Comentarios al CONPES sobre seguridad digital desde Sociedad Civil

Bogotá, 5 de febrero de 2016

El presente documento incluye los comentarios al Documento CONPES "Política Nacional de Seguridad Nacional" de las siguientes organizaciones

- Fundación Karisma (www.karisma.org.co)
- Fundación para la Libertad de Prensa (www.flip.org.co)
- Comisión Colombiana de Juristas (http://www.coljuristas.org)

Las siguientes personas naturales
- Amalia M. Toledo Hernández
- Germán Realpe Delgado
- Julio Gaitán Bohórquez
- Heidy Balanta

Reconocemos en el ejercicio propuesto por el gobierno nacional una intención de escuchar a los diferentes sectores y ampliar de esta forma su visión de la política de seguridad digital en el país. Sin embargo, llamamos la atención en el sentido de que el plazo otorgado para presentar comentarios resulta muy corto para la complejidad y extensión de este tema y por tanto los temas que se desarrollan en este documento pueden no ser suficientes ni ser desarrollados en la forma que nos gustaría hacerlo.

1.Comentarios a la Introducción

Para hacer la política, específicamente en la parte de darle contenido al principio del CONPES (PF1) *"Salvaguardar los derechos humanos y los valores fundamentales de los individuos (…)"* debía haberse tenido en cuenta, entre otros, los siguientes documentos que condensan los estándares internacionales y regionales para la defensa de derechos humanos en el contexto digital:

PROPUESTA DE REFERENCIAS A INCLUIR:

- Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. Comunicado de prensa sobre la adquisición e implementación de programas de vigilancia por parte de Estados del hemisferio (21 de julio de 2015).

- Declaración conjunta de las relatorías para Libertad de Expresión de la ONU y la OEA sobre programas de vigilancia y su impacto en la libertad de expresión.

- CIDH. Informe sobre Terrorismo y Derechos Humanos de la Comisión Interamericana de Derechos Humanos. OEA/Ser.L/V/II.116 Doc. 5 rev. 1 corr. 22 de octubre de 2002.

- Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A/HRC/23/40. 17 de abril de 2013.

- CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013 Ver:

- Declaración conjunta sobre libertad de expresión e internet de las relatorías para la libertad de expresión de la ONU, OSCE, OEA y CADHP. Ver.

- Naciones Unidas. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos El Derecho a la Privacidad en la Era Digital. A/HRC/27/37. 30 de junio de 2014.

- Naciones Unidas, Consejo de Derechos Humanos. Principios Rectores Sobre las Empresas y los Derechos Humanos. 2011.

2. Comentarios a los antecedentes y justificación

Con respecto a borradores anteriores del documento, la última versión supera la visión militar y desarrolla un enfoque económico del entorno digital. Sin embargo, aunque sugiere la importancia de la seguridad digital en lo social, no se ocupa de esta dimensión. La invisibilidad de los antecedentes que sugerimos a continuación explica la falta de acciones concretas destinadas a solucionar las causas que originan esos antecedentes, por lo que en este punto la política es insuficiente. Algunos de los hechos que deberían ser parte del contexto son:

a. Se debe ir más allá de los casos bancarios e incluir reportes sobre los casos de ataques y constantes violaciones a la seguridad digital de sectores de la sociedad colombiana que, dado el contexto de conflicto armado y posible postconflicto, resultan especialmente vulnerables: periodistas, defensores de derechos humanos, jueces, opositores y miembros de la sociedad civil. Los casos de las Chuzadas, Andrómeda, las recientes persecuciones a periodistas como Vicky Dávila y Claudia Morales y sus equipos de trabajo, el hurto de dispositivos de organizaciones civiles o

el uso de medios digitales para amenazarlas por razón de su trabajo son parte de nuestro contexto. No se trata de casos aislados. Según cifras de la Fundación para la Libertad de Prensa, tanto en 2015 como en 2014 se registraron 6 casos de agresiones contra periodistas en entornos digitales. Por otro lado, según esa misma organización, en el 2014 se presentaron 15 reportes de duplicaciones de cuentas en redes sociales con el fin de atacar la reputación de personas que ejercen el oficio periodístico. Asimismo, diferentes organizaciones de la sociedad civil y personas defensoras de derechos humanos son objeto constante de delitos contra sus sistemas de información[1], como también lo han sido las organizaciones de víctimas del conflicto armado, en especial aquellas vinculadas a los procesos legales de reclamación de tierras[2]

