Colombia, estrategia nacional en ciberseguridad y ciberdefensa

Coronel (R.) Jairo Andrés Cáceres García, Ejército de colombia

Introducción

Siempre se destaca el cómo ha cambiado el mundo y la forma en que vivimos, gracias a la tecnología. Generalmente con un enfoque positivo, aunque hay que reconocer que detrás de lo bueno puede venir lo malo, también se ha convertido en la solución más acertada para las empresas, y el factor estratégico fundamental para la economía de cualquier país, está produciendo cambios significativos en el ámbito económico, social, cultural, militar, político y en la educación de nuestro país. Más sin embargo, no todo es color de rosa, pues bien, ya están las ciberamenazas; por esto se debe entender el apagón de computadores, el ataque contra procesos industriales de fabricación de armas nucleares y otros que afectan de una forma importante a países que son atacados de una forma digital y virtual. El nuevo concepto de la guerra está basado en armas digitales mucho más difíciles de detectar.

El teórico de la guerra alemán Carl Von Clausewitz decía que "*la guerra es un acto de violencia para obligar a nuestro enemigo a hacer nuestra voluntad*". Pero, ¿se puede ejercer esa violencia desde un teclado? Sobre esta pregunta han discutido expertos en tecnología, seguridad y teóricos de la guerra. Aunque su conclusión no es unánime, las ciberamenazas son una realidad inevitable tanto tecnológica como políticamente.

Es importante tener presente que cuanto mayor es el desarrollo de una sociedad, mayor dependencia tiene a la tecnología y a los sistemas de información y comunicaciones, por ende mayor vulnerabilidad y mayor riesgo de sufrir incidentes de seguridad en la información e infraestructura crítica.

De acuerdo con el observatorio de Ciberseguridad en América Latina y del Caribe, el cibercrimen le cuesta al mundo US $ 575.000 millones anuales, y en América Latina y el Caribe, estos delitos cuestan alrededor de US$90.000 millones anuales.

Colombia es el primer país de América Latina en adoptar una estrategia para prevenir y enfrentar delitos y minimizar el nivel de riesgo de los ciudadanos ante amenazas o incidentes de naturaleza cibernética.

Dicha estrategia –gracias a la cual los colombianos podrán sentirse más seguros en el ciberespacio– fue aprobada por el Consejo Nacional de Política Económica y Social (Conpes) 3701 del 14 de julio del 2011, donde se establecen los lineamientos de Política para Ciberseguridad y Ciberdefensa, de Colombia, sesión que lideró el Presidente Juan Manuel Santos, de esta manera el país adopta una estrategia integral, lo cual se constituye en un paso muy importante de seguridad.

Una estrategia integral, comprensiva, que involucra todos los matices, las aristas para enfrentar retos de seguridad doméstica, de cibercrimen que puedan darse al interior de las distintas comunidades o individuos que utilizan el ciberespacio en nuestra sociedad.

Pero también retos de ciberdefensa, es decir, los riesgos de afectación de infraestructura crítica, hidroeléctrica, de transporte, de la propia seguridad o de instituciones importantes educativas o de salud, por amenazas que tienen que ver con la utilización del ciberespacio", indicó el Ministro de Defensa.

Asimismo el 28 de abril del 2016, el Gobierno Nacional emitió un segundo CONPES 3854 Política Nacional de Seguridad Digital, "Es precisamente por esto que la política nacional de

seguridad digital, objeto de este documento, cambia el enfoque tradicional al incluir la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital. Esto lo hace bajo cuatro principios fundamentales y cinco dimensiones estratégicas, que rigen el desarrollo de esta política. De los primeros destaca que la política nacional de seguridad digital debe involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas. Principios que se reflejan en las dimensiones en las que esta política actuará, las cuales determinan las estrategias para alcanzar su objetivo principal: fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital."

Resumen

El objetivo de este documento es ambientar a los lectores sobre la *"Visión Multilateral de la Ciberdefensa y Ciberseguridad en Colombia.*

Colombia no ha sido indiferente a la tendencia mundial, se ha incrementado considerablemente el uso de tecnologías de la información y las comunicaciones y así aumentando su nivel de riesgo ante las ciberamenazas.

