la guía metodológica para la evaluación del impacto socio económico de la gestión sistemática de riesgos de seguridad digital, dirigida a todos los actores de interés. Finalmente, debe fortalecer la estrategia *En TIC Confío* del Ministerio de Tecnologías de la Información y las Comunicaciones, mediante el cual se promueva la confianza en el uso del entorno digital y la gestión de riesgos de seguridad digital en Colombia.

- M1.5. Programas y proyectos de educación y fortalecimiento de capacidades a todos los actores de interés debidamente diseñados, respecto de los aspectos relevantes de la economía digital y de la política de seguridad digital, con un enfoque de gestión de riesgos.

El Gobierno nacional, debe crear contenido educativo respecto de los beneficios de la gestión de riesgos de seguridad digital en el desarrollo de actividades económicas y sociales en un entorno digital abierto dirigido a todos los actores de interés. De igual manera, debe diseñar programas y proyectos de fortalecimiento de capacidades de todos los actores de interés, respecto de la Seguridad Digital y crear material metodológico educativo para capacitar a los maestros de educación básica (primaria y secundaria), media y superior, respecto de los beneficios de la gestión de riesgos de seguridad digital. Finalmente, debe modernizar los currículos de educación básica (primaria y secundaria) y media, incluyendo contenidos educativos asociados a la gestión de riesgos de seguridad digital y promover la inclusión en todos los programas de educación superior de contenidos educativos asociados a la gestión de riesgos de seguridad digital.

### 5.3.2. Fomentar la prosperidad económica y social del país con la promoción de un entorno que permita desarrollar actividades digitales de manera abierta, confiable y segura

Con el fin de alcanzar este objetivo estratégico, se propone alcanzar las siguientes metas para cada una de las dimensiones estratégicas:

- M2.1. Marco legal y regulatorio armonizado para que todos los actores de interés implementen el marco de trabajo (principios y estrategias) de la Política Nacional de Seguridad Digital en sus actividades económicas y sociales.

El Gobierno nacional, debe compilar y actualizar la regulación en el sector de TIC teniendo en cuenta aspectos necesarios para la gestión de riesgos de seguridad digital, armonizar la normatividad que permita realizar eficientemente el almacenamiento, la retención y los procedimientos del suministro de información por parte de los proveedores de servicio de Internet en Colombia, y actualizar la ley de inteligencia con aspectos relacionados con la seguridad digital, incluyendo la participación de la comunidad de inteligencia y contrainteligencia, erigiendo así el cibercrimen como una amenaza contra la

estabilidad del Estado. Así mismo, debe adelantar un estudio de mejores prácticas respecto de los marcos legales y regulatorios a nivel internacional en torno a i) la protección de la privacidad y los datos personales y a ii) los derechos humanos, el derecho internacional humanitario y los valores fundamentales; bajo la gestión de riesgos de seguridad digital.

- M2.2. Incremento en el uso del entorno digital global, abierto, interconectado y dinámico por parte de todos los actores de interés maximizando beneficios económicos y sociales, mediante la gestión de riesgos de seguridad digital.

El Gobierno nacional, debe articular la estrategia de gestión de riesgos de seguridad digital con i) el Plan Nacional de Desarrollo 2014-2018, "*Todos por un Nuevo País – Paz, Equidad y Educación*", ii) con el Plan Vive Digital 2014-2018, y iii) con otras estrategias que fomenten la prosperidad económica y social en Colombia en el corto y mediano plazo. De igual forma, debe identificar los servicios públicos prestados, ya sea por entidades públicas o privadas que utilicen directa o indirectamente el entorno digital y debe identificar los objetivos económicos y sociales de cada política sectorial que implican actividades en el entorno digital sobre las cuales podrían existir riesgos de seguridad digital. También, se debe capacitar a todas las entidades del sector público respecto de las ventajas de un entorno digital global, abierto, interconectado y dinámico que maximice los beneficios económicos y sociales mediante la gestión de riesgos de seguridad digital. Finalmente, el Gobierno nacional debe evaluar la Política Nacional de Seguridad Digital, estimar el impacto económico de la misma sobre los actores de interés una vez se haya consolidado la implementación de la misma y debe estimular mejoras continuas en eficiencia y eficacia de la gestión de riesgos de seguridad digital.

- M2.3. Gestión de riesgos de seguridad digital implementada por parte de todos los actores de interés del sector público y evaluación del impacto socio económico de la política, así como la promoción de su implementación a los actores de interés del sector privado y de la sociedad civil.

El Gobierno nacional, debe identificar los riesgos de seguridad digital, mediante la guía metodológica establecida, así como adoptar y aplicar la metodología de gestión de riesgos de seguridad digital establecida de forma permanente. De acuerdo con el modelo detallado de coordinación definido, el Gobierno debe evaluar el avance periódico de aplicación de la gestión de riesgos de seguridad digital a las instancias de máximo nivel del Gobierno en Seguridad Digital y debe evaluar el impacto socio económico de la gestión de riesgos de seguridad digital, mediante la guía metodológica establecida.

- M2.4. Programas, proyectos y campañas de socialización y concientización a todos los actores de interés debidamente implementados, respecto de los aspectos

relevantes de la economía digital y de la política de seguridad digital, con un enfoque de gestión de riesgos.

El Gobierno nacional, debe implementar los programas y proyectos de concientización bajo el enfoque de cada sector a todos los actores de interés respecto de la Seguridad Digital, previamente diseñados. Así mismo, debe concientizar a todos los actores de interés respecto de aspectos del Derecho Internacional Humanitario y los Derechos Humanos en el entorno digital y mapear la relación entre las redes de la administración pública y sus proveedores de Internet con el fin de garantizar una cooperación eficaz en el manejo de incidentes de seguridad digital. De igual forma, debe promover el uso por parte del sector privado y de la sociedad civil de la guía metodológica para la identificación de riesgos de seguridad digital y la guía metodológica para la evaluación del impacto socio económico de la gestión de riesgos de seguridad digital.

- M2.5. Programas y proyectos de educación y fortalecimiento de capacidades a todos los actores de interés debidamente implementados, respecto de los aspectos relevantes de la economía digital y de la política de seguridad digital, con un enfoque de gestión de riesgos.

El Gobierno nacional, debe implementar los programas y proyectos de fortalecimiento de capacidades de todos los actores de interés respecto de la Seguridad Digital previamente diseñados. Así mismo, debe capacitar a los maestros de educación básica, media y superior respecto de los beneficios de la gestión de riesgos de seguridad digital y hacer seguimiento para asegurar que los currículos de educación básica (primaria y secundaria) y media en Colombia, incluyan los contenidos educativos asociados a la gestión de riesgos de seguridad digital y respecto de la inclusión de contenidos educativos asociados a la gestión de riesgos de seguridad digital en todos los programas de educación superior en Colombia. Finalmente, debe crear e implementar una estrategia de permanencia del talento humano que desarrolla actividades relacionadas con la seguridad digital en las organizaciones públicas.

### 5.3.3. Garantizar la integridad y seguridad de los individuos y del Estado, a nivel nacional y trasnacional, bajo un entorno digital creciente y dinámico

Con el fin de alcanzar este objetivo estratégico, se propone alcanzar las siguientes metas para cada una de las dimensiones estratégicas:

- M3.1. Marco legal y regulatorio comprensible, efectivo y adecuado con el fin de asegurar la seguridad nacional en un entorno digital.

El Gobierno nacional, debe armonizar el marco legal y regulatorio con las necesidades en materia de prevención, detección y atención de delitos y crímenes en el entorno digital y

el marco legal y regulatorio con las necesidades en materia de investigación, persecución y criminalización de nuevos tipos de delitos y crímenes en el entorno digital.

Adicionalmente, deberá presentar un proyecto de ley al Congreso de la República que incluya a los delitos informáticos como delitos fuente de lavado de activos, para así potenciar las capacidades de análisis de detección y prevención de la ciberdelincuencia de las entidades que hacen parte del Sistema Antilavado de Activos en Colombia."

- M3.2. Instancias y entidades de investigación y combate al crimen y la delincuencia en un entorno digital fortalecidas.

