Actualizar leyes, clave en la lucha contra un **crimen mutante**

Si bien se volvió un lugar común decir que los delincuentes están a la vanguardia de los especialistas que pretenden combatirlos, también es sabido que solo con un cerco mundial es posible neutralizarlos. Para ello es necesario armonizar las distintas legislaciones. Colombia ya se está orientando en esa vía.

Foto: Vicktor Hanacek, picjumbo.com, Creative Commons.

Aunque el Gobierno colombiano está muy comprometido con la seguridad informática, no necesariamente somos un país muy bien protegido contra el cibercrimen.

Con el objetivo de concordar la política pública colombiana con los avances tecnológicos, el Gobierno convocó a los distintos actores para diseñar el nuevo documento Conpes que impulsará el fortalecimiento de la ciberdefensa y la ciberseguridad. De acuerdo con el ministro de las Tecnologías de la Información y las Comunicaciones (MinTIC), David Luna, que hizo el anuncio el 3 de agosto del 2015, el documento regiría desde el 2016.

Las líneas estratégicas de esta política pública serán el fortalecimiento del marco jurídico y legal, la cultura de ciberseguridad y ciberdefensa, la investigación de desarrollos, las infraestructuras críticas cibernéticas y el trabajo de cooperación internacional.

En su diseño han participado la Policía Nacional, el Ministerio de Defensa, Planeación Nacional, el Ministerio de Justicia, MinTIC, la Fuerza Aérea, el Ejército Nacional, la Escuela de Guerra y la Cancillería, así como la sociedad civil, la industria y la academia.

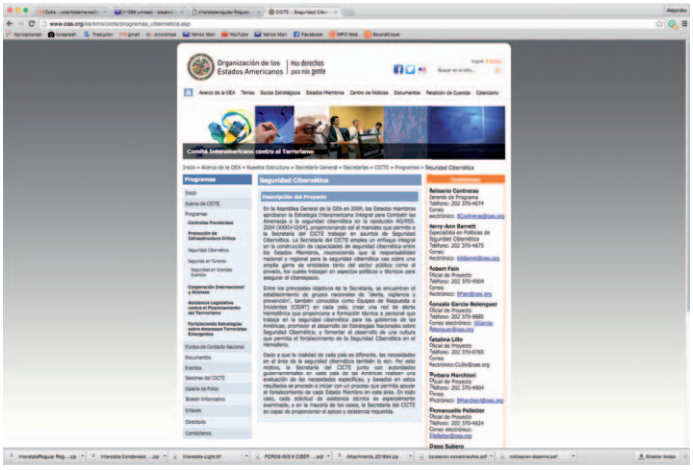
En la elaboración del nuevo Conpes se tuvo en cuenta el diagnóstico de una misión de la OEA sobre el estado de la ciberdefensa y la ciberseguridad en Colombia. De acuerdo con Wilmer Antonio Prieto, de Intel Security, somos el quinto país en las Américas y el noveno del mundo —como muchos otros que también están en el quinto y en el noveno lugar— más comprometido con estos temas, pero no necesariamente el quinto más protegido. En esa calificación se perciben los esfuerzos hechos desde el 2011, cuando se expidió el primer Conpes.

Los foristas coincidieron en que es necesario fortalecer el compromiso de los gobiernos, del sector privado y de la ciudadanía con estos asuntos pues, señala Adrián Eduardo Acosta, oficial de Crimen Digital de Interpol, una legislación aplicable debe hacer parte de la cultura.

Por su parte, Pablo Palacios, *programer officer* de la Unión Internacional de Telecomunicaciones (UIT), área de Chile, resaltó la importancia de generar marcos regulatorios que faciliten interconexión y convenios entre países. Aconseja tener Cert (del inglés *Computer Emergency Response Team*) regionales y subregionales que se coordinen con los nacionales y permitan crear una red que los haga fuertes en trabajo mancomunado, no solo en el apoyo y en la solución de incidentes sino en el intercambio de información, de mejores prácticas y de parámetros bajo los cuales son evaluados los incidentes.

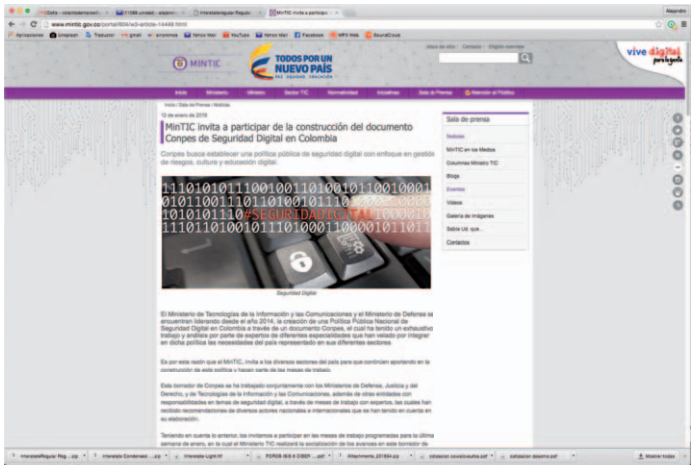
Sin embargo, la existencia de diferentes legislaciones restringe la investigación, porque puede suceder que una acción esté penalizada en un lugar, pero no donde se encuentra el servidor que usa el delincuente; o no hay convenios ni tratados que ayuden a judicializar a esta persona. La Interpol ya trabaja en conseguir que los comportamientos tipificados como crímenes lo sean en todos los Estados y que las penas sean similares. Así lo estipuló Adrián Eduardo Acosta, de esa entidad, mientras que Belisario Contreras, de la Secretaría del Comité contra el Terrorismo Interamericano de la OEA, aseguró que, en esta dirección, hay mandatos políticos regionales muy claros y compromisos adquiridos al más alto nivel por cada uno de los países miembros.