b. Desde el tema bancario la actual Ley 1273 de 2009, se queda corta para el hurto informático y la transferencia no consentida de activos. En la actualidad los delitos informáticos que son llevados en la justicia penal, no son examinados ni por el sector bancario, ni mucho menos por el MINTIC. El papel de las entidades bancarias es mínimo, y solo se limitan a decir que no responden ya que la responsabilidad es del usuario. Se desconoce por completo en los hurtos informáticos los aspectos de responsabilidad objetiva como los controles estrictos que deben tener las entidades financieras en cuanto a seguridad, integridad y manejo de la información.

c. Considerando el actual momento histórico colombiano y el papel que el gobierno ha jugado (y la prioridad que le ha dado al mismo), se debe establecer cómo encaja la nueva política de seguridad digital en el marco del posconflicto. Si esto implica un cambio de doctrina militar y de defensa, y brindar garantías de no repetición a las víctimas del conflicto armado. Ese cambio debe reflejarse en la nueva política y especialmente en el fortalecimiento de los principios de legalidad y de la reserva judicial para ordenar interceptación de comunicaciones. Debería contemplarse, además, el reconocimiento de responsabilidades por parte de todos los actores del conflicto armado en torno a vulneración de los derechos humanos y del derecho internacional humanitario en el ámbito digital.

---

[1] Boletín Trimestral Sistema de Agresiones contra Defensores de Derechos humanos en Colombia, julio-septiembre de 2015. Programa Somos Defensores (http://www.somosdefensores.org/attachments/article/135/Boletin-julio-septiembre-SIADDHH%202015.pdf)
Boletín Trimestral Sistema de Agresiones contra Defensores de Derechos humanos en Colombia, Enero- Marzo de 2014. Programa somos Defensores. (http://www.coljuristas.org/documentos/boletines/siaddhh_ener-mar_2014.pdf).
Terra Digna Denuncia Ante la Opinión Pública Asalto y Robo de información en sus Oficinas (https://justiciaambientalcolombia.org/2016/01/22/tierra-digna-denuncia/)

[2] "Robo de información afecta a la Asociación de Víctimas para la Restitución de Tierras de Urabá" (http://forjandofuturos.org/fundacion/index.php/sala-de-prensa/registro-de-medios/79-registro-de-medios/340-robo-de-informacion-afecta-a-la-asociacion-de-victimas-para-la-restitucion-de-tierras-de-uraba-)
"Roban en juzgado de las oficinas Unidad de Restitución de Tierras" (http://www.cacicastereo.com/index.php?option=com_k2&view=item&id=1124:roban-en-juzgado-de-las-oficinas-unidad-de-restitucion-de-tierras&Itemid=561)
"Encuentran USB robada con información sobre víctimas de 'paras'" (http://www.eltiempo.com/archivo/documento/CMS-8794432)
"El robo de una memoria USB con información confidencial sobre 2.000 víctimas ilustra la amenaza que enfrentan los que piden que se les devuelvan las tierras que les arrebataron" (http://www.semana.com/nacion/articulo/victimas-del-conflicto-mira-reclamar-tierras/234402-3)

d. Dentro de los antecedentes se debe reflejar que algunos estamentos del Estado han tenido injerencias ilegítimas en la intimidad de las comunicaciones de algunos sectores de la sociedad. El abuso de las capacidades de vigilancia de las comunicaciones debe registrarse como un riesgo para la seguridad digital de la sociedad colombiana. Se debe registrar y promover en esta nueva política, como una forma de fortalecimiento de la seguridad digital, el desarrollo de controles a ciertos poderes y facultades del Estado, de modo que los abusos por parte de algunos funcionarios debe ser tenido en cuenta como una fuente de riesgo a la seguridad digital. Del reconocimiento de esta situación como un antecedente podría modificarse algunas acciones ya planteadas, e incluso crear unas nuevas.