El Gobierno nacional, debe fortalecer la capacidad administrativa del Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia, adecuando la estructura orgánica de la entidad. De igual manera, debe implementar el Centro de Fusión para Investigación de Crímenes Económicos y Financieros (C2F2) y el Centro de Comunicaciones, Cómputo, Control y Comando para la Seguridad Digital (C4C). También debe fortalecer la capacidad administrativa de la Unidad de Información y Análisis Financiero (UIAF) y debe crear y fortalecer el observatorio de delitos en entorno digital, los laboratorios de informática forense y los centros de investigación en seguridad digital. Finalmente, debe mapear la relación entre las redes de la administración pública y sus proveedores de Internet con el fin de garantizar una cooperación eficaz en el manejo de incidentes de seguridad digital.

- M3.3. Marco de trabajo para mitigar el crimen y la delincuencia que atenten contra la seguridad nacional en un entorno digital, basado en un enfoque de gestión sistémica de riesgos de seguridad digital.

El Gobierno nacional, debe asegurar que el CCP de la Policía Nacional adopte y aplique la metodología de gestión de riesgos de seguridad digital establecida, informando el avance periódico de su aplicación a las instancias de máximo nivel del Gobierno en Seguridad Digital.

- M3.4. Mecanismos de socialización y concientización de tipologías comunes de crimen y delincuencia en un entorno digital que afecten la seguridad nacional y la manera de gestionar sus riesgos por parte de los actores de interés.

El Gobierno nacional, debe socializar periódicamente a todos los actores de interés respecto de los avances en el combate al crimen y a la delincuencia que atenten contra la seguridad nacional en el entorno digital. También, debe crear una red de vigilancia nacional de la Infraestructura Crítica Nacional con el sector privado y la sociedad civil. De igual forma, debe promover la implementación de CSIRTs sectoriales, definidos de acuerdo a la catalogación de las infraestructuras críticas nacionales, y el desarrollo de tanques de

pensamiento para abordar con innovación la gestión sistemática de riesgos de seguridad digital. Finalmente, debe diseñar e implementar esquemas tecnológicos y procedimentales para garantizar la identificación, autenticación y autorización de funcionarios, ciudadanos, activos de información y recursos que acceden a la infraestructura del Estado colombiano.

- M3.5. Funcionarios públicos responsables de garantizar la seguridad nacional en el entorno digital debidamente capacitados.

El Gobierno nacional, debe diseñar contenido educativo para fortalecer las capacidades de los funcionarios de las entidades de combate contra el crimen y de administración de justicia en Colombia responsables de adelantar actuaciones asociadas con la Seguridad Digital y fortalecer las capacidades y posibilidades de los funcionarios públicos para llevar a cabo pruebas y simulaciones de incidentes de seguridad digital.

### 5.3.4. Fortalecer la defensa y soberanía nacional bajo un entorno digital

Con el fin de alcanzar este objetivo estratégico, se propone alcanzar las siguientes metas para cada una de las dimensiones estratégicas:

- M4.1. Marco legal y regulatorio comprensible, efectivo y adecuado con el fin de asegurar la defensa nacional en un entorno digital.

El Gobierno nacional, debe adelantar una compilación de la normatividad en todos los sectores que impacte la Infraestructura Crítica Nacional con el fin de identificar medidas de seguridad digital entorno a la misma y armonizar el marco legal y regulatorio con las necesidades en materia de protección de la Infraestructura Crítica Nacional con un enfoque de gestión de riesgos de seguridad digital.

- M4.2. Instancias y entidades de protección de los intereses del país en un entorno digital y de las infraestructuras críticas fortalecidas.

El Gobierno Nacional, debe fortalecer las capacidades administrativas y operativas del Comando Conjunto Cibernético (CCOC), las Unidades Cibernéticas de las Fuerzas Militares y los organismos de Inteligencia del Estado. Así como, actualizar e incluir nuevos planes y proyectos para el fortalecimiento de la seguridad digital, haciendo énfasis en la ciberdefensa, e implementar los Centros de Operaciones cibernéticas de las Fuerzas Militares bajo la coordinación del CCOC. Así mismo, liderado por el ColCERT se debe actualizar el catálogo de Infraestructura Crítica Nacional con un enfoque de gestión de riesgos de seguridad digital, desarrollar una plataforma automatizada para compartir información con todos los actores de interés sobre amenazas e incidentes de seguridad digital, sean éstos relacionados con la ciberseguridad o la ciberdefensa. Adicionalmente, debe estructurar, actualizar e implementar

las guías de Riesgo Operacional para la mejora de la protección y resiliencia de la Infraestructura Crítica Nacional.

- M4.3. Marco de trabajo para asegurar la defensa nacional en un entorno digital, basado en un enfoque de gestión sistémica de riesgos de seguridad digital.

El Gobierno nacional, debe asegurar que el CCOC del CGFM adopte y aplique la metodología de gestión de riesgos de seguridad digital establecida, informando el avance periódico de su aplicación a las instancias de máximo nivel del Gobierno en Seguridad Digital.

- M4.4. Mecanismos de socialización y concientización de tipologías comunes de ataques que atenten contra la defensa nacional en entorno digital y la manera de gestionar sus riesgos por parte de los actores de interés.

El Gobierno nacional, debe socializar los planes de protección y defensa de la Infraestructura Critica Nacional a todos los actores de interés y las tipologías comunes de ataques que atenten contra la defensa nacional en entorno digital, así como la manera de gestionar sus riesgos por parte de los actores de interés. También debe realizar mesas de trabajo y convenios con todos los actores de interés que fomenten la discusión y la investigación con innovación respecto de la gestión de riesgos de seguridad digital. Así mismo, debe informar a las organizaciones privadas acerca de las ventajas de los CSIRTs en los respectivos sectores e industrias promoviendo su creación y establecer un grupo de trabajo integrado por representantes de todas las organizaciones que se ocupan de la investigación desarrollo e innovación en el campo de la seguridad digital.

- M4.5. Funcionarios públicos que trabajen con infraestructuras críticas en cualquier sector de la economía debidamente capacitados.

El Gobierno nacional y la academia deben diseñar contenido educativo para fortalecer las capacidades de los responsables de garantizar la seguridad digital, haciendo énfasis en la ciberdefensa y ciberseguridad, con un enfoque de gestión de riesgos y fortalecer las capacidades para llevar a cabo pruebas y simulaciones de incidentes de seguridad digital sobre la Infraestructura Crítica Nacional.

### 5.3.5. Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional

Con el fin de alcanzar este objetivo estratégico, se propone alcanzar las siguientes metas para cada una de las dimensiones estratégicas:

- M5.1. Marco de cooperación, colaboración y asistencia a nivel nacional e internacional, en torno a la seguridad digital.

El Gobierno nacional debe desarrollar e implementar una Agenda Estratégica de cooperación, colaboración y asistencia nacional e internacional en temas de seguridad digital. Así mismo, debe adelantar la revisión del marco jurídico vigente con el fin de implementar la diplomacia digital en Colombia.

- M5.2. Mecanismos de cooperación, colaboración y asistencia en torno a la seguridad digital, y estímulo del uso de estándares internacionales seguros e interoperables.

El Gobierno nacional, debe fomentar la creación y adhesión a redes de intercambio internacionales de información de seguridad digital. Así mismo, debe garantizar la presencia del colCERT, el CCP y el CCOC en organismos internacionales que traten el tema de seguridad digital y la firma de acuerdos de cooperación, colaboración o asistencia a nivel regional y mundial. Finalmente, debe fortalecer y garantizar la presencia del enlace de la Policía Nacional de Colombia en el EC3 de EUROPOL y el IGCI de INTERPOL.

- M5.3. Asistencia de representantes del país en eventos relevantes para compartir experiencias y mejores prácticas en la gestión de riesgos de seguridad digital, así como para establecer relaciones con todos los actores de interés, sean estos nacionales o internacionales.

El Gobierno nacional, debe identificar mejores prácticas en la gestión de riesgos de seguridad digital en el país, con el fin de colaborar y asistir a otros países u organizaciones internacionales, así como participar en eventos regionales e internacionales pertinentes para compartir experiencias y buenas prácticas en la gestión de riesgos de seguridad digital, estableciendo relaciones bilaterales y multilaterales entorno a la gestión de riesgos de seguridad digital.

- M5.4. Mejores prácticas a nivel nacional e internacional en torno a la socialización y concientización de actores de interés debidamente implementadas, respecto a aspectos relacionados con la seguridad digital, con un enfoque de gestión de riesgos.

