CONPES 3701: COLOMBIA HACIA UN FUTURO CON CIBERSEGURIDAD Y CIBERDEFENSA

López, Diana Marcela
Universidad Piloto de Colombia
Bogotá, Colombia
dlopez98@hotmail.com

Resumen - En este documento se muestra y analiza la estrategia desarrollada por el Gobierno Colombiano a través del documento CONPES 3701, para prevenir y contrarrestar las amenazas en el ámbito cibernético que puedan afectar la soberanía nacional del estado Colombiano.

Abstract - This paper shows and analyzes the strategy developed by the Colombian Government through the document CONPES 3701, to prevent and counter threats in the cyber realm that can affect the national sovereignty of the Colombian state.

Índice de Términos - Ciberseguridad, Ciberdefensa, Ciberespacio, Seguridad de la Información.

I. INTRODUCCIÓN

El avance tecnológico, el crecimiento en el uso de internet y el aumento de las transacciones monetarias por este medio, han ocasionado el incremento de los delitos informáticos, que amenazan no solo la integridad, disponibilidad y confidencialidad de uno de los activos más importantes "La Información", sino que afectan la seguridad de todo un Estado, colocando en riesgo la infraestructura critica tanto de entidades públicas como privadas, la cuales son las que mantienen la operación y la gobernabilidad de un país.

El ciberespacio ha visto un aumento de sus riesgos asociados a la seguridad, debido al incremento de las acciones ilícitas cometidas a un servicio informático, la utilización del internet por parte de grupos terroristas para ejecutar actividades de financiación, inteligencia, propaganda, captación y ciberespionaje

a gran escala entre estados y/o empresas y el incremento de los delitos contra la privacidad de los usuarios en Internet, son solo algunos de los retos a los que deben enfrentarse los responsables de las fuerzas de seguridad encargados de la Ciberseguridad y la Ciberdefensa de un país.

Para contrarrestar las amenazas a las que están expuestas las infraestructuras físicas y la información tanto del sector público como del privado en Colombia, el gobierno nacional ha trabajado mancomunadamente con diferentes entidades del orden nacional apoyados con la experiencia de aliados extranjeros, con el fin de generar un marco de gobernabilidad en Ciberseguridad y Ciberdefensa, el cuál plantea una estrategia con unos lineamientos, leyes e iniciativas que permiten pautar las acciones necesarias para la protección y fortalecimiento de la infraestructura crítica del Estado Colombiano, frente a emergencias cibernéticas que atenten o comprometan la Seguridad y Defensa Nacional.

II. ESTRATEGIA EN SEGURIDAD Y CIBERDEFENSA EN COLOMBIA

Para entrar en contexto debemos tener en claro algunos de los siguientes conceptos claves que serán usados durante la profundización del tema:

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. [1]

Ciberdefensa: Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional. [2]
Ciberespacio: Red interdependiente de infraestructuras de tecnología de la información, que incluye internet y otras redes de telecomunicaciones, sistemas computacionales, procesadores integrados y controladores de industrias críticas. [3]

Debido al aumento significativo en el uso de las tecnologías, lo cual se ha visto evidenciado en el crecimiento que ha tenido en los últimos años las conexiones a Internet de banda ancha, en donde el país pasó de tener 2,2 millones de conexiones en 2010 a 8,8 millones en 2014 de acuerdo a las estadísticas reveladas en el último informe trimestral del Ministerio de Tecnologías de la Información y las Telecomunicaciones (MINTIC), han ocasionado el aumento de vulnerabilidades a las que están expuestas las redes de comunicaciones y por ende lo que viaja a través de ella, toda la información de un país.

El siguiente gráfico muestra las estadísticas de crecimiento de internet en Colombia en los últimos años:

Figura 1 Crecimiento uso de internet en Colombia

Teniendo en cuenta los antecedentes de ataques cibernéticos en países como Estonia, Estados Unidos, Rusia y China entre otros, así como el aumento de ataques en los últimos años a Entidades oficiales y privadas en nuestro país, el Gobierno de Colombia desarrollo una estrategia en Julio del 2.011, donde se establecen los lineamientos de una política para la Ciberseguridad y Ciberdefensa, con el fin de contrarrestar las amenazas informáticas, a través del Consejo Nacional de Política Económica y Social, en el documento CONPES 3701.