e. Es necesario que el documento establezca claros organismos y mecanismos de control y supervisión al cumplimiento de la política y compromiso con los derechos humanos que ella establece.

f. Es necesario que el principio de protección a los derechos humanos que rige al documento CONPES sea desarrollado en el resto del documento, especialmente en las acciones concretas.
g. Es necesario que el documento busque integrar desde su justificación las necesidades en manejo de datos personales y privacidad. En primer lugar en dar una competencia a las instituciones como la Delegatura de Protección de Datos de la SIC, para que pueda realizar mayores controles a las empresas que almacenan, gestionan, datos personales fuera de Colombia. Así mismo, es necesario que desde la propia justificación del documento se analice las actualizaciones a la Ley 1273 de 2009, la cual se queda corta para enfrentar los nuevos tipos de delitos informáticos.

h. El documento de política es consistente en la participación de todos los actores en el marco de la metodología que propone. Sin embargo, es prioritario asignar responsabilidades claras a las empresas, debido al manejo de grandes cantidades de información personal de las personas consumidoras (la ciudadanía). El CONPES debe dejar responsabilidades claras a las empresas en el manejo de los datos, y como eje central debe ser el ciudadano, en el sentido que las medidas combativas para reducir el riesgo de ocurrencia de un delito, no sea el menoscabo de derechos y libertades de las personas.

PROPUESTA DE TEXTO: PENDIENTE POR DESARROLLAR. Desafortunadamente la premura del tiempo no nos permite sino enumerar los hechos que se deben incluir, creemos que de esa enumeración se puede desarrollar los textos que suplirán el vacío reportado

3. Comentarios al marco conceptual

La decisión que se plasma en este documento de basar esta política en la metodología de gestión de riesgos de seguridad digital resulta muy pertinente y la aplaudimos.

Sin embargo, recomendamos que esta gestión de riesgos de seguridad digital se reconozca expresamente como una metodología para hacer que la política de seguridad digital sea *“limitada y proporcionada, y procur[e] cumplir con fines legales precisos, que no*

comprometan las virtudes democráticas que caracterizan a la red".[3] A su vez, esto permitirá conectar el marco conceptual con los principios que se desarrollan más adelante.

La gestión de riesgos de seguridad digital es el mecanismo que permite evaluar desde la perspectiva de derechos humanos si las ganancias resultantes de una recomendación específica de seguridad son proporcionales al impacto resultante sobre los derechos de la ciudadanía. Creemos que en este punto la política se beneficiaría de analizar también las herramientas propuestas por ENISA para la Unión Europea y complementar así la visión que se recoge en el documento a partir de los documentos de la OCDE.

PROPUESTA DE TEXTO A INCLUIR: La gestión de riesgos de seguridad digital servirá para evaluar que las acciones de la política de seguridad digital respondan a los valores democráticos, es decir, que sean limitadas, proporcionadas y alineadas con los fines legales precisos.

PROPUESTA DE REFERENCIA A INCLUIR: European Union Agency for Network and Information Security (ENISA). (2014, 27 de noviembre). *An evaluation framework for cybersecurity strategies*[4].

4. Comentarios al diagnóstico

En el punto 4.2 *"Mesas de trabajo de alto nivel para analizar el estado de la política vigente"* se lee:

> *"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 las políticas de Ciberseguridad y Ciberdefensa para el país"*

El antecedente inmediato de esta solicitud del presidente fue el escándalo destapado por la revista Semana sobre la operación Andrómeda en la que se vieron envueltos funcionarios de la inteligencia militar por acceder ilegítimamente a las comunicaciones de negociadores del proceso de paz, tanto del gobierno como guerrilleros de las FARC, opositores políticos y periodistas. Unas semanas después la intrusión abusiva al correo del presidente fue el detonante de esta solicitud. Consideramos que es importante mencionar ese contexto en forma completa.