El Gobierno nacional debe establecer un acuerdo marco para la cooperación con el sector privado respecto de la identificación de mejores prácticas de seguridad digital, con un enfoque de gestión de riesgos. También, debe fomentar programas de intercambio académico con países aliados en temas asociados a la Seguridad Digital. Finalmente, debe

establecer y desarrollar la cooperación entre los servicios de inteligencia del país y entre las entidades nacionales e internacionales pertinentes en materia de seguridad digital.

- M5.5. Asistencia de representantes del país en asuntos de diplomacia y de los actores de interés en programas internacionales de capacitación en temas de seguridad digital, con un enfoque de gestión de riesgos.

El Gobierno nacional debe establecer una figura de enlace en el Ministerio de Relaciones Exteriores para abordar los temas de seguridad digital en el marco de la diplomacia digital. También debe crear e implementar un diplomado en Diplomacia Digital asociado al tema de seguridad digital dirigido a todos los actores de interés. Así mismo, debe promover la participación de representantes de los actores de interés en programas internacionales de capacitación en temas de seguridad digital.

## 5.4. Valoración de impacto económico de la política

La Comisión de Regulación de Comunicaciones (CRC) de Colombia, con apoyo de la Dirección de Estudios Económicos del Departamento Nacional de Planeación, estimó de manera preliminar 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[19]. Se estima que la implementación de la Política Nacional de Seguridad Digital al año 2020, impactaría positivamente la economía de Colombia, generándose aproximadamente 307.000[20] empleos y un crecimiento aproximado de 0,09% en la tasa promedio de variación anual del Producto Interno Bruto (PIB) durante los años 2015 a 2020, sin generar presiones inflacionarias. A continuación, la Tabla 5.1 presentan los resultados de la valoración del impacto económico. Los supuestos del ejercicio de valoración se presentan en el Anexo B del presente documento.



[19] El MEGC dinámico de la CRC es un instrumento de simulación económica y de evaluación de impactos 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 construidas sobre la base de la teoría económica generalmente aceptada, interactuando con aspectos fiscales y monetarios e inversión, con presencia de diversos agentes económicos.

[20] 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.

Tabla 5.1. Impacto económico de la implementación de la Política Nacional de Seguridad Digital en Colombia
(Promedios anuales para el periodo 2010-2020)

| Resultados | Unidad de Medida | Escenario Base | Escenario Colombia implementando la Gestión de Riesgos de Seguridad Digital | Diferencia |
|---|---|---|---|---|
| **Tasa de Cambio** | Pesos por U$1 | 2.619,04 | 2.620,46 | **1,42** |
| Variación | % | 5,44% | 5,45% | **0,01%** |
| | | | | |
| **Inflación al consumidor (canasta 2010)** | % | 5,17% | 5,17% | **0,00%** |
| | | | | |
| **PIB** | | 755.571 | 772.013 | **16.442** |
| Tasa de crecimiento | % | 4,35% | 4,44%% | **0,09%** |
| | | | | |
| **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 de DNP, 2015

## 5.5. Calendario de Seguimiento

El seguimiento a la ejecución física y presupuestal de este documento se desarrollará en la segunda sección del PAS (Anexo A). Este Plan de Acción se enmarca en las cinco Dimensiones Estratégicas, en los cinco Objetivos Estratégicos y en las veinticinco Metas establecidas. El cronograma de seguimiento se detalla en la Tabla 5.2.

Tabla 5.2. Cronograma de seguimiento

| Corte | Fecha |
|---|---|
| Primer corte | 31 de diciembre de 2016 |
| Segundo corte | 30 de junio de 2017 |
| Tercero corte | 31 de diciembre de 2017 |
| Cuarto corte | 30 de junio de 2018 |
| Quinto corte | 31 de diciembre de 2018 |
| Sexto corte | 30 de junio de 2019 |
| Informe de cierre | 31 de diciembre de 2019 |

Fuente: MINISTERIO TIC, 2015

En cada informe de seguimiento se deberá reportar también el nivel de ejecución de todas las acciones ya iniciadas pero aún no concluidas.

## 5.6. Esquema de Financiamiento

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

En la Tabla 5.3 se encuentran los recursos y las fuentes de los mismos, los cuales se ejecutarán durante el horizonte de ejecución de la Política Nacional de Seguridad Digital en Colombia por cada una de las entidades allí mencionadas.

**Tabla 5.3. Financiamiento estimado 2015-2018**
**(Millones de pesos)**

| Entidad | 2016 | 2017 | 2018 | TOTAL |
|---|---|---|---|---|
| MINTIC | $ | $ | $ | $ |
| MINDEFENSA | $ | $ | $ | $ |
| MINEDUCACIÓN | $ | $ | $ | $ |
| CANCILLERIA | $ | $ | $ | $ |
| MINJUSTICIA | $ | $ | $ | $ |
| MINCULTURA | $ | $ | $ | $ |
| MINCOMERCIO | $ | $ | $ | $ |
| MININTERIOR | $ | $ | $ | $ |
| MINHACIENDA | $ | $ | $ | $ |
| MINMINAS | $ | $ | $ | $ |
| MINTRANSPORTE | $ | $ | $ | $ |
| MINAGRICULTURA | $ | $ | $ | $ |
| MINVIVIENDA | $ | $ | $ | $ |
| MINAMBIENTE | $ | $ | $ | $ |
| MINSALUD | $ | $ | $ | $ |
| MINTRABAJO | $ | $ | $ | $ |
| **TOTAL** | **$** | **$** | **$** | **$** |

Fuente: MINISTERIO TIC, 2015



## 6. RECOMENDACIONES

El Ministerio de Tecnologías de la Información y las Comunicaciones recomienda al Consejo Nacional de Política Económica y Social:

- Aprobar la Política Nacional de Seguridad Digital en Colombia.

## 7. GLOSARIO

- **ACTORES DE INTERÉS**: El Gobierno Nacional, las organizaciones públicas y privadas, la academia y la sociedad civil.
- **CIBERDEFENSA**: Es el empleo de las capacidades militares ante amenazas o actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. Fuente: Ministerio de Defensa.
- **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.

- **GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL**: es el conjunto de acciones adoptadas para enfrentar los riesgos mientras se maximizan las oportunidades en el entorno digital. Es un esquema para enfrentar, prevenir y contrarrestar la materialización de amenazas o incidentes que puedan afectar la soberanía nacional y las actividades económicas y sociales de los ciudadanos. El utilizar un esquema de gestión de riesgos asegura que las medidas adoptadas sean apropiadas y conmensuradas.
- **RIESGO DE SEGURIDAD DIGITAL**: es la expresión utilizada para describir una categoría de riesgo relacionada con el uso, desarrollo y gestión del ambiente digital en el curso de cualquier actividad. 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.

## 8. BIBLIOGRAFÍA


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

CEPAL. (2014). *Economía Digital para el cambio estructural y la igualdad*. @LIS2. Recuperado de: http://repositorio.cepal.org/bitstream/11362/35408/1/S2013186_es.pdf

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. (2014a). Reparación para la Estrategia nacional para el Desarrollo de Infraestructura (REDI) – Sector TIC.

Departamento Nacional de Planeación. (2014b). 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

Hernández, Rodríguez. Realpe. (2014). Trabajo de Grado Maestría UNIANDES "*Estrategia Nacional de Ciberseguridad y Ciberdefensa para Colombia*"

Intel Security Labs. (2013). *The Economic Impact of Cybercrime and Cyber Espionage*. Center for Strategic and International Studies. Recuperado de: http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime.pdf

Intel Security Labs. (2014). Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. Center for Strategic and International Studies. Recuperado de: http://www.mcafee.com/jp/resources/reports/rp-economic-impact-cybercrime2.pdf

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

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

Intel Security Labs. (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

ISS. (2014). *Riding the digital wave – The impact of cyber capacity building on human development*. Institute for Security Studies - European Union. Recuperado de: http://www.iss.europa.eu/uploads/media/Report_21_Cyber.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 TIC. (2015a). *Informe de gestión al Congreso de la República de Colombia 2015*.

MINISTERIO TIC. (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

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. (2014). *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. (2014). *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.