Para dar cumplimiento a los objetivos y al plan de acción propuesto en dicho documento, el Ministerio de Justicia, el Ministerio de Relaciones Exteriores, el Departamento Administrativo de Seguridad, la Fiscalía General de la Nación y el Ministerio de Tecnologías de la Información y las Telecomunicaciones, definieron que el Ministerio de Defensa Nacional, lideraría y establecería los mecanismos necesarios para proteger a los ciudadanos de los riesgos cibernéticos.

El documento CONPES 3701, debía cumplir con los siguientes tres objetivos primordiales:

1. Adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar, generar recomendaciones para afrontar las amenazas y los riesgos que se presenten. [4]

2. Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en Ciberdefensa y Ciberseguridad. [5]

3. Fortalecer la legislación en estas materias, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales.[6]

Pero como y a través de que instancias Colombia enfrentará el gran reto de defender al Estado de ataques cibernéticos?

El siguiente gráfico presenta los organismos creados por el Gobierno de Colombia para proteger la

infraestructura crítica del país y su respectiva coordinación interna:

Figura. 2. Modelo de Coordinación

La primera instancia creada por el Gobierno Nacional fue el COLCERT en septiembre del 2.011, integrada por funcionarios civiles, militares y en comisión de otras Entidades; este Grupo de Respuesta a Emergencias Cibernéticas de Colombia, tiene como responsabilidad la coordinación de las acciones necesarias para la protección de la infraestructura crítica del estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional. [7]

Así mismo es muy importante resaltar que el COLCERT en noviembre del 2.013 fue aceptado como miembro del FIRST, Forum of Incidents Response and Security Teams, el cual reúne a todos los centros de coordinación CERT's alrededor del mundo, y de los diferentes sectores, tanto público como privado en pro del intercambio de información, lo que permite una respuesta más eficiente a los incidentes cibernéticos que deban atender. [8]

Otra instancia creada fue el Comando Conjunto Cibernético de las Fuerzas Militares, el cual está conformado por 20 expertos pertenecientes a los sectores de comunicaciones, ingeniería, aviación e inteligencia de las tres ramas de las Fuerzas Militares de Colombia, con el objetivo de preservar la defensa cibernética del Estado, responder ante ataques cibernéticos, asegurar la protección de infraestructura crítica, y defender las redes informáticas Militares. Como apoyo a esta Dependencia se creó en cada Fuerza (Ejército, Armada y Fuerzas Aérea) Unidades de Comando Cibernéticos.

Por otra parte y como ente responsable de la prevención, la investigación y apoyo en la judicialización de los delitos informáticos se creó el Centro Cibernético Policial (CCP), que cuenta con un comando de Atención Inmediata Virtual (CAI Virtual) para recibir las denuncias de los ciudadanos.

El CCP está operando con un personal de 120 funcionarios, el trabajo entre el CCP y el COLCERT ha sido muy coordinado, ya que este último ha suministrado al CCP, información de soporte para la identificación de perfiles de integrantes de Anonymous y el CCP ha brindado apoyo constante al COLCERT en la investigación judicial de diferentes casos en los que se ha comprometido la Ciberseguridad de varias entidades del Gobierno y del sector privado. [9]

El trabajo mancomunado de las instancias gubernamentales mencionadas anteriormente, ha logrado que Colombia apoye a otros países de América Latina en temas de Ciberseguridad y de igual forma hemos recibido un valioso apoyo de la Organización de los Estados Americanos (OEA) a través del Comité Interamericano contra el Terrorismo (CICTE) .

Pese a los grande esfuerzos y avances que ha hecho el Gobierno para prevenir y contrarrestar las amenazas en el ámbito Cibernético, en la vigencia del 2.014 año en el que finalizo el plan del CONPES 3701, se presentaron una serié de sucesos que afectaron la Ciberseguridad del Estado, como el

caso de la central de interceptaciones Andrómeda y el seguimiento a correos electrónicos y chats de personajes de la vida pública que obligaron al presidente Juan Manuel Santos a crear el Plan de Ciberseguridad y Ciberdefensa, con la formalización de una Comisión Digital, que depende directamente del Presidente de la República y de la Agencia Nacional de Seguridad Cibernética. Ambos entes la Comisión y la Agencia acopiarán todos los esfuerzos públicos, privados, regulatorios, de relacionamiento internacional y crearán políticas de Ciberseguridad y Ciberdefensa para el país, así mismo fortalecerán las oficinas de seguridad digital de las Fuerzas Militares y de la Policía Nacional y también acordaran convenios internacionales y articularán a la empresa privada, y a la ciudadanía en torno a una política pública única sobre seguridad digital.