PROPUESTA DE TEXTO: Las revelaciones de posibles abusos de las facultades de vigilancia que se habrían realizado contra negociadores del proceso de paz en la Habana (tanto del gobierno como de la guerrilla de las FARC, periodistas y opositores políticos) en

---

[3] Botero, Catalina, Libertad de Expresión e Internet, Comisión Interamericana de Derechos Humanos, OEA/Ser.L/V/II. CIDH/RELE/INF.
11/13, 31 de diciembre de 2013, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf

[4] Disponible en http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1.

una operación fachada de inteligencia militar llamada “Andrómeda” y la filtración de correos personales del Presidente Juan Manuel Santos, fruto de una intrusión abusiva en su cuenta de correo, fueron el detonante y confirmaron el incremento en incidentes de seguridad digital. Es por eso que, en el mes de febrero de 2014, el Presidente Juan Manuel Santos solicitara la creación de una Comisión de Expertos nacionales de alto nivel liderada por los ministerios 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 las políticas de Ciberseguridad y Ciberdefensa para el país.

En el punto 4.3 *“Problemática general”* se establecen cinco problemas de la actual política que tendrían que ser resueltos en esta ocasión. Los problemas denuncian la falta de claridad de la política de seguridad digital, la falta de vinculación de todos los actores, la necesidad de nuevas capacidades para enfrentar delitos, la carencia de capacidades de protección de la infraestructura crítica y la defensa nacional y, finalmente, la obligación de mejorar la cooperación.

Aunque no es equivocada, esta formulación de los problemas de seguridad digital actuales se queda corta respecto a la realidad del país. Como se mencionó anteriormente, han ocurrido graves hechos que comprometen la seguridad digital de la ciudadanía, no ya desde un punto de vista de seguridad nacional o del ahora prevalente financiero o económico, sino que afectan directamente, entre otros, el disfrute del derecho a la intimidad y el ejercicio de la libertad de expresión en todas sus dimensiones.[5] Por tanto, debe reconocerse como parte del problema dimensiones de esa otra realidad

PROPUESTA DE TEXTO: Proponemos agregar los siguientes.

1. Colombia necesita balancear los poderes excepcionales de las diferentes autoridades con controles democráticos adecuados a dichas capacidades. La falta de controles a las capacidades que se otorgan a las fuerzas de seguridad para efectos de combatir el crimen y asegurar la defensa nacional han facilitado el abuso de las facultades legales excepcionales, interfiriendo con derechos fundamentales y afectando ilegítimamente a la ciudadanía en general, pero especialmente a grupos como los periodistas, los/as defensores/as de derechos humanos, víctimas del conflicto armado, líderes/liderezas de oposición y la judicatura.
2. La realidad del posconflicto impone el reconocimiento de sujetos y sectores particularmente vulnerables cuya sensibilidad aumentará por la labor que realizan o el rol que tienen dentro de la sociedad en esta etapa de la historia colombiana. Esto hace que la información que manejan sea de interés especial para determinados sectores que representan riesgos. Adicionalmente, sus condiciones hacen que la forma en que se realizan aproximaciones o acciones concretas a su favor deban tener enfoques diferenciados.
3. En conexión con lo anterior y considerando las particularidades del caso colombiano, al igual que la apuesta que esta nueva política hace por la promoción y defensa de los derechos humanos, se hace necesario plantear una figura asimilable a la de infraestructura crítica para pensar en la protección de estructuras comunicacionales de sectores como el de medios y defensores/as de derechos humanos que garantizan un entorno democrático en el postconflicto y que

[5] Ver “Comentarios a antecedentes”.

permitirían, por ejemplo, establecer que algunas infraestructuras informacionales como bases de datos sensibles (de víctimas, tierras, desmovilizados, etcétera) tengan esa calidad. De esta manera también recibirían una especial protección en virtud de la importancia del trabajo que realizan estas organizacione/instituciones.

5. Comentarios a la definición de la política

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

Comentario: El Objetivo General de la política de seguridad digital tiene varios problemas:

Primero, no habla de que el objetivo sea que en Colombia exista un entorno digital seguro y sano, sino que el Conpes tiene como propósito que los diferentes actores hagan un uso responsable de ese entorno. Más que un objetivo general, pareciera uno instrumental (específico).