Ponemon Institute. (2015). *2015 Cost of Cyber Crime Study: Global*. Recuperado de: https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

PwC. (2011). *Measuring Industry Digitization – Leaders and Laggars in the Digital Economy*. Recuperado de: http://www.strategyand.pwc.com/reports/measuring-industry-digitization-leaders-laggards

PwC. (2012). *The 2012 industry digitization index*. Recuperado de: http://www.strategyand.pwc.com/media/file/The-2012-industry-digitization-index.pdf

PwC. (2015). *The Global State of Information Security® Survey 2016 Turnaround and transformation in cybersecurity*. Recuperado de: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html

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

Tufts University. (2013). Digital Evolution Index - The Next Billion Consumers Move Onto the Global Stage. Estudio de The Fletcher School para Datacash de MASTERCARD. Recuperado de:

http://insights.mastercard.com/digitalevolution/Digital_Evolution_Index_Key_Findings.pdf
UIT. (2011). *ITU National Cibersecurity Strategy Guide*. Recuperado de:
UIT. (2015). Measuring he Information Society Report 2015. Recuperado de:
Verizon. (2015). 2015 Data Breach Investigations Report. Recuperado de: http://www.verizonenterprise.com/DBIR/2015/

## 9. ANEXOS

Anexo A: Plan de Acción y Seguimiento (PAS)

Anexo B: Estimación del impacto económico de la adopción e implementación de la Política Nacional de Seguridad Digital para Colombia

## ANEXO A: Plan de Acción y Seguimiento (PAS)

La Tabla A.1 presenta veinticinco acciones que serán adelantadas por cada una de las entidades responsables y con el fin de alcanzar las cinco metas propuestas para fortalecer la capacidad institucional, normativa, administrativa y de gestión en materia de seguridad digital para Colombia, desde el más alto nivel.

**Tabla A.1. Acciones para fortalecer la capacidad institucional, normativa, administrativa y de gestión en materia de seguridad digital para Colombia, desde el más alto nivel**

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE1 | Fortalecer la capacidad institucional, normativa, administrativa y de gestión en materia de seguridad digital para Colombia, desde el más alto nivel | | | | |
| **Código de Meta** | **Meta** | **Código de Acción** | **Acción** | **Entidad Responsable** | **Fecha de Finalización** |
| M1.1 | Marco de trabajo institucional para la implementación de la Política General de Seguridad Digital. | A1.1.1. | Crear la figura de Consejero Presidencial para la Seguridad Digital, con la idoneidad y competencias específicas, dotado de las herramientas jurídicas que le permitan desempeñar su cargo como autoridad y coordinador nacional de la Política General de Seguridad Digital. | PRESIDENCIA<br>MINTIC<br>DNP | 4Q2016 |
| | | A1.1.2. | Modificar el Decreto 32 de 2013 "*por la cual se crea la Comisión Nacional Digital y de Información Pública*", conformando la instancia de máximo nivel en el Gobierno para la orientación superior de la ejecución de la Política Nacional de Seguridad Digital en Colombia. | PRESIDENCIA<br>MINTIC<br>DNP | 1Q2017 |
| | | A1.1.3. | Convertir al *Grupo de Respuestas a Incidentes Cibernéticos de Colombia* (colCERT) en el órgano articulador y coordinador del desarrollo de medidas preventivas y reactivas de Seguridad Digital en Colombia, el cual responderá ante las instancias de máximo nivel en el Gobierno. | PRESIDENCIA<br>MINTIC<br>MINDEFENSA | 4Q2016 |
| | | A1.1.4. | Crear en cada ministerio y departamento administrativo de orden nacional la figura de enlace sectorial en términos de Seguridad Digital con las instancias de máximo nivel en el Gobierno y con otras entidades. | PRESIDENCIA<br>MINTIC | 1Q2017 |
| | | A1.1.5. | Crear el *Centro Criptológico Nacional* como autoridad de certificación de la seguridad digital y autoridad de certificación criptológica en Colombia y el *Centro de Excelencia Nacional de Seguridad Digital* como un espacio de pensamiento estratégico que tiene como objetivo integrar aspectos de investigación, innovación y desarrollo, educación y concienciación en temas de Seguridad Digital. | PRESIDENCIA<br>MINTIC<br>MINDEFENSA | 2Q2017 |
| M1.2 | Estructura y mecanismos de coordinación efectivas para abordar los temas de seguridad digital, entre todos los actores de interés, fortaleciendo la institucionalidad desde el más alto nivel. | A1.2.1. | Diseñar un modelo dinámico de coordinación y cooperación que defina roles, responsabilidades y funciones, así como una matriz de comunicación y seguimiento entre las instancias de máximo nivel del Gobierno: i) con los ministerios y departamentos administrativos de orden nacional y ii) con el sector privado y la sociedad civil; con el fin de abordar los temas de Seguridad Digital en Colombia. | PRESIDENCIA<br>DNP<br>MINTIC<br>MINDEFENSA<br>MINJUSTICIA<br>CANCILLERIA | 4Q2016 |
| | | A1.2.2. | Crear una Agenda Nacional de Seguridad Digital con el fin de priorizar los intereses nacionales y las prioridades en torno al tema, involucrando a todos los actores de interés. | PRESIDENCIA<br>DNP<br>MINTIC<br>MINDEFENSA | 2Q2017 |

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE1 | Fortalecer la capacidad institucional, normativa, administrativa y de gestión en materia de seguridad digital para Colombia, desde el más alto nivel | | | | |
| **Código de Meta** | **Meta** | **Código de Acción** | **Acción** | **Entidad Responsable** | **Fecha de Finalización** |
| | | | | MINJUSTICIA<br>MINCULTURA<br>CANCILLERIA | |
| | | **A1.2.3.** | Definir una metodología única y unos estándares mínimos para el registro, manejo, control, detección temprana y reporte de incidentes en el entorno digital con un enfoque de gestión de riesgos de seguridad digital. | PRESIDENCIA<br>MINTIC<br>MINDEFENSA | 2Q2017 |
| | | **A1.2.4.** | Definir los mecanismos y protocolos de intercambio seguro y eficiente de información estatal entre las entidades del Gobierno y con los diferentes actores de interés. | PRESIDENCIA<br>MINTIC | 2Q2017 |
| | | **A1.2.5** | Fortalecer la capacidad administrativa del *Grupo de Respuestas a Incidentes Cibernéticos de Colombia* (colCERT), adecuando la estructura orgánica del MINDEFENSA. | PRESIDENCIA<br>MINDEFENSA | 1Q2017 |
| **M1.3** | Metodología para la gestión de riesgos de seguridad digital. | **A1.3.1.** | Diseñar una metodología para la gestión sistemática de riesgos de seguridad digital a nivel nacional con el fin de fomentar la prosperidad económica y social en el país. | MINTIC | 1Q2017 |
| | | **A1.3.2.** | Tramitar, ante las instancias de máximo nivel del Gobierno en Seguridad Digital definidas y ante las entidades del Gobierno responsables, la aprobación de la metodología de gestión sistemática de riesgos de seguridad digital. | PRESIDENCIA<br>MINTIC<br>DAFP | 2Q2017 |
| | | **A1.3.3.** | Generar los mecanismos administrativos de adopción de la gestión sistemática de riesgos de seguridad digital, bajo la metodología establecida, en todos los ministerios y departamentos administrativos de orden nacional. | PRESIDENCIA<br>DAFP | 2Q2017 |
| | | **A1.3.4.** | Crear una guía metodológica para la identificación de riesgos de seguridad digital, dirigida a todos los actores de interés, siendo éstos el Gobierno Nacional, las organizaciones públicas y privadas y la sociedad civil. | PRESIDENCIA<br>DNP<br>MINTIC | 2Q2017 |
| | | **A1.3.5.** | Crear una guía metodológica para la evaluación del impacto socio económico de la gestión sistemática de riesgos de seguridad digital, dirigida a todos los actores de interés, siendo éstos el Gobierno Nacional, las organizaciones públicas y privadas y la sociedad civil. | PRESIDENCIA<br>DNP<br>MINTIC | 2Q2017 |
| **M1.4** | Programas, proyectos y campañas de socialización y concientización a todos los actores de interés debidamente diseñados, respecto de los aspectos relevantes de la economía digital y de la política de seguridad digital, con un enfoque de gestión de riesgos. | **A1.4.1.** | Fortalecer la estrategia *En TIC Confío* del MINISTERIO TIC, mediante el cual se promueva la confianza en el uso del entorno digital y la gestión de riesgos de seguridad digital en Colombia. | MINTIC | 1Q2017 |
| | | **A1.4.2.** | Crear campañas nacionales de concientización destinada a aumentar la confianza en el uso del entorno digital, con enfoque en la salvaguarda de los derechos humanos y los valores fundamentales. | MINEDUCACIÓN<br>MINCULTURA<br>MINTIC | 2Q2017 |
| | | **A1.4.3.** | Diseñar programas y proyectos de concientización de todos los actores de interés respecto de la Seguridad Digital. | MINEDUCACIÓN<br>MINCULTURA<br>MINTIC | 2Q2017 |
| | | **A1.4.4.** | Diseñar un plan de socialización de la guía metodológica para la identificación de riesgos de seguridad digital, dirigida a todos los actores de | PRESIDENCIA<br>MINTIC | 3Q2017 |

