

CÁMARA DE REPRESENTANTES
COMISIÓN SEGUNDA
Nombre: Manif
Fecha: 02-08-17 Hora: 4:10 PM
Radicado: 043



Bogotá D.C.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

FECHA: 28/7/2017

HORA: 09:36:53

FOLIOS: 4

REGISTRO NO: 1068506

DESTINO: CAMARA DE REPRESENTANTES

Doctor
BENJAMÍN NIÑO FLÓREZ
Secretario General
Comisión Segunda
CAMARA DE REPRESENTANTES
Correo: csegunda.camara@gmail.com
Carrera 7 No. 8-68, piso 5°
Edificio Nuevo del Congreso
Bogotá D.C

Asunto: **Respuesta Proposición No. 47 de junio 6 de 2017 "finalidad de esclarecer el ciber ataque que se presentó el pasado viernes 12 de mayo, prevención de nuevos actos" presentada por el HR Andrés Felipe Villamizar Ortiz.**

En atención a la Proposición No. 47 cuya "Finalidad es esclarecer el Ciber Ataque que se presentó el pasado viernes 12 de mayo, prevención de nuevos actos", radicada por el Honorable Representante Andrés Felipe Villamizar Ortiz; de manera atenta me permito dar respuesta al cuestionario en los asuntos de competencia de la Institución, así:

1. **¿Cuenta el Estado Colombiano con una Política Pública que procure la protección de datos y garantice la seguridad de los conciudadanos en el ciberespacio?**

El pasado 11 de abril de 2016 el Consejo Nacional de Política Económica y Social, aprobó el documento CONPES 3854, la cual es la nueva Política Nacional de Seguridad Digital, que pretende lograr que el Gobierno, las organizaciones públicas y privadas, la fuerza pública, la academia y los ciudadanos en general en Colombia, puedan contar con un entorno digital confiable y seguro que maximice los beneficios económicos y sociales, impulsando la competitividad y productividad en todos los sectores de la economía.

vive digital
para la gente

Si bien esta política busca que se distingan claramente 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, todo dirigido hacia una gestión de riesgos de seguridad digital, no es directamente una política pública sobre la protección de datos.

2. ¿El Conpes actual de seguridad informática es suficiente? ¿Incluye las herramientas necesarias para que las FFMM y policía puedan adelantar su trabajo de forma eficiente?

Considerando que el CONPES 3854 de Seguridad Digital es complementario al CONPES 3701/11, los cuales buscan avanzar en el desarrollo de capacidades para enfrentar amenazas cibernéticas, otorgándole corresponsabilidad a la Policía Nacional, para garantizar la Ciberseguridad en el territorio nacional a partir de acciones tendientes a identificar, anticipar, prevenir y judicializar a los responsables de las amenazas que atenten contra la Ciberseguridad Ciudadana, siendo esta una iniciativa gubernamental pertinente y efectiva para cumplir los compromisos enfocados en convertir el ciberespacio en un escenario de confianza para el desarrollo de actividades productivas y de prestación de servicios seguros.

Ahora bien, desde el ámbito de responsabilidad compartida y coordinada, entendida esta, como la acción compartida entre gobierno, sector privado, academia y ciudadanos, el documento CONPES 3854, establece una línea de acción clara para las instituciones en pro de garantizar la seguridad de los individuos y del Estado en el entorno digital, con enfoque de gestión de riesgos.

Sin embargo, tal y como se manifestó a través del diagnóstico del documento Conpes 3854, existe la necesidad de fortalecer las capacidades tanto humanas, como técnicas, de formación de personal, fortalecimiento de infraestructura y gobernanza, así mismo como la necesidad de complementar una legislación en materia de seguridad digital para la defensa del Estado en y a través del Ciberespacio.

3. ¿Existía alguna forma, herramienta o tecnología que permita prevenir ataques como el del pasado 12 de mayo?

Es pertinente precisar que el rol que desempeña los ciudadanos y los usuarios finales es muy importante al momento de evitar la materialización de éste tipo de ataques, siendo ellos quienes pueden ser el eslabón más débil en la cadena de la seguridad, adicionalmente las Entidades y los ciudadanos pueden contar con medidas de prevención tales como la toma de backups, la actualización de Sistemas Operativos y aplicaciones entre otros que permitan prevenir el impacto de los ataques.

Teniendo en cuenta lo anterior, el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), desarrollo el Modelo de Seguridad y Privacidad de la Información el cual se incorporó como parte integral del Manual de implementación de la Estrategia de Gobierno en Línea. Este manual, describe todas aquellas acciones respecto a seguridad de la información que se deben ejecutar por

parte de las entidades del Orden Nacional y Territorial tendientes a garantizar la confidencialidad, la integridad y la disponibilidad de la información, así como la responsabilidad, la finalidad y el

consentimiento relacionado con el uso de los datos personales. Adicionalmente el MINTIC, brinda acompañamiento a las Entidades del Estado en la implementación de sistemas de Seguridad de la Información de acuerdo a lo estructurado en el Modelo de Seguridad y Privacidad de la Información.

4. ¿Hace parte Colombia de algún tratado internacional que procure la protección de datos y garantice la seguridad de los ciudadanos en el ciberespacio?

No, en la actualidad Colombia no hace parte de ningún tratado que procure la protección de datos y garantice la seguridad de los ciudadanos en el ciberespacio.

5. ¿Hace parte Colombia de algún tratado internacional que garantice la judicialización de los perpetradores de ataques en el ciberespacio?

No, en la actualidad Colombia no hace parte de ningún tratado internacional que garantice la judicialización de los perpetradores de ataques en el ciberespacio, sin embargo, en la actualidad el Ministerio de Defensa Nacional, el Ministerio de Relaciones Exteriores, el Ministerio de Justicia y del

Derecho y el Ministerio de Tecnologías de la información y las Comunicaciones se encuentran realizando las gestiones necesarias para presentar a consideración del Honorable Congreso de la República, el Proyecto de Ley por medio de la cual se dé aprobación del "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

Cualquier inquietud adicional, con gusto será atendida.

Atentamente,


DANIEL QUINTERO CALLE
Viceministro TI

Ministerio de Tecnologías de la Información y las Comunicaciones

Proyectó: Yubelly Astrid Monroy – Asesora Viceministerio TI
Revisó: Juanita Rodríguez – Directora de Estándares y Arquitectura de TI
Elizabeth Blandon – Directora de Gobierno en Línea
Julio Cesar Mancipe – Subdirección Seguridad y Privacidad
Esteban Restrepo – Asesor Despacho Viceministro