Seguidamente, al leer el objetivo se mantiene la pregunta ¿para qué se busca ese ambiente seguro? Aunque algo se vislumbra al decir que “contribuyendo al crecimiento de la economía nacional, y maximizando de esta manera los beneficios obtenidos de una mayor prosperidad económica, política y social del país”, lo que se describe es que el gobierno cambia el foco militar del Conpes de 2011 por uno económico que promueve la OCDE para sus países. En el caso colombiano, se queda corto frente a una realidad social que ya hemos denunciado. Falta la dimensión ciudadana, pues este texto no ofrece un foco en las personas que luego sí se sugiere en los principios que informan la política.

También hay que notar que dentro de los actores falta la comunidad técnica.

Finalmente, el texto parece sugerir que la política es de aplicación exclusiva a las personas nacionales colombianas, dejando de lado a sinnúmero de personas extranjeras que residen y trabajan, inclusive comercian, en el territorio nacional. Por lo tanto, se sugiere que a lo largo del documento, en lugar de hablar de colombianos, se utilice una acepción más amplia como ciudadanía.

PROPUESTA DE TEXTO:
La política nacional de seguridad digital tiene como objetivo lograr un entorno digital colombiano libre, abierto, seguro, confiable e inclusivo con el concurso de todas las partes interesadas: el Gobierno Nacional y los territoriales, las organizaciones públicas y privadas, la academia, la comunidad técnica, y la sociedad civil. Internet en Colombia deberá ser un espacio para el libre ejercicio de los derechos de la ciudadanía y para el crecimiento de la economía nacional que maximice los beneficios obtenidos de una mayor prosperidad económica, política y social del país a través del fortalecimiento de las capacidades de todas las partes interesadas, según corresponda, para identificar, gestionar y mitigar los riesgos de las actividades digitales.

> **Texto 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*

Comentario: No es claro lo que se entiende por “valores fundamentales”. Se debe enfocar la política en los derechos humanos y si se desea, se deben describir los valores fundamentales a los que se refieren, sobre todo, si estos se desarrollan en contextos y diagnóstico ya descritos. Por tanto, se propone el siguiente cambio.

PROPUESTA DE TEXTO PF1:
Mantener un Internet libre, abierto, seguro e inclusivo salvaguardando los derechos humanos de las personas, protegiendo especialmente la libertad de expresión, el derecho a la información, el de la intimidad, el habeas data y la protección de datos, y promoviendo los valores democráticos y del Estado de Derecho. En caso de limitación a estos derechos, debe ser bajo medidas excepcionales y estar conforme con la Constitución Política y los estándares internacionales aplicables. Estas medidas, deben ser proporcionales, necesarias y en un marco de legalidad.

> **Texto 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*

Comentario: Proponemos ajustar el texto para corregir la traducción del inglés de “multistakeholder” por el término “múltiples partes interesadas”, no “actores interesados” como aparece. Además, se debe incluir a la comunidad técnica como una parte actora dentro de esta propuesta. En general, en todos los apartes del documento en los que aparecen “actores de interés” debe hablarse de “múltiples partes interesadas”.

PROPUESTA DE TEXTO PF2:
Adoptar un enfoque incluyente y colaborativo que involucre activamente a todas las partes interesadas en la seguridad digital del país y de sus habitantes, lo que incluye al Gobierno Nacional, los entes territoriales, las organizaciones públicas y privadas, la academia, la comunidad técnica 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.

En el documento en general siempre que aparezca actores interesados se debe hablar de múltiples partes interesadas y si se describen estos actores se debe revisar que siempre estén los mismos, pues no aparece la comunidad técnica y, en ocasiones, no están todos.

> **Texto 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.*

Comentario: La gobernanza, como se desprende del documento CONPES, no tiene que ver con el modelo multistakeholder –de múltiples partes interesadas– que viene funcionando en Internet. La redacción debe reflejar el espíritu de este modelo.

PROPUESTA DE TEXTO DE2:
Gobernanza del entorno digital: articulación y armonización de las múltiples partes interesadas a través del estímulo a su participación, con el fin de gestionar la seguridad digital.

> **Texto DE4:** *Cultura ciudadana para la seguridad digital: sensibilización de todos los actores de interés, para fomentar una cultura ciudadana responsable en la seguridad digital.*

Comentario: Para desarrollar efectivamente la llamada "cultura ciudadana para la seguridad digital", el Estado debe contribuir a través de la construcción de capacidades entre todos las partes interesadas, pero, sobre todo, en la sociedad civil, en la comunidad técnica que defienda sus intereses y en los funcionarios del Estado que deben protegerlos.