Como avance significativo y en concordancia con lo anterior, en los meses de marzo y abril del 2.014 una comisión de expertos en Ciberseguridad y Ciberdefensa de Canada, España, Estados Unidos, Reino Unido, República Dominicana, Estonía, Israel, Corea del Sur y Uruguay, convocados por la Organización de los Estados Americanos (OEA), analizaron las actividades que diferentes entidades han realizado en este campo, llegando a la conclusión que a pesar de que Colombia tiene una gran capacidad técnica y tecnológica, muy avanzada para la región y no muy lejos de las grandes potencias, todavía, en temas de operatividad y de coordinación aún falta mucho camino por recorrer.

Como recomendación la Comisión de expertos le sugirió al Gobierno la creación de un órgano de control en cabeza de un civil, quién ejercería una especie de veeduría ciudadana y rendiría cuentas a la Presidencia sobre los reportes de Ciberdefensa y Ciberseguridad emitidos por las centrales de inteligencia del Ministerio de Defensa y de la Policía Nacional

III. CAPACITACIÓN Y CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Una vez creados y articulados los organismos encargados de prevenir y contrarrestar toda amenaza e incidente de naturaleza cibernética que afecte al estado, es fundamental educar socialmente a las personas con el objetivo de que adopten una posición consciente de la seguridad en el Ciberespacio.

Para ello se han venido desarrollando una serie de capacitaciones, seminarios y diplomados especializados en Ciberseguridad y Ciberdefensa en convenio entre MinTIC y la Escuela Superior de Guerra, en donde se ha contado con la participación de funcionarios que laboran en los organismos creadas por el Gobierno de Colombia para proteger la infraestructura crítica del país, funcionarios de más de 20 entidades públicas y privadas, así mismo se dicta una cátedra de Ciberguerra dirigida a los altos mandos militares. [10]

De igual manera el COLCERT ha adelantado capacitaciones para el gobierno, la rama judicial, la fuerza pública y el sector privado, y viene recibiendo asesoría del NICE (National Initiative for Cibersecurity Education) y entidades como el CICTE (Comité Interamericano contra el Terrorismo), el Comando Sur y el Departamento de Justicia de Estados Unidos, han prestado servicios de capacitación a funcionarios colombianos.

Otra avance significativo en el tema de capacitación es que el Ministerio de Defensa y el Ministerio de TICs logró que el Sena incluyera dentro de su oferta educativa cursos de Ciberseguridad y Ciberdefensa, lo que permitirá que ciudadanos del común tengan acceso a recibir formación en temas tan importantes y relevantes para un país como lo es la seguridad y defensa en el ámbito cibernético.

Por otra parte a través de la campaña “En TIC confío”, del Ministerio de TICs se están llevando cabo campañas de sensibilización y concienciación a nivel empresarial en el sector público y privado y se crearon unas mesas de trabajo para diseñar campañas de uso seguro de internet.

Pero si bien es cierto y aunque el gobierno Colombiano está realizando un esfuerzo significativo en el tema de la creación de instancias que trabajan mancomunadamente para salvaguardar

la infraestructura critica del estado de un posible espionaje informático o un sabotaje cibernético, evidentemente se requiere concientizar a los ciudadanos a todos los niveles, iniciando desde los centros educativos y todas las instituciones tanto de carácter público como privado, teniendo como base que un usuario del común con acceso a sistemas informáticos, debe tener unas mínimas nociones de cómo mantener su entorno cibernético seguro, de que y como se puede publicar en el ciberespacio, sin comprometer la privacidad, confidencialidad y disponibilidad de sus datos.