Gracias a sus buenas prácticas en cuanto a las nuevas tecnologías, Colombia ha escalado siete posiciones en el reporte global de las tecnologías de la información. Este rendimiento positivo se ve reflejado por el crecimiento de usuarios en internet —alrededor de 6.634.659 personas son suscriptoras de banda ancha en el país— y la reducción de costos en tarifas de prestación de este servicio.

No hay duda. Llegó una nueva guerra basada en armas digitales mucho más difíciles de detectar. Un ataque digital al sistema informático de una entidad o de un país puede causar daños inmensos y su recuperación puede tomar un tiempo muy largo.

Desarrollo

Con respecto a la seguridad cibernética, Colombia ha sido objeto de ataques. Un caso a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo "hacktivista" autodenominado Anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas. Este ataque se dio en protesta al Proyecto de Ley "*por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet"*. Este grupo ha atacado indistintamente entidades públicas y privadas, entre las que se cuentan PayPal, el banco suizo Post Finance, MasterCard, Visa y páginas web del gobierno Suizo. (Información tomada del documento CONPES 3701).

En el año 2011 el gobierno Colombiano, elaboró el CONPES 3701 (Consejo Nacional de Política Economía Social), máximo organismo de coordinación de la política económica en Colombia. No dicta decretos, sino que da la línea y orientación de la política macro, sobre un tema específico, en este caso la *Ciberseguridad y la Ciberdefensa.*

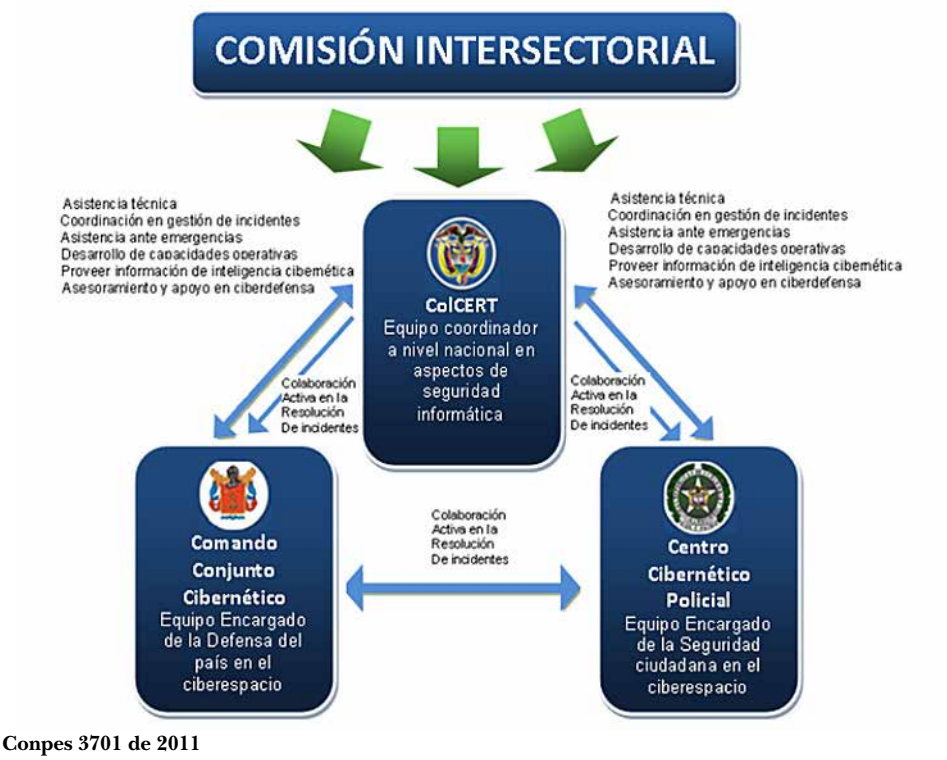
El Conpes está presidido por el primer mandatario del país y la secretaría técnica la ejerce el jefe del Departamento Nacional de Planeación, que elabora los documentos para ser tratados en cada una de las sesiones.

Fue así que nació el CONPES 3701 el 14 de julio del 2011, que trata sobre los "Lineamientos De Política Para Ciberseguridad Y Ciberdefensa" de Colombia, el cual busca generar lineamientos de política en ciberseguridad y ciberdefensa tendiente a desarrollar una estrategia nacional para contrarrestar el crecimiento de las amenazas informáticas que afectan significativamente al

país. Asimismo, recopila antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

En cumplimiento del CONPES 3701, Colombia empezó a estructurar una ciberdefensa sólida, innovadora, creativa y siempre actualizada, no solo para prevenir ataques informáticos contra instituciones estatales, sino para poder estructurar una ciberdefensa activa, algo que se debe hacer para la defensa del TI gubernamental. La ciberdefensa que se implemente debe ser proactiva, dinámica y al día con las amenazas que puedan llegar. Debe ser un laboratorio con un radar digital que permita ver en forma oportuna las posibles amenazas.

Dentro de los aspectos más resaltantes del CONPES 3701, está la conformación de la *Comisión Intersectorial,* con representación del Ministerio de Defensa Nacional con el ColCERT, el Comando Conjunto Cibernético (CCOC) en el Comando general de las FFMM y finalmente el Centro Cibernético Policial (CCP) a cargo de la Policía Nacional:



Fuente: Conpes 3701 de 2011

- *El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert),* encargado de coordinar a escala nacional los aspectos de ciberseguridad y ciberdefensa.

- *El Comando Conjunto Cibernético de las Fuerzas Militares,* (CCOC) que tendrá la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio.

- *El Centro Cibernético Policial,* (CCP) que estará a cargo de la prevención e investigación y apoyará la judicialización de los delitos informáticos. Para ello, contará con un comando de Atención Inmediata Virtual (CAI Virtual), para recibir las denuncias de los ciudadanos.

Importante citar que en el mes de marzo del 2014, el presidente de Colombia, solicitó una asesoría internacional, con expertos en seguridad cibernética, y apoyo de la OEA, fue así como se instaló "*La Misión de asistencia técnica en Seguridad Cibernética*". El Ministro de Defensa Dr. Pin-

zón, reafirmó el compromiso del gobierno Colombiano, en dar los pasos necesarios y crear los mecanismos para proteger a Colombia en materia de ciberseguridad y ciberdefensa, así mismo que las FFAA de Colombia deben prepararse para proteger a la Nación de cualquier ataque que pueda venir del ciberespacio y por ello debemos tener una ciberinteligencia y ciberdefensa, para enfrentar estos retos...

Los expertos internacionales que participaron de esta Misión de Asistencia Técnica son funcionarios de los gobiernos de Canadá, España, Estados Unidos, el Reino Unido, República Dominicana, Estonia, Israel, Corea del Sur y Uruguay. De igual forma, además de funcionarios de la OEA, esta Comisión Internacional contó con la participación de representantes del Consejo de Europa (COE), el Foro Económico Mundial (WEF), INTERPOL, Organización de las Naciones Unidas (ONU), la Organización para la Cooperación y el Desarrollo Económico (OCDE), y la Universidad de Oxford. Las recomendaciones de los expertos fueron redactadas en sesiones privadas, con el objetivo de garantizar un análisis equilibrado e imparcial de las necesidades y pasos a seguir que deberían ser considerados por el gobierno colombiano.

Dentro de las principales recomendaciones de esa misión de asistencia, están:

Primero. Armonización con la Convención de Budapest: La legislación Colombiana debe armonizarse con la Convención de Budapest, en especial, en Derecho Procesal Penal, y posteriormente solicitar adherirse a esta convención del Consejo de Europa.

Segundo. Tener en cuenta legislaciones exitosas en Delitos Informáticos: Le recomiendan a Colombia tener en cuenta legislaciones de ciberdelincuencia como la de República Dominicana y la de Portugal, así mismo, recomiendan la importancia de utilizar en la legislación términos tecnológicamente neutrales, esto, con el objetivo de facilitar la interpretación y aplicación de la ley penal.

Tercero. Retención mandatoria de datos de tráfico: Se recomienda a Colombia la retención mandatoria de datos de tráfico por un término mínimo de un año, garantizando los derechos constitucionales del país, en particular los derechos a la privacidad y protección de datos personales.

Cuarto. Participación de actores claves para regulación: Establece la promoción de la participación del sector privado, sector académico y de la sociedad civil en leyes y reglamentaciones en materia de infraestructura critica, seguridad cibernética bajo garantía de confidencialidad.

Quinto. Otras recomendaciones relevantes: Se realizaron otras recomendaciones relevantes como es la capacitación a jueces y fiscales en materia de delitos informáticos, así como el manejo adecuado de la evidencia digital, la implementación de mecanismos de cooperación internacional.

La misión respondió positivamente a la solicitud del Presidencial, y fue así que se realizó entre el 31 de marzo y el 4 de abril del 2014, atraves del *Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE)*, que pertenece a la Secretaria de Seguridad Multidimensional de la OEA. Estuvo integrada por 18 reconocidos expertos de diferentes organizaciones internacionales y países, relacionados anteriormente. El objetivo de la Misión fue la elaboración de una serie de recomendaciones que proporcionaran al Gobierno una sólida base técnico-profesional para su eventual implementación.

Para recapitular sobre los avances de Colombia en materia de Ciberseguridad y Ciberdefensa, después de 4 años de ejecución del CONPES 3701, del cual Colombia es pionero en Latinoamérica, actualmente ocupa por ende un puesto muy destacado en el continente.

El enfoque de la política de Ciberseguridad y Ciberdefensa, (CONPES 3701), se focalizó en contrarrestar el crecimiento de las amenazas cibernéticas bajo los objetivos de defensa del país;

y lucha contra el cibercrimen. Posicionando a Colombia como una de los líderes en la materia a nivel regional, dejando de lado *la gestión del riesgo en el entorno digital.* Aspecto muy importante en el incremento en el uso de las TIC para realizar actividades económicas y sociales.

Con base en lo anterior nació el CONPES 3854 el 11 de abril del 2016, *la política nacional de seguridad digital,* el cual cambia el enfoque tradicional al incluir la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital. Esto lo hace bajo cuatro principios fundamentales y cinco dimensiones estratégicas, que rigen el desarrollo de esta política. De los primeros destaca que la política nacional de seguridad digital debe involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas. Principios que se reflejan en las dimensiones en las que esta política actuará, las cuales determinan las estrategias para alcanzar su objetivo principal: fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital. Para lograrlo, se implementarán acciones en torno a cinco ejes de trabajo.

Finalmente, como se mencionó anteriormente el 28 de abril del 2016, el Gobierno Nacional emitió un segundo CONPES 3854 Política Nacional de Seguridad Digital, "el enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del país; y (ii) lucha contra el cibercrímen. Si bien esta política ha posicionado a Colombia como una de los líderes en la materia a nivel regional, ha dejado de lado la gestión del riesgo en el entorno digital. Enfoque esencial en un contexto en el que el incremento en el uso de las TIC para realizar actividades económicas y sociales, ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Hecho que demanda una mayor planificación, prevención, y atención por parte de los países. Tema del cual se ocupa el CONPES 3854, de abril del 2016." ❑

Coronel (R.)Jairo Cáceres, Ejército de Colombia. Se graduó como oficial de artillería de la Escuela Militar de Cadetes del Ejército Colombiano y se escalafonó al Cuerpo Logístico y Administrativo. Bajo banderas durante 31 años, pasó a la reserva activa en 2007. Desempeñó cargos importantes en la área Logística, y como catedrático de Ciberguerra y Logística Militar y en Apoyo a Servicios para Combate en Operaciones contra el Narcoterrorismo. Escribió el libro "Guerra Cibernética; Campo de Batalla del Siglo XXI" y es autor del manual de Seguridad Informática Ejército. Egresado de la Universidad Autónoma Guadalajara, México con un Máster en Informática. Representó al Ministerio de Defensa Nacional como experto ante la comisión internacional con representantes del Consejo de Europa y otros países de OEA. Orador principal de la Escuela de Guerra del Ejército en el área de Ciberseguridad y Ciberdefensa. Ha escrito varios artículos sobre Ciberguerra y Logística Militar en revistas nacionales e internacionales.