PROPUESTA DE TEXTO DE4:
Cultura ciudadana para la seguridad digital: sensibilización y construcción de capacidades de todas las partes interesadas, especialmente de la sociedad civil, de la comunidad técnica y de los funcionarios públicos, para crear y fomentar una cultura ciudadana responsable en la seguridad digital.

6. Sobre el Plan de Acción

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

Comentario: Es necesario determinar con claridad las diferentes funciones de los organismos que pueden hacer de una u otra forma vigilancia de las comunicaciones. En este sentido, debe establecerse la prohibición de usar herramientas tecnológicas que afecten la privacidad de comunicaciones por parte de organismos no facultados para hacerlo.

M 2.1. 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.

Comentario: Es preocupante que en este punto se proponga considerar *"el cibercrimen como una amenaza contra la estabilidad del Estado"*, ya que de este modo se estaría desconociendo el principio básico de separación de poderes. En efecto, la propuesta

atentaría contra la división funcional entre la Policía Nacional y las autoridades judiciales, de un lado, y los organismos de inteligencia y seguridad y las fuerzas armadas (dependientes del Ejecutivo), de otro. La declaración citada autorizaría el tratamiento del crimen y las amenazas a la seguridad nacional como una misma cosa. Por tanto, ese aparte debe desaparecer. Así mismo, debe incluirse la mención al principio fundamental Nº 1 del CONPES.

PROPUESTA DE TEXTO M 2.1
El Gobierno nacional, en todo caso cumpliendo con el principio fundamental n° 1 (PF1), consistente en "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" y la ley 1581 de 2012, 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.

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

Comentario: Sobre este aspecto la metodología de riesgo debería partir sobre el enfoque dado en la norma ISO 31000, de acuerdo a riesgos estratégicos y operativos. La metodología ISO 31000, permite en la práctica establecer objetivos, riesgos y controles que pueden ser de mayor aplicación en los distintos actores del gobierno nacional.

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.

Comentario: La seguridad nacional como un valor deseable para toda la ciudadanía no puede limitarse a la seguridad nacional, debe ser redactado nuevamente esto. No solo se requiere socializar y concientizar en gestión de riesgos también en análisis del riesgo que cumplan con los principios de la política.

PROPUESTA DE TEXTO:
M3.4. Mecanismos de socialización y concientización tanto de tipologías comunes que afecten la seguridad digital y gestión de riesgos, como del análisis y cumplimiento integral de la política de seguridad digital por parte de las múltiples partes interesadas.

7. Comentarios a las acciones del CONPES

Desafortunadamente, el plazo asignado para comentar el CONPES no nos permite hacer un trabajo más detallado sobre esta sección que es quizá la más importante. Entendemos que existe premura en el gobierno para desarrollar esta política, sin embargo, la ausencia

de la dimensión humana es todavía un vacío sensible del documento. A pesar de ser un principio fundamental de la nueva política, consideramos que no está suficientemente desarrollado en el resto de ella. Si se acogen nuestros comentarios, será evidente que hace falta un plan de acción para desarrollarlo, por tanto, **solicitamos al gobierno que se nos de un plazo mayor** que permita hacer esos comentarios.

Sin embargo, dejamos algunos comentarios y propuestas que no pueden se consideradas las más importantes o prioritarias, sino simplemente las que alcanzamos a desarrollar más fácilmente en el corto plazo otorgado para comentar más de 100 acciones que no responden en su generalidad al marco conceptual, en donde el primer principio es el reconocimiento y promoción de los derechos humanos.

> ***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.*

Comentario: ¿Se necesita un nuevo cargo? ¿Qué funciones tendrá?. La figura de Consejero no es viable sin antes no darle un marco jurídico para que pueda integrar las distintas entidades.

> ***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*

Comentario: Para la creación de esta figura, se requiere la participación del Departamento Administrativo de la Función Pública, quien es el ente competente para estos casos. Por lo tanto se sugiere que se incorpore al DAFP en este proceso. Por otro lado, para no aumentar más la burocracia, se sugiere que se incorpore que esta figura, la puede desempeñar el Director de TI de las entidades públicas, debido que actualmente son ellos quien están a cargo de estos temas.

> ***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*.

Comentario: ¿Qué hará este nuevo organismo?

> **A1.2.5** *Fortalecer la capacidad administrativa del Grupo de Respuestas a Incidentes Cibernéticos de Colombia (colCERT), adecuando la estructura orgánica del MINDEFENSA.*

Comentario: El enfoque social de la nueva política debería considerar independizar colCERT del Ministerio de Defensa para que pueda responder mejor a las tareas de corte

civil que tiene a su cargo. Esto no debe verse como un detrimento del aspecto defensivo de la seguridad digital pues aún se cuenta con el Comando Conjunto Cibernético. En la actualidad no existe una correcta integración del Colcert con otras entidades es el caso de la policía, la Delegatura de Protección de Datos, la rama judicial, entre otras.

> ***A2.1.2.*** *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.*

Comentario: La retención de datos obligatoria por parte de los proveedores de servicios de telefonía e internet es innecesaria y desproporcionada[6]. Así se desprende de los estándares internacionales fijados, entre otros, por la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos[7]. Así mismo, en el marco conceptual se cita la Directiva 2006/24/CE del Parlamento Europeo y aún la sentencia del Tribunal de Justicia Europeo que encontró dicha directiva es inválida por afectar injustificadamente derechos fundamentales.

Sería equivocado entonces llevar una medida que es reconocida internacionalmente por lesionar gravemente derechos fundamentales, de las comunicaciones celulares al campo de Internet. Por esta razón, el Decreto 1704 de 2012 y la Ley 1621 de 2013 deben ser derogadas en lo que tiene que ver con la retención de datos de comunicaciones.

PROPUESTA DE TEXTO:
A2.1.2. Armonizar con los estándares nacionales e internacionales de protección de Derechos Humanos la normatividad que permite realizar el almacenamiento, la retención y los procedimientos del suministro de información por parte de los proveedores de servicio de comunicación 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.*

Comentario: La Ley Estatutaria debe actualizarse para reflejar una adecuado respeto a los derechos fundamentales de la ciudadanía, especialmente si se tiene en cuenta las capacidades tecnológicas que ha adquirido el Estado para vigilar las comunicaciones.

En general, es importante delimitar la actualización que se haga a la Ley 1621. No basta decir que se enmarcan actividades de ciberseguridad y ciberdefensa. También es clave, primer lugar, establecer mecanismos legales claros para la salida de información. Actualmente, la ley dispone que quien quiera obtener información de inteligencia debe "acudir a los mecanismos legales". En la práctica, los organismos de inteligencia no aplican estos mecanismos. Por tanto, en la ley debe hacerse las correspondientes remisiones a la

---

[6] Castañeda, J. (2015). ¿Es legítima la retención de datos en Colombia?. Recuperado de: https:// karisma.org.co/?wpdmdl=6259

[7] CIDH (2013). Libertad de expresión e internet. OEA/Ser.L/V/II.149 Doc.50, Capítu- lo IV, p rr. 55.

Ley 1712 de 2014. Esto es clave porque la falta de mecanismos claros es un incentivo para el tráfico de información. En segundo lugar, debe establecerse prohibiciones claras, por ejemplo, que no se pueda usar software malicioso para adelantar actividades de inteligencia. Tercero, debe profundizarse el control a todo nivel de las actividades de inteligencia de forma que sea efectivo y garantice que no haya abuso de las facultades excepcionales que se les ha reconocido.

PROPUESTA DE TEXTO:
A. 2.1.3. 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, la Ciberdefensa, y el cumplimiento del Principio Fundamental n° 1 del presente documento, consistente en 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.

> ***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.*
>
> ***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.*

Comentario: para las acciones A.2.1.4 y A.2.1.5 sería recomendable tener en cuenta que no basta con hacer los estudios. Debe ser claro que ellos deben informar las decisiones de reforma de los marcos institucionales y legales para que efectivamente éstos sean compatibles con las exigencias de la protección de la privacidad y de los datos personales así como con los derechos fundamentales.