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE1 | Fortalecer la capacidad institucional, normativa, administrativa y de gestión en materia de seguridad digital para Colombia, desde el más alto nivel | | | | |
| **Código de Meta** | **Meta** | **Código de Acción** | **Acción** | **Entidad Responsable** | **Fecha de Finalización** |
| | | | interés, siendo éstos el Gobierno Nacional, las organizaciones públicas y privadas y la sociedad civil. | | |
| | | A1.4.5. | Diseñar un plan de socialización de la guía metodológica para la evaluación del impacto socio económico de la gestión sistemática de riesgos de seguridad digital, dirigida a todos los actores de interés, siendo éstos el Gobierno Nacional, las organizaciones públicas y privadas y la sociedad civil. | PRESIDENCIA MINTIC | 3Q2017 |
| M1.5 | Programas y proyectos de educación y fortalecimiento de capacidades a todos los actores de interés debidamente diseñados, respecto de los aspectos relevantes de la economía digital y de la política de seguridad digital, con un enfoque de gestión de riesgos. | A1.5.1. | Crear contenido educativo respecto de los beneficios de la gestión de riesgos de seguridad digital en el desarrollo de actividades económicas y sociales en un entorno digital abierto dirigido a todos los actores de interés. | MINEDUCACION MINTIC | 2Q2017 |
| | | A1.5.2. | Diseñar programas y proyectos de fortalecimiento de capacidades de todos los actores de interés, respecto de la Seguridad Digital. | MINEDUCACION MINTIC | 2Q2017 |
| | | A1.5.3. | Crear material metodológico educativo para capacitar a los maestros de educación básica (primaria y secundaria), media y superior, respecto de los beneficios de la gestión de riesgos de seguridad digital. | MINEDUCACION | 2Q2017 |
| | | A1.5.4. | Modernizar los currículos de educación básica (primaria y secundaria) y media, incluyendo contenidos educativos asociados a la gestión de riesgos de seguridad digital. | MINEDUCACION | 3Q2017 |
| | | A1.5.5. | Promover la inclusión en todos los programas de educación superior de contenidos educativos asociados a la gestión de riesgos de seguridad digital. | MINEDUCACION | 3Q2017 |

Fuente: MINISTERIO TIC, 2015

La Tabla A.2 presenta veinticinco acciones que serán adelantadas por cada una de las entidades responsables y con el fin de alcanzar las cinco metas propuestas para fomentar la prosperidad económica y social del país con la promoción de un entorno que permita desarrollar actividades digitales de manera abierta, confiable y segura.

**Tabla A.2. Acciones para fomentar la prosperidad económica y social del país con la promoción de un entorno que permita desarrollar actividades digitales de manera abierta, confiable y segura**

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE2 | Fomentar la prosperidad económica y social del país con la promoción de un entorno que permita desarrollar actividades digitales de manera abierta, confiable y segura | | | | |
| **Código de Meta** | **Meta** | **Código de Acción** | **Acción** | **Entidad Responsable** | **Fecha de Finalización** |
| M2.1 | Marco legal y regulatorio armonizado para que todos los actores de interés implementen el marco de trabajo (principios y estrategias) de la Política | A2.1.1. | Compilar y actualizar la regulación en el sector de TIC teniendo en cuenta aspectos necesarios para la gestión de riesgos de seguridad digital. | MINTIC | 3Q2017 |
| | | A2.1.2. | Armonizar la normatividad que permita realizar eficientemente el almacenamiento, la retención y los procedimientos del suministro de información por | MINTIC MINJUSTICIA MINDEFENSA | 3Q2017 |

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE2 | Fomentar la prosperidad económica y social del país con la promoción de un entorno que permita desarrollar actividades digitales de manera abierta, confiable y segura | | | | |
| **Código de Meta** | **Meta** | **Código de Acción** | **Acción** | **Entidad Responsable** | **Fecha de Finalización** |
| | Nacional de Seguridad Digital en sus actividades económicas y sociales. | | parte de los proveedores de servicio de Internet en Colombia. | | |
| | | **A2.1.3.** | Actualizar la Ley Estatutaria No. 1621 del 17 de abril de 2013 de inteligencia y contrainteligencia, con el fin de enmarcar las actividades relacionadas con la seguridad digital, haciendo énfasis en la Ciberseguridad y la Ciberdefensa. | MINDEFENSA MINJUSTICIA | 3Q2017 |
| | | **A2.1.4.** | Adelantar un estudio de mejores prácticas respecto de los marcos legales y regulatorios a nivel internacional en torno a la protección de la privacidad y los datos personales bajo la gestión de riesgos de seguridad digital. | MINTIC | 2Q2017 |
| | | **A2.1.5.** | Adelantar un estudio de mejores prácticas respecto de los marcos legales y regulatorios a nivel internacional en torno a los derechos humanos, el derecho internacional humanitario y los valores fundamentales bajo la gestión de riesgos de seguridad digital. | MINJUSTICIA MINTIC | 2Q2017 |
| **M2.2** | Incremento en el uso del entorno digital global, abierto, interconectado y dinámico por parte de todos los actores de interés maximizando beneficios económicos y sociales, mediante la gestión de riesgos de seguridad digital. | **A2.2.1.** | Recomendar a las instancias de máximo nivel del Gobierno en Seguridad Digital, medidas de articulación y coherencia de la gestión de riesgos de seguridad digital con i) el Plan Nacional de Desarrollo 2014-2018 "*Todos por un Nuevo País – Paz, Equidad y Educación*", ii) con el Plan Vive Digital 2014-2018, y iii) con otras estrategias que fomenten la prosperidad económica y social en Colombia en el corto y mediano plazo. | DNP MINTIC | 4Q2016 |
| | | **A2.2.2.** | Identificación y reporte a las instancias de máximo nivel del Gobierno en Seguridad Digital de los servicios públicos prestados ya sea por entidades públicas o privadas que utilicen directa o indirectamente el entorno digital. | TODOS LOS MINISTERIOS | 4Q2016 |
| | | **A2.2.3.** | Revisión de la política sectorial e identificación y reporte a las instancias de máximo nivel del Gobierno en Seguridad Digital de sus objetivos económicos y sociales que implican actividades en el entorno digital sobre las cuales podrían existir riesgos de seguridad digital. | TODOS LOS MINISTERIOS | 4Q2016 |
| | | **A2.2.4.** | Capacitar al resto de entidades del sector público respecto de las ventajas de un entorno digital global, abierto, interconectado y dinámico que maximice los beneficios económicos y sociales mediante la gestión de riesgos de seguridad digital. | MINTIC | 1Q2017 |
| | | **A2.2.5.** | Evaluar la Política Nacional de Seguridad Digital, estimar el impacto económico de la misma sobre los actores de interés y estimular mejoras continuas en eficiencia y eficacia de la gestión de riesgos de seguridad digital. | DNP | 4Q2019 |
| **M2.3** | Gestión de riesgos de seguridad digital implementada por parte de todos los actores de interés del sector público y evaluación del impacto socio económico de la política, así como la promoción de su | **A2.3.1.** | Identificar los riesgos de seguridad digital, mediante la guía metodológica establecida. | TODOS LOS MINISTERIOS | 2Q2017 |
| | | **A2.3.2.** | Adoptar y aplicar la metodología de gestión de riesgos de seguridad digital establecida. | TODOS LOS MINISTERIOS | Continuo desde 3Q2017 |
| | | **A2.3.3.** | De acuerdo con el modelo detallado de coordinación definido, informar el avance periódico de aplicación de la gestión de riesgos de seguridad digital a las | TODOS LOS MINISTERIOS | Continuo desde 1Q2018 |

