OFI17-00095267 / JMSC 100170

Bogotá D.C. jueves, 03 de agosto de 2017

Doctor
BENJAMIN NIÑO FLOREZ
Secretario General
Comisión Segunda de Relaciones Exteriores, Comercio Exterior, Defensa y Seguridad Nacional
Cámara de Representantes
Carrera 7 No 8-68 Piso 5, Edificio Nuevo del Congreso
Bogotá

Asunto: Respuesta de fondo EXT17-00082534- Proposición N° 47 de junio 06 de 2017.

Respetado doctor Niño:

Atendiendo a la solicitud presentada por esta Consejería el pasado 28 de julio de 2017, relacionada con ampliar el plazo legal otorgado para dar respuesta de fondo al cuestionario correspondiente a la Proposición No 47 de junio 06 de 2017, formulado para esclarecer el ciberataque presentado el pasado viernes 12 de mayo e identificar las mejores iniciativas para la prevención de nuevos actos, procedo a dar respuesta a cada una de las preguntas a cargo, así:

Pregunta 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?"*

La política pública de Seguridad Digital en Colombia se encuentra actualmente en el documento CONPES 3854, aprobado el 11 de abril de 2016 por el Consejo Nacional de Política Económica y Social, cuyo propósito es lograr que el Gobierno, las organizaciones públicas y privadas, la Fuerza Pública, la academia y los ciudadanos en general cuenten 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.

Esta política señala los objetivos de prosperidad económica y social, los objetivos de defensa y lucha contra el crimen y la delincuencia en el entorno digital, está dirigida a la gestión de riesgos de seguridad digital, enmarcada entre otras normas, dentro de la protección de los datos personales. La protección de datos está reglamentada jurídicamente dentro de un conjunto de leyes nacionales específicas para este tema.

Pregunta 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?"*

Calle 7 No. 6-54, Bogotá, Colombia
PBX (57 1) 562 9300
Código Postal 111711
www.presidencia.gov.co

Colombia actualmente cuenta con el CONPES 3701 de 2011, a través del cual se establecen los lineamientos de política para ciberseguridad y ciberdenfensa, y con el CONPES 3854 de 2016, que contiene la política nacional de seguridad digital y complementa el primer documento; dentro de las finalidades de estos documentos está la de avanzar en el desarrollo de capacidades para enfrentar amenazas cibernéticas, y por ello a través de la Policía Nacional se garantiza 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 misma.

El documento CONPES 3854 de 2016 respecto a la responsabilidad compartida y coordinada entre Gobierno, sector privado, academia y ciudadanos, establece la línea de acción 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.
En desarrollo de estos documentos, y con el fin de brindar al Estado colombiano herramientas para el cumplimiento de sus funciones, el Ministerio de Tecnologías de la Información y las Comunicaciones viene trabajando un enfoque de gestión de riesgos que implica fortalecer las capacidades humanas y técnicas, la formación de personal, la infraestructura y gobernanza; a la vez, desde la Consejería Presidencial de Seguridad se ha coordinado con el Ministerio de Justicia la construcción de herramientas normativas que fortalezcan la seguridad digital y defensa del Estado en y a través del Ciberespacio.

Finalmente, atendiendo a lo señalado por el Ministerio de Defensa *"las amenazas cibernéticas son dinámicas y cambian de manera permanente"*, siempre debe considerarse la necesidad de actualizar los documentos de esta política puesto que si bien actualmente las Fuerzas Militares y la Policía Nacional cuentan con herramientas eficientes para mitigar el riesgo de las amenazas, estas no son ni serán suficientes por cuanto todos los días hay nuevas amenazas de difícil detección.

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

El rol que desempeñan los ciudadanos y los usuarios finales del ciberespacio es muy importante al momento de evitar la materialización de éste tipo de ataques, por lo que pueden ser ellos el eslabón más débil en la cadena de la seguridad; sin embargo, las entidades y los ciudadanos pueden contar con medidas de prevención como la toma de backups, actualización de sistemas operativos y aplicaciones, entre otros, que permitan prevenir el impacto de los ataques.

Aunado a lo anterior, en el marco de la prevención, el Ministerio de Tecnologías de la Información y las Comunicaciones desarrolló el Modelo de Seguridad y Privacidad de la Información, incorporado al Manual de Implementación de la Estrategia de Gobierno en Línea; el Manual, describe todas las acciones respecto a seguridad de la información que deben ejecutar las entidades del orden nacional y territorial para garantizar la confidencialidad, integridad y disponibilidad de la información, así como la responsabilidad, finalidad y consentimiento relacionado con el uso de los datos personales.

Para ello, el Ministerio brinda acompañamiento a las entidades del Estado en la implementación de sistemas de gestión de seguridad de la información de acuerdo al mencionado Modelo.

Calle 7 No. 6-54, Bogotá, Colombia
PBX (57 1) 562 9300
Código Postal 111711
www.presidencia.gov.co

En consecuencia, la adopción de las medidas citadas previenen los ataques que se presenten en y a través del ciberespacio.

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

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

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

Actualmente Colombia no hace parte de algún tratado internacional que garantice la judicialización de los perpetradores de ataques en el ciberespacio; sin embargo, el Gobierno Nacional a través de la Consejería Presidencial de Seguridad, 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, adelantan 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.

Preguntas 6 y 9. "*Cuál es la capacidad instalada en la actualidad para contrarrestar la guerra cibernética que se está presentando actualmente?*

Teniendo en cuenta la información suministrada por el Ministerio de Defensa Nacional, el concepto de guerra cibernética hace referencia al ciberespacio como dominio de acción y dos (2) o más Estados como actores, por lo que en el marco de dicha definición ningún país ha reconocido oficialmente que se afronta una guerra cibernética, sino ataques a plataformas tecnológicas con diferentes propósitos.

La capacidad instalada de Colombia está representada por sus líderes en ciberseguridad y ciberdefensa, es decir por el Grupo de Respuesta a Emergencia Cibernéticas- ColCERT, el Comando Conjunto de Operaciones Cibernéticas-CCoC, el Centro Cibernético Policial -CCP y el Ministerio de Tecnologías de la Información y las Comunicaciones, quienes han realizado actividades para prevenir y dar respuesta a los ataques cibernéticos.

Así, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, tiene como responsabilidad central la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado ante emergencias que atenten o comprometan la seguridad y defensa nacional, y gestiona la respuesta a incidentes cibernéticos, como los que se han venido presentando.

Calle 7 No. 6-54, Bogotá, Colombia
PBX (57 1) 562 9300
Código Postal 111711
www.presidencia.gov.co

A la vez, en respuesta a los incidentes de ciberseguridad la Policía Nacional implementó el CAI Virtual desde el año 2007, como iniciativa online de atención policial contra el delito cibernético en Latinoamérica garantizando una respuesta inmediata a los requerimientos de los ciudadanos. Este servicio virtual genera un espacio de consulta, prevención, orientación y atención de incidentes informáticos que afectan a la ciudadanía en general a través del portal www.caivirtual.policia.gov.co, el cual cuenta con un *chat* disponible en horario 24/7, donde se atienden los requerimientos en la materia; así mismo, se puede interactuar en la cuenta de *Twitter* @*CaiVirtual* y en el perfil de *Facebook* "caivirtual", en de los cuales se difunden alertas de ciberseguridad respecto a las modalidades utilizadas por los ciberdelincuentes.

Con el propósito de ampliar la respuesta a este numeral, la Consejería aportará información del Centro Cibernético Policial –CCP, relacionada con las actividades por ellos adelantadas para salvaguardar la seguridad de los ciudadanos en el ciberespacio:

- Emisión de alertas preventivas a través de redes sociales con el fin dar a conocer las nuevas amenazas y modalidades delictivas utilizadas por los ciberdelincuentes, a través de medios electrónicos, las cuales logran la sensibilización y prevención para contrarrestar dichas conductas.

- Charlas de seguridad digital para dar a conocer las modalidades del cibercrimen que afectan a las distintas entidades del sector público y privado.

- Iniciativa "Café de Expertos" que coadyuva al acceso e interacción entre los diferentes sectores, para la cual el CCP dispuso un micrositio al que pueden acceder interlocutores del sector privado, permitiéndoseles generar discusiones, propuestas de buenas prácticas, información de nuevas amenazas y tendencias de "cibercrimen", o solicitar atención especializada a los problemas que en materia cibernética les afectan.
  En este espacio participan los sectores financiero, educativo, gubernamental, servicios públicos, telecomunicaciones, energético e hidrocarburos, y se facilita la comunicación con los homólogos en investigación criminal cibernética a nivel internacional, entre los que se encuentra el *European Cibercrime Center - EC3*.

- De igual forma, el Centro Cibernético Policial -CCP cuenta con siete (7) frentes investigativos especializados en atender diferentes modalidades del delito informático: oferta ilícita de productos y servicios en línea, convivencia ciudadana en Internet, abusos de niños, niñas y adolescentes en la *web*, *malware*, *carding*, estafas, hurto *on line* y amenazas emergentes.

- El Laboratorio de Informática Forense de la Dirección de Investigación Criminal de la Policía Nacional, como unidad de apoyo técnico que cuenta con las más modernas herramientas de software y hardware empleadas en la materia, es una unidad a la vanguardia en tecnología, con la cual se contribuye a los procesos investigativos de las principales autoridades.

  Se efectúan análisis especializados de dispositivos de almacenamiento de información electrónica tales como equipos de cómputo, discos duros, memorias USB, entre otros. Igualmente el laboratorio cuenta con herramientas especializadas que permiten la extracción de evidencia digital almacenada en teléfonos móviles, y con sofisticadas herramientas para el análisis de bases de datos, permitiendo identificar, relacionar, obtener registros de *bigdata*. También realizan análisis

Calle 7 No. 6-54, Bogotá, Colombia
PBX (57 1) 562 9300
Código Postal 111711
www.presidencia.gov.co

especializados de *malware* con los cuales se logra establecer la funcionalidad del *software* malicioso.

Se llevan a cabo procesos de recolección, preservación, análisis y presentación de evidencia digital, cumpliendo con los principios de disponibilidad, integridad, no repudiación y observancia que son sustentables ante los estrados judiciales.

Pregunta 7. "*Existen en Colombia instituciones Educativas pioneras en investigaciones sobre seguridad informática? O en el Centro de Educación Militar?"*

En el país la Universidad Piloto de Colombia, la Universidad Autónoma de Occidente y la Universidad Pontificia Bolivariana cuentan con enfoque especial de seguridad de la información; a la vez, las universidades Católica, Sergio Arboleda, Politécnico Grancolombiano, entre otras, ofrecen especializaciones en seguridad de la información.

Adicionalmente Colombia cuenta con dos (2) programas de Maestría: el primero en la Universidad de los Andes relacionado con seguridad de la información, y el segundo en la Escuela Superior de Guerra sobre Ciberseguridad y Ciberdefensa.

En ambas modalidades de postgrado al finalizar el programa de estudio los estudiantes tienen como opción de grado realizar desarrollo de investigaciones.

Pregunta 8. *"Cuáles son los resultados tangibles de las operaciones que la fuerza pública ha implementado frente a los ataques cibernéticos?"*

Atendiendo a que Colombia cuenta con diferentes instancias para prevenir, coordinar, atender, controlar, proporcionar recomendaciones y regular incidentes o emergencias cibernéticas, los resultados de la Fuerza Pública se presentarán en dos (2) escenarios diferentes: resultados de las Fuerzas Militares, a través del Comando Conjunto Cibernético CCOC[1], enfocados a la defensa de la infraestructura crítica, y resultados de la Policía Nacional a través del Centro Cibernético Policial CCP[2].

- Resultados Fuerzas Militares – CCOC

a) Protección y defensa de la infraestructura critica cibernética militar.
b) Apoyo a la ciberdefensa de infraestructuras criticas cibernéticas nacionales.
c) Conciencia situacional en los operadores y propietarios de Infraestructuras Criticas Cibernéticas.
d) Visualización y alertamiento temprano ante incidentes.
e) Gestión de incidentes cibernéticos.
f) Sensibilización y concientización en materia cibernética.

[1] Información suministrada por Ministerio de Defensa.
[2] Información suministrada por CCP.

Calle 7 No. 6-54, Bogotá, Colombia
PBX (57 1) 562 9300
Código Postal 111711
www.presidencia.gov.co

g) Fortalecimiento de una cultura cibernética.
h) Publicación de la guía para la identificación de infraestructura crítica cibernética nacional.
i) Análisis de los sectores estratégicos desde la óptica cibernética en Colombia.
j) Generación del Catálogo Nacional de Infraestructura Critica Cibernética Nacional versión 1.0.

a. Resultados Policía Nacional – CCP

Los resultados presentados por la Policía Nacional - Centro Cibernético Policial - CCP se enfocan en acciones de prevención y judicialización adelantadas contra organizaciones criminales, así:

a) Siete (7) operaciones contra estructuras criminales.
b) Cinco (5) organizaciones desarticuladas.
c) Siento sesenta y ocho (168) capturas.
d) Diez (10) acciones internacionales (2 organizaciones criminales transnacionales).
e) Ciento doce (112) comunicaciones SIENA con EUROPOL.

Ahora bien, con el propósito de atender el ataque informático mundial del pasado 12 de mayo, que afectó a más de 150 países, entre ellos Colombia, el Centro Cibernético Policial- CCP a través del @CAIVIRTUAL, dispuso de un Puesto de Mando Unificado -PMU de servicio de atención especial a la ciudadanía para brindar orientación, prevención y atención.

En este caso las redes sociales del Centro Cibernético Policial (@caivirtual) permitieron generar alertas preventivas para mitigar y orientar las acciones a seguir por los ciudadanos, así como identificar los siguientes resultados:

- La página www.caivirtual.policia.gov.co registró 20.186 visitantes únicos durante el incidente, incrementándose en un 504% las visitas al sitio web. (cifra normal son 4.000 visitas semanal)
- Se atendieron 1.746 incidentes, de los cuales 52 han reportado ser víctimas.
- Se recibieron 160 muestras de *malware*.
- Se generaron 59 alertas en redes sociales.
- Se lograron impactar más de 619.520.294 millones de cuentas en *Twitter* a nivel global.
- Índice de satisfacción del 92.8 % de todos los incidentes atendidos.

A la vez, es importante informar que en el marco del ataque la articulación de las diferencias instancias y de la Policía Nacional- Centro Cibernético Policial CCP arrojó los siguientes resultados:

- La comunicación con agencias policiales extranjeras fue fundamental para el intercambio de información en tiempo real ante este tipo de ataque.
- La difusión de alertas en medios de comunicación fue de gran apoyo y permitió generar conciencia y sensibilizar a la ciudadanía, mostrando una articulación institucional de las entidades del Gobierno.

Calle 7 No. 6-54, Bogotá, Colombia
PBX (57 1) 562 9300
Código Postal 111711
www.presidencia.gov.co

- Las capacidades forenses desplegadas en el Laboratorio de Informática del Centro Cibernético Policial - CCP, la plataforma de análisis de *malware* de Europol "EMAS" y el sitio web nomoreransom.org, fueron fundamentales para la atención de los diferentes incidentes recepcionados por los canales de comunicación del CAI VIRTUAL.
- El servicio prestado en el sitio web caivirtual.policia.gov.co para cargar las muestras de *malware*, permitió atender y analizar los incidentes reportados integralmente.
- El Puesto de Mando Unificado –PMU para atención a la ciudadanía fue coordinado por la Consejería Presidencial de Seguridad, Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional, Grupo de Respuesta a Emergencia Cibernéticas- ColCERT, el Comando Conjunto de Operaciones Cibernéticas-CCoC, Centro Cibernético Policial - CCP y demás sectores involucrados, logrando articular esfuerzos para mitigar este ataque global.
- La comunicación constante entre los responsables permitió unificar criterios y acciones a seguir frente a esta amenaza informática.

Pregunta 10. *"Existen operaciones de inteligencia militar y policial que busquen prevenir ciberataques?"*

En relación con la pregunta 10 es importante indicar que la Consejería Presidencial de Seguridad consultó al Ministerio de Defensa Nacional sobre las operaciones referidas, indicándose que *"Cada unidad cibernética de las Fuerzas Militares y de Policía Nacional, cuenta con capacidades para mitigar y prevenir ciberataques o amenaza hostiles que puedan afectar la seguridad nacional o cualquiera infraestructura critica que tienen el carácter de reservado."*.

Finalmente, es importante tener en cuenta que la información suministrada es de aquella prevista en los artículos 18 y 19 de la ley 1712 de 2014 y en consecuencia debe ser tratada con la reserva correspondiente.

Cordialmente,

JUAN CARLOS RESTREPO PIEDRAHITA
Consejero Presidencial de Seguridad

Copia: GR (RA) Óscar Naranjo Trujillo
Vicepresidente de la República
Elaboró: Yubelly/ace

Calle 7 No. 6-54, Bogotá, Colombia
PBX (57 1) 562 9300
Código Postal 111711
www.presidencia.gov.co