Es importante recalcar la importancia de crear conciencia en nuestras futuras generaciones, quienes están accediendo a muy temprano edad al uso de las nuevas tecnologías, por ello a través de programas educativos, campañas sociales y prevención desde el hogar a través del uso de herramientas básicas como antivirus, configuración del firewall, actualizaciones automáticas y la vigilancia por parte de los padres a los contenidos de la web que sus hijos consultan y en el manejo de las redes sociales, de esta manera estaríamos formando ciudadanos responsables en un uso seguro de internet, capaces de identificar claramente las amenazas a las que están expuestos y de esta manera minimizaríamos en gran medida el riesgo de un ataque cibernético en un futuro.

IV. LEGISLACIÓN COLOMBIANA EN CIBERSEGURIDAD

Uno de los objetivos trazados dentro de la estrategia contemplada en el documento CONPES 3701, es la de fortalecer la legislación Colombiana en temas de Ciberseguridad y Ciberdefensa. Pero se ha logrado fortalecer y desarrollar la legislación Colombiana en este tema?

Como antecedes de carácter jurídico en Colombia se tiene la Ley 1273 del 05 de enero del 2.009, que trata de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

El 14 de Enero del 2.013 se creó la Comisión Digital y de información estatal en cumplimiento al Documento CONPES 3701 del 14 de julio de 2011, encargada de coordinar y orientar el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado Colombiano, emitir los lineamientos rectores del Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Defensa Nacional y asesorar al Gobierno Nacional en materia de políticas para el sector de tecnologías de la información y las comunicaciones.

Por otra parte el 11 de septiembre de 2.013, el Consejo de Ministros de Europa dio su aprobación para invitar a Colombia a adherir a la Convención de Budapest, que trata sobre “Delito Cibernético", este convenio es el único marco global existente para aplicar una política penal común con el objetivo de proteger a la sociedad frente a la ciberdelincuencia, mediante la adopción de legislación adecuada y el fortalecimiento de la cooperación internacional. [11]

En este orden de ideas la Convención de Budapest termina siendo entonces una de las posibles salidas al frente jurídico que pueden traer los protocolos para la Ciberdefensa y el Ciberespacio. La idea, según fuentes del Ministerio de Defensa, es crear una hoja de ruta en términos operacionales para que no se violen los derechos humanos pero que tampoco quede sin protección la soberanía de la nación. Además, que Colombia pueda llegar a cumplir con las exigencias de los estándares internacionales y tener mejores prácticas en temas jurídicos.

A través del Manual 3.0 de Gobierno en Línea, el Ministerio de TICs generó una serie de directrices en temas de seguridad de la información basado en estándares internacionales, que deberán ser implementadas por las entidades del sector público.

Un antecedente muy importante son las recomendaciones dadas por la Organización de los Estados Americanos (OEA), entre las que se encuentran: Establecer un régimen rápido y

eficiente para asegurar la cooperación internacional en la prevención, investigación y persecución penal de los delitos informáticos, creando un punto de contacto para La Red 24 / 7, disponible las 24 horas del día, 7 días a la semana, con la finalidad de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito y solicitar a las principales empresas proveedoras de servicios de internet, que albergan servidores con datos de ciudadanos de Colombia, que revisen los mecanismos de cooperación en materia penal, a fin de posibilitar que estas compañías respondan a tiempo las solicitudes de asistencia en materia penal. [12]

Sin embargo, la tecnología va mucho más rápido que la legislación. En ese sentido, mientras se crean normas para atacar delitos cibernéticos, surgen nuevas tecnologías para burlarlas y los criminales se aprovechan de esta situación. Aparte de esto, falta capacitación en este campo entre los organismos judiciales, el problema es el desconocimiento en la materia de parte de jueces, fiscales y organismos de policía judicial.

Por lo anterior el Estado debe capacitar a los organismos judiciales en el tema de sensibilización y apropiación de las tecnologías de la información y la organización de cursos tanto en materia de delitos informáticos como en los aspectos técnicos y jurídicos de la obtención de evidencia digital, en la legalidad y constitucionalidad de la extracción de la evidencia digital, así como promover con la participación del sector privado, leyes y reglamentaciones que regulen las obligaciones para las empresas que tienen bajo su control infraestructura critica, deben reportar los incidentes de seguridad cibernética en un plazo no mayor a 48 horas, bajo garantía de confidencialidad.