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE2 | Fomentar la prosperidad económica y social del país con la promoción de un entorno que permita desarrollar actividades digitales de manera abierta, confiable y segura | | | | |
| **Código de Meta** | **Meta** | **Código de Acción** | **Acción** | **Entidad Responsable** | **Fecha de Finalización** |
| | implementación a los actores de interés del sector privado y de la sociedad civil. | | instancias de máximo nivel del Gobierno en Seguridad Digital. | | |
| | | A2.3.4. | Evaluar el impacto socio económico de la gestión de riesgos de seguridad digital, mediante la guía metodológica establecida. | TODOS LOS MINISTERIOS | 4Q2018 y 4Q2019 |
| | | A2.3.5. | De acuerdo con el modelo detallado de coordinación definido, informar los resultados de la evaluación de impacto socio económico a las instancias de máximo nivel del Gobierno en Seguridad Digital. | TODOS LOS MINISTERIOS | 1Q2019 y 1Q2020 |
| M2.4 | Programas, proyectos y campañas de socialización y concientización a todos los actores de interés debidamente implementados, respecto de los aspectos relevantes de la economía digital y de la política de seguridad digital, con un enfoque de gestión de riesgos. | A2.4.1. | Implementar los programas y proyectos de concientización bajo el enfoque de cada sector a todos los actores de interés respecto de la Seguridad Digital | PRESIDENCIA TODOS LOS MINISTERIOS | Continuo desde 3Q2017 |
| | | A2.4.2. | Concientizar a todos los actores de interés respecto de aspectos del Derecho Internacional Humanitario y los Derechos Humanos en el entorno digital. | MINJUSTICIA MINTIC | Continuo desde 3Q2017 |
| | | A2.4.3. | Mapear la relación entre las redes de la administración pública y sus proveedores de Internet con el fin de garantizar una cooperación eficaz en el manejo de incidentes de seguridad digital. | PRESIDENCIA TODOS LOS MINISTERIOS | Continuo desde 3Q2017 |
| | | A2.4.4. | Promover el uso de la guía metodológica para la identificación de riesgos de seguridad digital por parte del sector privado y de la sociedad civil. | PRESIDENCIA TODOS LOS MINISTERIOS | Continuo desde 3Q2017 |
| | | A2.4.5. | Promover el uso de la guía metodológica para la para la evaluación del impacto socio económico de la gestión de riesgos de seguridad digital por parte del sector privado y de la sociedad civil. | PRESIDENCIA TODOS LOS MINISTERIOS | Continuo desde 3Q2018 |
| M2.5 | Programas y proyectos de educación y fortalecimiento de capacidades a todos los actores de interés debidamente implementados, respecto de los aspectos relevantes de la economía digital y de la política de seguridad digital, con un enfoque de gestión de riesgos. | A2.5.1. | Implementar los programas y proyectos de fortalecimiento de capacidades de todos los actores de interés respecto de la Seguridad Digital. | MINEDUCACION MINTIC MINDEFENSA | Continuo desde 3Q2017 |
| | | A2.5.2. | Capacitar a los maestros de educación básica, media y superior respecto de los beneficios de la gestión de riesgos de seguridad digital. | MINEDUCACION | Continuo desde 4Q2017 |
| | | A2.5.3. | Hacer seguimiento para asegurar que los currículos de educación básica (primaria y secundaria) y media en Colombia, incluyan los contenidos educativos asociados a la gestión de riesgos de seguridad digital. | MINEDUCACION | Continuo desde 2Q2018 |
| | | A2.5.4. | Hacer seguimiento de la inclusión de contenidos educativos asociados a la gestión de riesgos de seguridad digital en todos los programas de educación superior en Colombia. | MINEDUCACION | Continuo desde 2Q2018 |
| | | A2.5.5. | Crear e implementar una estrategia de permanencia del talento humano que desarrolla actividades relacionadas con la seguridad digital en las organizaciones públicas. | PRESIDENCIA TODOS LOS MINISTERIOS | Continuo desde 4Q2016 |

Fuente: MINISTERIO TIC, 2015



La Tabla A.3 presenta diecisiete acciones que serán adelantadas por cada una de las entidades responsables y con el fin de alcanzar las cinco metas propuestas para garantizar la integridad y seguridad de los individuos, a nivel nacional y trasnacional, bajo un entorno digital creciente y dinámico.

## Tabla A.3. Acciones para garantizar la integridad y seguridad de los individuos, a nivel nacional y trasnacional, bajo un entorno digital creciente y dinámico

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE3 | Garantizar la integridad y seguridad de los individuos, a nivel nacional y trasnacional, bajo un entorno digital creciente y dinámico | | | | |
| **Código de Meta** | **Meta** | **Código de Acción** | **Acción** | **Entidad Responsable** | **Fecha de Finalización** |
| M3.1 | Marco legal y regulatorio comprensible, efectivo y adecuado con el fin de asegurar la seguridad nacional en un entorno digital. | A3.1.1. | Armonizar el marco legal y regulatorio con las necesidades en materia de prevención, detección y atención de delitos y crímenes en el entorno digital. | MINDEFENSA<br>MINJUSTICIA<br>MINTIC | 3Q2017 |
| | | A3.1.2. | Armonizar el marco legal y regulatorio con las necesidades en materia de investigación, persecución y criminalización de nuevos tipos de delitos y crímenes en el entorno digital y presentar un proyecto de ley al Congreso de la República que incluya a los delitos informáticos como delitos fuente de lavado de activos. | MINDEFENSA<br>MINJUSTICIA<br>MINTIC<br>UIAF | 3Q2017 |
| M3.2 | Instancias y entidades de investigación y combate al crimen y la delincuencia en un entorno digital fortalecidas. | A3.2.1. | Fortalecer la capacidad administrativa del *Centro Cibernético Policial* (CCP) de la Policía Nacional de Colombia, adecuando la estructura orgánica de la entidad. Así mismo fortalecer la Unidad de Información y Análisis Financiero (UIAF) | PRESIDENCIA<br>MINDEFENSA | 1Q2017 |
| | | A3.2.2. | Implementar el Centro de Fusión para Investigación de Crímenes Económicos y Financieros (C2F2). | MINDEFENSA | 2Q2017 |
| | | A3.2.3. | Implementar el Centro de Comunicaciones, Cómputo, Control y Comando para la Seguridad Digital (C4C) | MINDEFENSA | 2Q2017 |
| | | A3.2.4. | Crear y fortalecer y el observatorio de delitos en entorno digital, los laboratorios de informática forense y los centros de investigación en seguridad digital. | MINDEFENSA<br>MINTIC | 3Q2017 |
| | | A3.2.5. | Mapear la relación entre las redes de la administración pública y sus proveedores de Internet con el fin de garantizar una cooperación eficaz en el manejo de incidentes de seguridad digital. | TODOS LOS MINISTERIOS | Continuo desde 4Q2016 |
| M3.3 | Marco de trabajo para mitigar el crimen y la delincuencia que atenten contra la seguridad nacional en un entorno digital, basado en un enfoque de gestión sistémica de riesgos de seguridad digital. | A3.3.1. | Adoptar y aplicar la metodología de gestión de riesgos de seguridad digital establecida por parte del CCP de la Policía Nacional. | MINDEFENSA | Continuo desde 3Q2017 |
| | | A3.3.2. | De acuerdo con el modelo detallado de coordinación definido, informar el avance periódico de aplicación de la gestión de riesgos de seguridad digital por parte del CCP de la Policía Nacional a las instancias de máximo nivel del Gobierno en Seguridad Digital. | MINDEFENSA | Continuo desde 1Q2018 |
| M3.4 | Mecanismos de socialización y concientización de tipologías comunes de crimen y delincuencia en un entorno digital que afecten la seguridad nacional y la manera de gestionar sus riesgos por parte de los actores de interés. | A3.4.1. | Socializar periódicamente a todos los actores de interés respecto de los avances en el combate al crimen y a la delincuencia que atenten contra la seguridad nacional en el entorno digital. | MINDEFENSA | Continuo desde 3Q2018 |
| | | A3.4.2. | Crear una red de vigilancia nacional de la Infraestructura Crítica Nacional con el sector privado y la sociedad civil. | MINDEFENSA<br>MINTIC | 2Q2017 |
| | | A3.4.3. | Promover la implementación de CSIRTs sectoriales, definidos de acuerdo a la catalogación de las infraestructuras críticas nacionales. | PRESIDENCIA<br>MINDEFENSA | Continuo desde 4Q2016 |
| | | A3.4.4. | Promover el desarrollo de tanques de pensamiento para abordar con innovación la gestión sistemática de riesgos de seguridad digital | PRESIDENCIA<br>MINDEFENSA<br>MINTIC | Continuo desde 2Q2017 |
| | | A3.4.5. | Diseñar e implementar esquemas tecnológicos y procedimentales para garantizar la identificación, autenticación y autorización de funcionarios, ciudadanos, activos de información y recursos que acceden a la infraestructura del Estado colombiano. | PRESIDENCIA<br>MINTIC | 2Q2017 |
| M3.5 | Funcionarios públicos responsables de garantizar la seguridad nacional en el | A3.5.1. | Diseñar contenido educativo para fortalecer las capacidades de los funcionarios de las entidades de administración de justicia en Colombia responsables de | MINDEFENSA<br>MINJUSTICIA | 1Q2017 |