PROPUESTA DE TEXTO:
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 para armonizar la normativa interna con estos derechos.

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 para armonizar la normativa interna con estos derechos.

> ***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)*
>
> ***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.

Comentario: el fortalecimiento de las capacidades de organismos de seguridad e inteligencia necesariamente tiene que venir acompañado del fortalecimiento de los controles a esas entidades para prevenir los abusos cuya ausencia fue notada en la parte de Antecedentes y con la obligación de que las facultades o acciones con que se fortalezcan se acompañen de un análisis de riesgo que permita establecer las posibles afectaciones a derechos humanos con el fin de mitigarlas apropiadamente (mediante disposiciones equivalentes como controles).

PROPUESTA DE TEXTO:
A3.2.1. Fortalecer la capacidad administrativa y los controles 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). Las modificaciones deberán responder a un análisis del riesgo sobre la afectación a derechos humanos.

A4.2.1. Fortalecer la capacidad administrativa y operativa y los controles 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. Las modificaciones deberán responder a un análisis del riesgo sobre la afectación a derechos humanos.

***A3.4.3.** Promover la implementación de CSIRTs sectoriales, definidos de acuerdo a la catalogación de las infraestructuras críticas nacionales.*

Comentario: Organizaciones de la sociedad civil podrían recibir favorablemente la creación de un CSIRT para atender trabajar y reaccionar a sus incidentes informáticos. Esto podría verse obstaculizado por la creación de CSIRT solo en virtud de las infraestructuras críticas nacionales si acaso dentro de ellas no se contempla, por ejemplo, la infraestructura informática que emplean estas organizaciones para el desarrollo de su trabajo. Por eso debe abrirse la redacción para que estas necesidades sean tenidas en cuenta.

PROPUESTA DE TEXTO:
A3.4.3. Promover la implementación de CSIRTs sectoriales, definidos de acuerdo a la catalogación de las infraestructuras críticas nacionales o a las necesidades de sectores vulnerables como organizaciones de la sociedad civil, asociaciones de víctimas o desmovilizados o periodistas.

Comentario General: El documento CONPES de 2011 y el actual carecen totalmente de una análisis de género que entra en conflicto con la política nacional de equidad de género, recogida en los Lineamientos de la Política Pública para la Equidad de Género para las Mujeres. En este sentido, nuestra propuesta es generar una nueva acción que recoja el compromiso del Estado en adelantar la equidad de género en sus políticas, en este caso, en la de seguridad digital.

Nueva acción sugerida: **Incorporar la perspectiva de género en las acciones, posibles indicadores y estructuras de la política nacional de seguridad digital**

Encargar un estudio que presente un diagnóstico de la seguridad digital en Colombia desde una perspectiva de género, con el fin de que la cultura de seguridad digital que la política busca adelantar cuente con elementos que ayuden a promover la equidad de género y el empoderamiento de las mujeres en los espacio digitales. Asimismo, el gobierno debe comprometerse a promover que en las nuevas estructura propuesta exista un balance de género en su composición. Esto también ha de conllevar un proceso de capacitación para que el sector digital, espacio predominantemente masculino, también fomente la participación activa de las mujeres. Finalmente, el gobierno buscará la construcción de indicadores para medir avances en este tema de la seguridad digital frente a la equidad de género.

8. Comentarios al Glosario

Aunque se eliminaron definiciones problemáticas de anteriores borradores del CONPES cómo "privacidad" el glosario actual es insuficiente y no permite aclarar varios puntos del documento. Por ejemplo, hace falta claridad sobre lo qué significan amenazas y riesgos, entre otras razones, porque eso permitiría clasificar algunos ataques oficiales a la seguridad digital de la ciudadanía.

Aunque este aparte del documento es quizá el menos desarrollado y que debe ser ajustado por los responsables del documento proponemos algunas definiciones que consideramos importantes:

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Art. 3 Ley 1581 de 2012)

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento (Ibíd.)
Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Ibíd.).
Datos sensibles: Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. (Art. 5, Ley 1581 de 2012).

Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:
a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares. (Art. 6, Ley 1581 de 2012)