Jairo Pantoja, experto en Estrategias e Implementación de Proyectos de Seguridad Informática Corporativa de Symantec, califica la cooperación como asunto crítico en el combate de este flagelo, y señala que



http://www.oas.org/es/sms/cicte/programas_ciberneticа.asp

La Organización de Estados Americanos facilita la cooperación entre sus Estados miembros para prevenir el terrorismo cibernético.



http://www.mintic.gov.co/portal/604/w3-article-14449.html

En la elaboración del nuevo documento Conpes sobre ciberdefensa y ciberseguridad el Gobierno invitó a participar a los estamentos de la industria y la academia.

debe darse entre empresas, instituciones y gobiernos: "Es importante replicar aquello que detectemos en nuestra red de inteligencia, porque las amenazas actúan rápidamente".

En Colombia existen algunas de esas alianzas y han facilitado operaciones en la *deep web* para atacar la venta de software malicioso, de drogas y de medicamentos ilegales. Esas coaliciones también se han aprovechado en la preparación de personal en buenas prácticas en el manejo de esa red, comentó el teniente Óscar Mojica, del Centro Cibernético Policial de la Dijin.

A pesar de ello, según Álvaro José Chávez, director del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCert), de la Dirección de la Seguridad Pública e Infraestructura del Ministerio de Defensa, el ColCert ha identificado las siguientes problemáticas: las entidades no están obligadas a compartir información con las demás; no se cuenta con capacidad técnica ni humana para mantener un flujo constante y real de información que permita identificar incidentes en las estructuras, y muchas entidades desconocen la existencia de las oficinas dedicadas a la seguridad informática.

Por su parte, el coronel Fredy Bautista García, jefe del Centro Cibernético Policial, habló de las herramientas con las que ese cuerpo especializado actúa: 25 unidades dispuestas en 25 ciudades del país y 8 equipos de informática forense de gestión de incidentes. Además, disponen del sitio web www.ccp.gov.co, de aplicaciones como *Protection* especializadas en control y orientación parental, un portal de denuncia en línea y un CAI virtual. Recientemente se vincularon al grupo expertos del G8 y de la Red 24/7, de las unidades de Cibercrimen de Interpol, para garantizar el acceso y la preservación de los datos para una investigación judicial.

El grupo de la Policía busca la consolidación de los equipos de respuesta a incidentes que, con la evidencia recolectada, analizan el código malicioso y los dispositivos infectados, hacen trazabilidad, identifican los vectores de ataque y las vulnerabilidades. En el Observatorio del Cibercrimen estas serán un indicador de los últimos avances en la ciberseguridad de los ciudadanos y de las instituciones públicas y privadas y para garantizar la respuesta.

> **"En el Conpes 2.0 hemos planteado una fiscalía especializada en cibercrimen. Por ahora se ha conseguido la destinación exclusiva de algunos fiscales que atenderán estas situaciones".**
>
> **Coronel Fredy Bautista**

Renovar la ley colombiana

En busca de corregir los vacíos que ha traído el ciberdelito se hace necesario actualizar también la reglamentación del país, de tal forma que, además, permita enfrentarlo en conjunción con otras naciones. Empero, los legisladores no están pendientes de las nuevas tecnologías o de los crímenes que estas facilitan para hacer leyes contra ellos. "Esperemos que este proceso sea más dinámico; por ahora es muy lento", señala Adrián Eduardo Acosta, oficial de Crimen Digital de la Interpol.

Eso es lo que pretende impulsar el Conpes sobre ciberseguridad, pues Colombia necesita ponerse al día en el tema. El coronel Fredy Bautista asegura que hay dos leyes importantes en la materia: la Ley 1273 de 2009 y la Ley 906 de 2004. La primera estableció nueve tipos penales autónomos de delitos cibernéticos y la creación de un nuevo bien jurídico (la protección de la información y de los datos y la definición de los atentados contra la confidencialidad, la integridad y la disponibilidad). Además, involucró otras dos conductas: el hurto por medios informáticos y la transferencia no consentida de activos. La segunda diseñó

una línea procedimental para investigación. "En el Conpes 2.0 hemos planteado una fiscalía especializada en cibercrimen —dice—. Por ahora se ha conseguido la destinación exclusiva de algunos fiscales que atenderán estas situaciones".

Entre otras tareas pendientes, el teniente Óscar Mojica, del Centro Cibernético Policial de la Dijin, mencionó la actualización del Código Penal "para que no se quede corto a la hora de judicializar estos delitos".

¿Y los derechos humanos y la privacidad?

Una forma de empezar a combatir crímenes que mutan tan rápidamente como la tecnología es "adaptarnos y empezar a investigar distinto a como lo hacíamos antes, partiendo del hecho de que luchamos con organizaciones muy bien formadas, dedicadas exclusivamente a tratar de delinquir a través de internet —aconseja Adrián Eduardo Acosta—. En este sentido, las empresas de tecnología cobran preponderancia porque son las que nos brindan mucha información, la Policía ya no es la primera fuente".

Sin embargo, esta realidad ha alertado a los defensores de derechos humanos que ven un peligro en los vacíos legales y en la posibilidad del desbordamiento del poder de las autoridades en desmedro del derecho a la privacidad.

Para ellos, existe una tensión entre ciberseguridad y el derecho a la privacidad y a la intimidad. Carolina Botero, abogada de la Fundación Carisma, dice que el reto será entender esos conceptos, su alcance y mantenerse alerta, de tal forma que aspectos como el debido proceso o el derecho de asociación y otros no se vean afectados. Lo anterior implica mejorar los controles a la actividad de inteligencia porque la entidad democrática destinada a ello —la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia del Senado— no es operativa y sus informes son secretos. "Sin grandes modificaciones a la legislación, el Estado podría hacer reportes de transparencia y permitir así una mayor vigilancia de la sociedad civil".

Avances del Conpes 3701

La capitán Milena Elizabeth Realpe Díaz, analista del Comando Conjunto Cibernético de las Fuerzas Militares, y Jorge Fernando Bejarano Lobo, director de Estándares y Arquitecturas de TI del MinTIC, explicaron los ejes estratégicos y las unidades de soporte de este documento de política pública cuyo objeto es priorizar la inversión oficial. Estos son algunos de los temas que tratará:

1. Gobernanza: articulación de los esfuerzos e iniciativas para cumplir los objetivos.
2. Desarrollo de capacidades en tecnología, fortalecimiento del capital humano; implementación de observatorios y centros de excelencia; capacidades criptológicas.
3. Generación de conciencia y cultura con capacitación, fortalecimiento de programas de prevención en todos los estamentos; investigación, innovación y desarrollo.
4. Elaboración de un catálogo nacional de infraestructura crítica cibernética para su protección y para la gestión de incidentes que las involucren.
5. Marco legal. Se propiciará una ley en ciberdefensa y ciberseguridad. Se abordarán, entre otros, los siguientes temas relacionados con el ciberespacio: derecho internacional humanitario y derechos humanos; criptología; cooperación y diplomacia; cooperación nacional; redes de intercambio de información, reporte de incidentes e investigación.
6. Seguimiento e indicadores para controlar y gestionar el cumplimiento de las instancias responsables.

En lo anterior coincide el abogado Mateo Gómez, de la Comisión Colombiana de Juristas, y va más allá al destacar que ni la Ley Estatutaria de Inteligencia y Contrainteligencia, ni la Ley de Acceso a la Información y Transparencia están sometidas a una rendición de cuentas ciudadana porque se considera que tratan asuntos de seguridad nacional, "pero esa es una idea que no es legítima en un Estado de Derecho". De tal manera exhorta a diseñar una regulación muy específica con la cual los ciudadanos tengan la capacidad de prever hasta dónde puede llegar una investigación en el ciberespacio. Esto se justifica porque "cuando el Estado ejerce su poder en escenarios como los de las nuevas tecnologías tiene una capacidad invasiva y de intromisión en la esfera de la intimidad que debe limitarse".

La nube es otro escenario donde se requieren garantías de confiabilidad y respeto del manejo que se le da a la información de los consumidores que, cada vez con mayor frecuencia, se convierten en usuarios de estos servicios. "Muchas de las empresas de tecnología están migrando hacia allí. Y eso genera una gran responsabilidad", dice Andrés Umaña, de la dirección de Asuntos Legales y Corporativos de Microsoft, quien señala que todas las compañías tienen una política de transparencia entre sus procesos, en la recolección de datos y es importante la protección de lo que se captura. Pero la abogada Botero asegura que esto no sucede entre las locales y mucho menos en las *apps*, que afectan la vida cotidiana.

La posición de Katitza Rodríguez, directora internacional de los derechos de Electrónica Frontier Foundation, difiere de la de los dos abogados. Ella opina que "la privacidad no está por encima de todo, no hay derechos absolutos, hay que limitarlos conforme al derecho internacional para permitir que los servicios de inteligencia y la Policía hagan su trabajo, pero sí es necesario un balance". Por otra parte, le parece legítimo hacer minería con la metadata (datos sobre los datos), aunque plantea cuestiones aún sin resolver como qué mandos legales autorizan el uso de esas herramientas: "Hay muchas dudas sobre información que es muy íntima".

En tanto, el coronel Fredy Bautista afirma que en el Conpes se contempla la necesidad de generar el equilibrio entre las garantías para la seguridad ciudadana, el derecho a la privacidad y la necesidad de investigar. ■