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE3 | Garantizar la integridad y seguridad de los individuos, a nivel nacional y trasnacional, bajo un entorno digital creciente y dinámico | | | | |
| Código de Meta | Meta | Código de Acción | Acción | Entidad Responsable | Fecha de Finalización |
| | entorno digital debidamente capacitados. | | adelantar actuaciones asociadas con la Seguridad Digital. | | |
| | | A3.5.2. | Capacitar a los funcionarios de las entidades de administración de justicia en Colombia responsables de adelantar actuaciones asociadas con la Seguridad Digital. | MINDEFENSA MINJUSTICIA | Continuo desde 2Q2017 |
| | | A3.5.3. | Fortalecer las capacidades y posibilidades de los funcionarios públicos para llevar a cabo pruebas y simulaciones de incidentes de seguridad digital. | MINDEFENSA | Continuo desde 2Q2017 |

Fuente: MINISTERIO TIC, 2015

La Tabla A.4 presenta diecisiete acciones que serán adelantadas por cada una de las entidades responsables y con el fin de alcanzar las cinco metas propuestas para fortalecer la defensa y soberanía nacional bajo un entorno digital.

Tabla A.4. Acciones para fortalecer la defensa y soberanía nacional bajo un entorno digital

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE4 | Fortalecer la defensa y soberanía nacional bajo un entorno digital | | | | |
| Código de Meta | Meta | Código de Acción | Acción | Entidad Responsable | Fecha de Finalización |
| M4.1 | Marco legal y regulatorio comprensible, efectivo y adecuado con el fin de asegurar la defensa nacional en un entorno digital. | A4.1.1. | Adelantar una compilación de la normatividad en todos los sectores que impacte la Infraestructura Crítica Nacional con el fin de identificar medidas de seguridad digital entorno a la misma. | PRESIDENCIA MINTIC MINDEFENSA | 2Q2017 |
| | | A4.1.2. | Armonizar el marco legal y regulatorio con las necesidades en materia de protección de la Infraestructura Crítica Nacional con un enfoque de gestión de riesgos de seguridad digital. | PRESIDENCIA TODOS LOS MINISTERIOS | 3Q2017 |
| M4.2 | Instancias y entidades de protección de los intereses del país en un entorno digital y de las infraestructuras críticas fortalecidas. | A4.2.1. | Fortalecer la capacidad administrativa y operativa del *Comando Conjunto Cibernético* (CCOC) del Comando General de las Fuerzas Armadas (CGFM) de Colombia, de las Unidades Cibernéticas de las Fuerzas Militares y de los organismos de Inteligencia del Estado., adecuando la estructura orgánica de la entidad. | PRESIDENCIA MINDEFENSA | 1Q2017 |
| | | A4.2.2. | Crear el Centro Nacional de Protección y Defensa de Infraestructura Critica Nacional liderado por el CCOC y los Centros de Operaciones cibernéticas de las Fuerzas Militares. | MINDEFENSA | 2Q2017 |
| | | A4.2.3. | Elaborar el catálogo de Infraestructura Crítica Nacional con un enfoque de gestión de riesgos de seguridad digital y actualizarlo periódicamente. | MINDEFENSA | 3Q2017 |
| | | A4.2.4. | Desarrollar una plataforma automatizada para compartir información con todos los actores de interés sobre amenazas e incidentes de seguridad digital. | MINDEFENSA | 4Q2017 |
| | | A4.2.5. | Estructurar, actualizar e implementar las guías de Riesgo Operacional para la protección y mejora de la resiliencia de la Infraestructura Crítica Nacional. | MINDEFENSA | 2Q2017 |
| M4.3 | Marco de trabajo para asegurar la defensa nacional en un entorno digital, basado | A4.3.1. | Adoptar y aplicar la metodología de gestión de riesgos de seguridad digital establecida por parte del CCOC del CGFM. | MINDEFENSA | Continuo desde 3Q2017 |

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE4 | Fortalecer la defensa y soberanía nacional bajo un entorno digital | | | | |
| Código de Meta | Meta | Código de Acción | Acción | Entidad Responsable | Fecha de Finalización |
| | en un enfoque de gestión sistémica de riesgos de seguridad digital. | A4.3.2. | De acuerdo con el modelo detallado de coordinación definido, informar el avance periódico de aplicación de la gestión de riesgos de seguridad digital por parte del CCOC del CGFM a las instancias de máximo nivel del Gobierno en Seguridad Digital. | MINDEFENSA | Continuo desde 1Q2018 |
| M4.4 | Mecanismos de socialización y concientización de tipologías comunes de ataques que atenten contra la defensa nacional en entorno digital y la manera de gestionar sus riesgos por parte de los actores de interés. | A4.4.1. | Socializar los planes de protección y defensa de la Infraestructura Critica Nacional a todos los actores de interés. | MINDEFENSA | Continuo desde 3Q2017 |
| | | A4.4.2. | Socializar y concientizar a todos los agentes de interés en las tipologías comunes de ataques que atenten contra la defensa nacional en entorno digital y la manera de gestionar sus riesgos por parte de los actores de interés. | MINDEFENSA | Continuo desde 3Q2017 |
| | | A4.4.3. | Realizar mesas de trabajo y convenios con todos los actores de interés que fomenten la discusión y la investigación con innovación respecto de la gestión de riesgos de seguridad digital | MINDEFENSA | Continuo desde 3Q2017 |
| | | A4.4.4. | Informar a las organizaciones privadas acerca de las ventajas de los CSIRTs en los respectivos sectores e industrias promoviendo su creación. | PRESIDENCIA MINDEFENSA | Continuo desde 4Q2016 |
| | | A4.4.5. | Establecer un grupo de trabajo integrado por representantes de todas las organizaciones que se ocupan de la investigación desarrollo e innovación en el campo de la seguridad digital. | PRESIDENCIA MINDEFENSA MINTIC | 1Q2017 |
| M4.5 | Funcionarios públicos que trabajen con infraestructuras críticas en cualquier sector de la economía debidamente capacitados. | A4.5.1. | Diseñar contenido educativo para fortalecer las capacidades de los funcionarios responsables de garantizar la seguridad digital, haciendo énfasis en la ciberdefensa, con un enfoque de gestión de riesgos | MINDEFENSA MINJUSTICIA | 1Q2017 |
| | | A4.5.2. | Capacitar a los funcionarios de los responsables de garantizar la seguridad digital, haciendo énfasis en la ciberdefensa, con un enfoque de gestión de riesgos | MINDEFENSA MINJUSTICIA | Continuo desde 2Q2017 |
| | | A4.5.3. | Fortalecer las capacidades y posibilidades de los funcionarios públicos para llevar a cabo pruebas y simulaciones de incidentes de seguridad digital sobre la Infraestructura Crítica Nacional. | PRESIDENCIA MINDEFENSA | Continuo desde 2Q2017 |

Fuente: MINISTERIO TIC, 2015



La Tabla A.5 presenta dieciséis acciones que serán adelantadas por cada una de las entidades responsables y con el fin de alcanzar las cinco metas propuestas para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

### Tabla A.5. Acciones impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE5 | impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional | | | | |
| Código de Meta | Meta | Código de Acción | Acción | Entidad Responsable | Fecha de Finalización |
| M5.1 | Marco de cooperación, colaboración y asistencia a | A5.1.1. | Desarrollar e implementar una Agenda Estratégica de cooperación, colaboración y asistencia nacional e internacional en temas de seguridad digital. | CANCILLERIA MINTIC MINDEFENSA | 1Q2017 |

| Código de Objetivo | Objetivo Estratégico | | | | |
|---|---|---|---|---|---|
| OE5 | impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional | | | | |
| Código de Meta | Meta | Código de Acción | Acción | Entidad Responsable | Fecha de Finalización |
| | nivel nacional e internacional, en torno a la seguridad digital. | A5.1.2. | Revisión del marco jurídico vigente con el fin de implementar la diplomacia digital en Colombia. | CANCILLERIA | 4Q2016 |
| M5.2 | Mecanismos de cooperación, colaboración y asistencia en torno a la seguridad digital, y estímulo del uso de estándares internacionales seguros e interoperables. | A5.2.1. | Identificación de estándares internacionales seguros e interoperables en torno a la seguridad digital. | MINTIC MINDEFENSA | 1Q2017 |
| | | A5.2.2. | Fomentar la creación y adhesión a redes de intercambio internacionales de información de seguridad digital. | CANCILLERIA MINTIC MINDEFENSA | 1Q2017 |
| | | A5.2.3. | Garantizar la presencia del colCERT, el CCP y el CCOC en organismos internacionales que traten el tema de seguridad digital. | CANCILLERIA MINDEFENSA | 4Q2016 |
| | | A5.2.4. | Garantizar la firma de acuerdos de cooperación, colaboración o asistencia entre el colCERT, el CCP y el CCOC, a nivel regional y mundial. | CANCILLERIA MINDEFENSA | 1Q2017 |
| | | A5.2.5. | Fortalecer y garantizar la presencia del enlace de la Policía Nacional de Colombia en el EC3 de EUROPOL y el IGCI de INTERPOL. | CANCILLERIA MINDEFENSA | 1Q2017 |
| M5.3 | Asistencia de representantes del país en eventos relevantes para compartir experiencias y mejores prácticas en la gestión de riesgos de seguridad digital, así como para establecer relaciones con todos los actores de interés, sean estos nacionales o internacionales. | A5.3.1. | Identificar mejores prácticas en la gestión de riesgos de seguridad digital en el país, con el fin de colaborar y asistir a otros países u organizaciones internacionales. | PRESIDENCIA | Continuo desde 2Q2017 |
| | | A5.3.2. | Participar en eventos regionales e internacionales pertinentes para compartir experiencias y buenas prácticas en la gestión de riesgos de seguridad digital. | CANCILLERIA MINDEFENSA MINTIC | Continuo desde 2Q2017 |
| | | A5.3.3. | Establecer relaciones bilaterales y multilaterales entorno a la gestión de riesgos de seguridad digital. | CANCILLERIA MINDEFENSA MINTIC | Continuo desde 2Q2017 |
| M5.4 | Mejores prácticas a nivel nacional e internacional en torno a la socialización y concientización de actores de interés debidamente implementadas, respecto a aspectos relacionados con la seguridad digital, con un enfoque de gestión de riesgos. | A5.4.1. | Establecer un acuerdo marco para la cooperación con el sector privado respecto de la identificación de mejores prácticas de seguridad digital, con un enfoque de gestión de riesgos | MINDEFENSA MINTIC | 1Q2017 |
| | | A5.4.2. | Fomentar programas de intercambio académico con países aliados en temas asociados a la Seguridad Digital. | CANCILLERIA MINDEFENSA MINTIC | Continuo desde 2Q2017 |
| | | A5.4.3. | Establecer y desarrollar la cooperación entre los servicios de inteligencia del país y entre las entidades nacionales e internacionales pertinentes en materia de seguridad digital. | CANCILLERIA MINDEFENSA | 1Q2017 |
| M5.5 | Asistencia de representantes del país en asuntos de diplomacia y de los actores de interés en programas internacionales de capacitación en temas de seguridad digital, con un enfoque de gestión de riesgos. | A5.5.1. | Establecer una figura de enlace en la CANCILLERIA para abordar los temas de seguridad digital en el marco de la diplomacia digital. | CANCILLERIA | 4Q2016 |
| | | A5.5.2. | Crear e implementar un diplomado en Diplomacia Digital asociado al tema de seguridad digital dirigido a todos los actores de interés. | MINDEFENSA MINTIC CANCILLERIA | 2Q2017 |
| | | A5.5.3. | Promover la participación de representantes de los actores de interés en programas internacionales de capacitación en temas de seguridad digital. | MINDEFENSA MINTIC CANCILLERIA | 2Q2017 |

Fuente: MINISTERIO TIC, 2015

## ANEXO B: Estimación del impacto económico de la adopción e implementación de la Política nacional de seguridad digital para Colombia

La Comisión de Regulación de Comunicaciones (CRC) de Colombia, con apoyo de la Dirección de Estudios Económicos del Departamento Nacional de Planeación, estimó de manera preliminar 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.

El MEGC dinámico de la CRC es un instrumento de simulación económica y de evaluación de impactos 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 construidas sobre la base de la teoría económica generalmente aceptada, interactuando con aspectos fiscales y monetarios e 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.

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 presenta a modo de ilustración las características y los resultados del escenario base, de la Política Nacional de Seguridad Digital, la cual deberá fundamentarse en lograr que el Gobierno Nacional, las organizaciones públicas y privadas, la academia y la sociedad civil en Colombia, hagan un uso responsable y seguro del entorno digital abierto, a través del fortalecimiento de sus capacidades para identificar y gestionar los riesgos de las actividades digitales, maximizando así los beneficios obtenidos de una mayor prosperidad económica, política y social del país.

- Escenario Base

Los siguientes son los supuestos considerados y los resultados estimados con el MEGC para el Escenario Base:

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, 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 y 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 US$3.000 y US$6.000 millones de dólares.

Resultados

Para el Escenario Base, la tasa de crecimiento promedio anual entre 2010 y 2020, del Producto Interno Bruto nacional (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 y 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 inflacionarios a las que está expuesta la economía nacional, superando las metas establecidas por Banco de la Republica (entre 2% y 3% anual). De igual manera, 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 sustancial 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 éstos 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 todos los actores de interés en Colombia: i) Gobierno nacional, organizaciones públicas y privadas, academia y sociedad civil. El escenario contempla las políticas aplicadas durante 2015 y una proyección hipotética del mismo 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, 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 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 enfocada a la gestión de riesgos para la 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.

- De la misma manera, se debe tener en cuenta que el segundo efecto grande 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 implicado. 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 debe realizar un gasto adicional en la protección de la infraestructura crítica 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, 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" [21] 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, protegiendo la propiedad intelectual evitando el plagio o copia de los desarrollos realizado por las empresas, reflejado en un aumento en el crecimiento económico. El modelamiento de este efecto será a través de un aumento en la inversión privada.

Se realizarán 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.

[21] El efecto "*crowding out*" es el efecto desplazamiento es una situación en la que la capacidad de inversión de las empresas se reduce debido a la deuda pública.

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). De igual manera, una inflación de alrededor del 5% no representa una amenaza latente para la economía colombiana.

En términos de ocupación, la Política Nacional de Seguridad Digital en Colombia habría creado 307.222 puestos de trabajo adicionales en la economía nacional. En el tema de ocupación esta cifra podría ser elevada, pero al ser un promedio de los últimos años, se puede pensar que esté sobre estimado este valor, ya que el crecimiento del empleo en los últimos años fue significativo, por ende esta cifra debe tomarse con cautela. El mayor gasto público y la mayor inversión pública que el plan implica son los responsables de dichos mayores crecimiento y ocupación.

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

A pesar de causar un leve crecimiento económico, la Política Nacional de Seguridad Digital tiene un impacto positivo sobre muchos sectores de la economía que no son medibles o que por el mismo tamaño de la misma, sus efectos se ven diluidos en los diferentes canales de trasmisión de la política. 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 ultimo 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.