A pesar de que en la justicia colombiana todavía no existe una cultura sólida digital, el país al ser pionero en materia de legislación de delitos informáticos, goza de un reconocimiento internacional. Pero lo más importante es que se les ha enviado un mensaje muy claro a los delincuentes: en Colombia sí se están investigando los delitos informáticos.

V. CONCLUSIONES

1. A pesar de que el estado Colombiano en los últimos años ha trabajado arduamente en el tema de Ciberseguridad y Ciberdefensa, es importante continuar y hacer parte de este proceso tanto al sector público como privado, con financiamiento que permita su continuo fortalecimiento y el pensamiento común deberá ser la forma de manejar, regular y enfrentar este problema de una manera inteligente, ponderada y obviamente basado en el conocimiento y en la experticia internacional, quienes darán sugerencias a las iniciativas gubernamentales para blindar a Colombia y a sus entidades de ataques cibernéticos.

2. Teniendo en cuenta que las empresas privadas se encuentran en una constante evolución en la forma de prestar y adquirir servicios, el riesgo en la protección de la información, bien puede disminuir o aumentar, sin contar con casos como el espionaje industrial, la vulneración de secretos industriales y otros fenómenos que alimentan la competencia desleal entre diferentes competidores y que cada vez se hacen más frecuentes en temas de ciberdelincuencia.

3. Las amenazas hoy en día son bastante avanzadas, necesitan una infraestructura de seguridad que trabaje conectada y permita actuar inteligentemente para la prevención de incidentes y la defensa de ataques. Actualmente no es suficiente tener un software de antivirus en los equipos de la organización. Se requiere contar con una tecnología que permita el análisis avanzado de amenazas y comportamientos anómalos. Para esto es necesario tener el 100 % de visibilidad de la información que transita en la organización.

4. La seguridad y defensa del ciberespacio tiene implicaciones civiles y económicas y esto lo convierte en un objetivo estratégico de la seguridad nacional, por lo tanto las personas que ostentan tal responsabilidad deben estar intelectualmente

preparados para sumir la defensa de un país en el teatro de operaciones del ciberespacio.

5. Es evidente que se deben generar mecanismos para crear conciencia ciudadana en temas de seguridad informática y para ello se requiere que toda la sociedad interactúe desde todos sus ámbitos, en el hogar, en las instituciones educativas, en las empresas, para crear un ambiente más seguro y confiable, en nuestro espacio cibernético.

6. Sería clave en el tema de trasferencia de conocimientos invertir en un plan de capacitación internacional apoyado por los altos niveles de gobierno con el objetivo de disminuir la brecha de conocimiento. El plan puede incluir programas de intercambio de corto, mediano y largo plazo con organismos relevantes en ciberseguridad, evaluaciones técnicas de y hacia otros países, y mayor cooperación con expertos internacionales.

REFERENCIAS

[1] [2] Ciberdefensa y Ciberseguridad. (2013, Junio). [En línea]. Disponible: http://www.cibercolombia2014.com/CyberIC.pdf

[3] Ciberseguridad y Ciberdefensa: Una primera aproximación. (2009, Octubre). [En línea]. Disponible: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

[4] [5] [6] Conpes. Documento Conpes 3701. (2.011, Julio 14)

[7] Ministerio de Defensa Nacional. (2009, Octubre). [En línea]. http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/ ciberdefensa.pdf

[8] Grupo de Respuestas a Emergencias Cibernéticas de Colombia. (2.010, Noviembre 22. [En línea]. Disponible: www.colcert.gov.co

[9] Centro Cibernético Policial. [En línea]. www.ccp.gov.co

[10] Diplomado en Ciberseguridad y Ciberdefensa. (2015, Enero). [En línea]. Disponible: http://www.esdegue.edu.co/node/5182

[11][12] Misión de Asistencia Técnica de Seguridad Cibernética (2.014, Abril). [En línea]. Disponible: http://www3.digiware.net/sites/default/files/Recomendaciones_COLOMBIA_SPA.pdf

FIGURAS

[1] Crecimiento de Internet en Colombia. [En línea] Disponible: http://es.slideshare.net/Ministerio_TIC/rendicin-de-cuentas-2014-37071547

[2] Documento Conpes 3701. Modelo de Coordinación. 14 de Julio de 2011. [En línea] Disponible: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf