La Seguridad y la Ciberdefensa en Colombia

Quintero Agudelo Yolanda
Yolja8@gmail.com
Universidad Piloto de Colombia

Abstract - With the launch of Cyber Security and Cyber Policy in the Colombian state is to protect critical infrastructure, the services provided to citizens, systems and assets on which operations are supported by entities the country, based on the prevention, detection and response to potential computer security incidents.

Resumen - Con la puesta en marcha de la política de Ciberseguridad y Ciberdefensa en el estado Colombiano, se busca proteger la infraestructura crítica, los servicios que se proveen a los ciudadanos, los sistemas y activos sobre los que se soportan las operaciones de las entidades en el país, teniendo como base la prevención, detección y reacción frente a los posibles incidentes de seguridad informática.

Índice de Términos—Amenaza Informática, Ciberdefensa, Ciberseguridad, Seguridad Informática-Política, Activo, Información, Cibercrimen, Cibernética.

I. INTRODUCCIÓN

El avance de las tecnologías y los medios asociados a éstas, hacen que día a día sea más difícil prevenir ataques cibernéticos y ciberterroristas en una nación, más aun en un país como el nuestro, donde no existe una conciencia ni política ni social al respecto.

Retomando las palabras del doctor VÍCTOR MONTERO, cuando dice: "Las personas todavía asocian la palabra ciberterrorismo con un filme de ciencia ficción y no existe un real entendimiento del significado del término", dice: "La palabra 'terrorismo' es tan fuerte que mucha gente cree que 'ciberterrorismo' es hacer explotar bombas con un mouse, algo que de seguro es posible, pero más comúnmente asociado a Hollywood que a la vida cotidiana." [1], son una muestra fehaciente de la falta de madurez en el tema en América, lo cual entorpece la aplicación y puesta en marcha de políticas de seguridad y ciberdenfensa en estos países, especialmente en Colombia.

II. ANTECEDENTES DE LA CIBERSEGURIDAD Y DEFENSA EN COLOMBIA

A. Fundamento legal

La Ciberdefensa y la ciberseguridad en Colombia está cimentada en:

- ✓ Ley 527 de 1999 - Comercio Electrónico [2]
- ✓ Ley 599 DE 2000 [3].
- ✓ Ley 962 de 2005 [4].
- ✓ Ley 1150 de 2007 [5].
- ✓ Ley 1266 de 2008 [6].
- ✓ Ley 1273 de 2009 [7].
- ✓ Ley 1341 de 2009 [8].
- ✓ Ley 1581 de 2012 [9].
- ✓ Ley 1712 de 2014 [10].
- ✓ Decreto 032 de 2013 [11].
- ✓ Decreto 2364 de 2012 [12].
- ✓ Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009 [13].
- ✓ Circular 052 de 2007 (Superintendencia Financiera de Colombia) [14].
- ✓ Documento CONPES 3701 de 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa [15].

B. Definición del Ciberseguridad y Ciberdefensa para el Estado Colombiano

***Ciberseguridad*:** "Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética" [15].

Ciberdefensa: "Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional" [15].

C. ¿Cómo hemos evolucionado en el tema?

A raíz de los diferentes incidentes de seguridad cibernética que han sufrido múltiples países entre ellos Colombia, es importante destacar que el Estado Colombiano ha venido realizando esfuerzos importantes en ésta materia, con el fin de proteger integralmente a sus conciudadanos.

1) Elaboración de lineamientos para la ciberseguridad y ciberdefensa en Colombia

"Es una obligación de todo Estado soberano proteger su infraestructura cibernética. Cualquier deterioro en la misma, no sólo afectaría al ciudadano común, sino también numerosos aspectos gubernamentales, industriales y del comercio" [16].

Es por ello que el Estado Colombiano con la puesta en marcha de una estrategia para la ciberseguridad y ciberdefensa a través del "CONPES 3701", buscó fundamentar mecanismos normativos, organizacionales e institucionales que le permitan afrontar los nuevos retos en seguridad cibernética en el país.

No se puede olvidar que la información es un Activo que, como otros importantes activos corporativos, industriales y comerciales tienen Valor para cualquier organización, y por tanto debe ser protegida adecuadamente, para ello se necesita legislación nacional en seguridad informática.

2) La activación del colCERT busca contrarrestar tres pilares problemáticos, así:

1. "Las iniciativas y operaciones en ciberseguridad y ciberdefensa no están coordinadas adecuadamente: A pesar de existir algunos esfuerzos institucionales (tanto privados como públicos), se ha identificado que no existen organismos a nivel nacional constituidos para coordinar y desarrollar operaciones de ciberseguridad y ciberdefensa. Por tanto, no ha sido posible implementar los mecanismos suficientes y adecuados para contrarrestar ataques cibernéticos y proteger los intereses del Estado en el ciberespacio.

Se evidencia una debilidad en la difusión, concienciación, generación de una cultura de prevención y acción segura en ciberseguridad, dirigida tanto al sector público como al privado, así como a la sociedad civil" [16].

Para ejemplificar éste eje se podrían retomar las palabras de VÍCTOR MONTERO, Director Ejecutivo de Operaciones de la Consultora Argentina Onapsis, cuando dijo: "la gran mayoría de las empresas que confían toda su información en sus infraestructuras críticas de negocio son en la actualidad susceptibles a estos ataques y no son conscientes de ello. Modificaciones de datos contables y de facturación, robo de fórmulas e información de patentes, manipulación de legajos y plantillas, robo de información de stock, clientes y secretos comerciales... todo esto también es ciberterrorismo" [1].

2. "Debilidad en la oferta y cobertura de capacitación especializada en ciberseguridad y ciberdefensa: El conocimiento en el área de ciberseguridad y ciberdefensa tanto en el sector público como en el privado es limitado. Si bien en el país existen algunas instituciones de educación superior que ofrecen especializaciones en seguridad informática y derecho informático, se ha identificado que la oferta académica en programas especializados en estas áreas es reducida. En consecuencia, un número significativo de personas que acceden a algún tipo de formación en el área de seguridad de la información, lo hacen mediante programas ofrecidos por instituciones extranjeras, en los que no se profundiza sobre la realidad colombiana" [15].

3. "Debilidad en regulación y legislación de la protección de la información y de los datos": [15]. Aunque ya existe en el país legislación sobre delitos informáticos, aún falta mucha comprensión en éstos temas para que se apliquen de forma más correcta en las leyes Colombianas, profundizando en ésta problemática de penalización en ciberdefensa y seguridad informática.

D. Aspectos relevantes de la Ciberseguridad y Ciberdefensa en Colombia

- ✓ "En conjunto el colCERT y CCP han respondido a incidentes de ciberseguridad, en donde se ha asesorado a diferentes organismos en temas de ciberseguridad y se ha atendido judicialmente incidentes.

- ✓ Con la CRC se está trabajando la regulación de los ISPs para conservar los logs de uso de Internet.

- ✓ 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.

- ✓ El Ministerio de Justicia actualmente adelanta una revisión integral del Código Penal, específicamente para el tema de tipificación actual de los delitos informáticos.

- ✓ El ColCERT es punto de contacto internacional para estos temas. Así mismo, sobresale el trabajo que se ha venido haciendo con la CICTE y los programas de cooperación y asistencia técnica en esta materia.

- ✓ El Gobierno está evaluando la posibilidad de adhesión al Convenio de Budapest" [17].

- ✓ En Colombia, se presentó una caída en 2012 con respecto a 2011 de la manifestación de delitos cibernéticos. [18].

- ✓ El Grupo de Respuesta a Emergencias Cibernéticas de Colombia participó del Ejercicio de Gestión de Crisis organizado por el Comité Interamericano contra el Terrorismo - CICTE, el pasado 25 de junio de 2013 en Washington D.C. [19].

- ✓ "A pesar del incremento en las cifras de delitos cibernéticos, estudio reciente revela que Colombia se posiciona como líder en Latinoamérica, ya que ningún otro país cuenta con una Política Nacional de Seguridad Cibernética. En el informe, "Tendencias en la Seguridad Cibernética en América Latina y el Caribe y respuestas de los Gobiernos", publicado por la Organización de los Estados Americanos - OEA, en colaboración con la firma TrendMicro, se revela que en 2012 se presentó un incremento en las cifras de los delitos cibernéticos en la región.

- ✓ Entre las cifras presentadas, se estima que dicho incremento se encuentra entre el 8% y 40% para la región; para el caso de Colombia, se presentó una caída en 2012 con respecto a 2011 de la manifestación de delitos cibernéticos, reportada por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, el ente coordinador en materia de seguridad cibernética a nivel nacional. Entre otros casos, Chile también reportó una disminución considerable en ataques de phishing y un 33% menos en cibercrimen, esto gracias a la acción del componente de judicialización. El componente de judicialización de Colombia, reportó el arresto de Jorge Maximiliano "Pacho" Viola, uno de los mayores cibercriminales a nivel internacional, quien tenía bajo su poder, más de 8.000 tarjetas de crédito clonadas" [20].

- ✓ En Colombia, se presentó una caída en 2012 con respecto a 2011 de la manifestación de delitos cibernéticos. [20].

E. Directrices Generales

"Según el documento CONPES 3701, el cual busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país" [19], el Ministerio de Tecnologías de la Información y Comunicaciones, a través del Plan Vive Digital, plantea los siguientes vectores con miras a la innovación frente a los servicios al ciudadano:

- ✓ "Directrices estratégicas de Ciberseguridad y ciberdefensa.

- ✓ Gestión integrada de riesgos.
- ✓ Gestión integrada de incidentes.
- ✓ Educación, formación y divulgación en ciberseguridad.
- ✓ Desarrollo de aplicaciones y ambientes móviles.
- ✓ Identificación (unificar los mecanismos de identificación de la ciudadanía colombiana).
- ✓ Elementos particulares para las entidades de inteligencia y defensa nacional" [19].

F. Actualmente que estamos haciendo

Nuestro país pretende iniciar un nuevo programa de ciberdefensa y seguridad digital, por ello: "El presidente de la República ya tiene en su despacho un documento general de diagnóstico y recomendaciones en ciberseguridad y ciberdefensa que nació de la discusión entre grupos de expertos del sector privado coordinados por una comisión especial conformada por los ministerios de Justicia, Defensa y TIC, que el mismo primer mandatario ordenó a comienzos de febrero de este año ante el escándalo de las 'chuzadas digitales' del grupo 'Andrómeda"... [21].

Estas recomendaciones fueron analizadas por expertos de 10 países, quienes encontraron lo siguiente:

¿Qué encontraron los expertos?

- ✓ "Lo primero que encontraron los expertos al analizar los planes en materia de ciberdefensa y seguridad digital en Colombia es que somos un país "líder en experiencia para proteger infraestructura informática y un ejemplo para otras naciones", según dijo al diario El Espectador el secretario ejecutivo de la OEA, Neil Klopfenstein.

- ✓ "Las acciones y grupos de trabajo de las unidades de seguridad e investigación informática y forense de la Policía y las Fuerzas Armadas están en un alto nivel", según el Ministro de las TIC, Diego Molano Vega.

- ✓ Desde el 2011 Colombia cuenta con una política de ciberseguridad y ciberdefensa detallada en el CONPES 3701, la cual creó cuatro organizaciones para la protección interna y externa del país en el ámbito digital.

- ✓ Por ello para Molano "el deber de la seguridad digital es de todos los colombianos, del sector privado, sincronizados con el Estado" [21].

- ✓ "Según mediciones del Centro de Cibercrimen de Microsoft, en los Estados Unidos, así como de empresas como Symantec, McAfee y Eset, Colombia es un país que ya muestra altos índices de criminalidad digital.

- ✓ Robos de identidad digital con fines extorsivos; de recursos de entidades, empresas y personas; ataques dirigidos contra oficinas del Estado y compañías financieras; 'secuestro' de equipos e información pública y privada, son algunas de las modalidades que más crecen en Colombia" [21].

¿Qué tendrá el nuevo programa?

- ✓ "Dos sistemas. Colombia tendría un sistema de seguridad externa (ciberdefensa) y otro de políticas internas (ciberseguridad). Ambos con coordinación unificada y con enlace directo a Presidencia.

- ✓ Refuerzo de personal. El pie de fuerza en seguridad digital crecerá. Se destinarán más recursos a los comandos y grupos de investigación de defensa y seguridad digitales.

- ✓ Más tecnología. Según el ministro, representado por Molano el país cuenta con tecnología de punta para la lucha contra el cibercrimen. En éste aspecto se aumentará el presupuesto y el trabajo con expertos privados.

- ✓ Leyes fuertes. Judicializar a tiempo y de manera efectiva a los delincuentes digitales será punto clave. El marco legislativo actual requiere de revisión y endurecimiento.

- ✓ ¿Y la inteligencia?, Las entidades que controlan y vigilan la seguridad y la defensa nacionales en el campo digital estarán mejor 'armadas' a la

hora de recabar información y datos que permitan evitar riesgos para la Nación.

- ✓ Promulgación. Aún no se conocen los detalles exactos del nuevo plan de ciberdefensa y ciberseguridad que anunciará, con sus respectivas Decretos, el Presidente Santos" [21].

III. CONCLUSIONES

Colombia es víctima de ataques cibernéticos, aunque muchas entidades del estado, públicas y privadas, no sean consciente de ello.

La falta de consciencia, cultura en seguridad informática y conocimiento hace que Colombia ocupe uno de los primeros puestos en el área de inseguridad informática. Es necesario contrarrestar cada uno de los anteriores aspectos y reforzar la parte legal para penalizar los delitos informáticos.

Colombia ya ha empezado el camino a la seguridad informática pero aún está lejos de alcanzar un buen nivel. Pues sí países como Estados Unidos sufren ataques que generan daños sin importar sí tienen una organización bien capacitada encargada de responder a estos incidentes no es descabellado pensar que Colombia sufra ataques que ni son detectados y mucho menos contrarrestados.

La amenaza crece día a día de una forma exponencial y es por ello que el esfuerzo en seguridad debe crecer de forma rápida. Para ellos todos los sectores deben estar integrados y en éste caso liderados por el Gobierno Nacional.

Colombia con la activación del colCERT, ha logrado avances significativos a nivel regional, a pesar de la poca madurez que tenemos en el área de la seguridad y ciberdefensa en nuestra nación.

Con la creación de la Ley 1712 de 2014, "*por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones*", se evidencia que nuestro país quiere seguir madurando en el tema de la seguridad informática.

Con la Política Nacional de Ciberseguridad y Ciberdefensa, Colombia busca fortalecer sus capacidades de respuesta ante incidentes cibernéticos, con el fin de estar a la vanguardia de las nuevas tendencias del cibercrimen.

REFERENCIAS

[1] VÍCTOR MONTERO, Director Ejecutivo De Operaciones de la Consultora Argentina Onapsis (www.onapsis.com).

[2] COLOMBIA. CONGRESO DE LA REPÚBLICA, Ley 527 de 1999 - Comercio Electrónico

[3] COLOMBIA. CONGRESO DE LA REPÚBLICA, Ley 599 DE 2000, Por la cual se expide el Codigo Penal.

[4] COLOMBIA. CONGRESO DE LA REPÚBLICA, Ley 962 de 2005.

[5] COLOMBIA. CONGRESO DE LA REPÚBLICA, Ley 1150 de 2007.

[6] COLOMBIA. CONGRESO DE LA REPÚBLICA, Ley 1266 de 2008.

[7] COLOMBIA. CONGRESO DE LA REPÚBLICA, Ley 1273 de 2009.

[8] COLOMBIA. CONGRESO DE LA REPÚBLICA, Ley 1341 de 2009.

[9] COLOMBIA. CONGRESO DE LA REPÚBLICA, Ley 1581 de 2012.

[10] COLOMBIA. CONGRESO DE LA REPÚBLICA, Ley 1712 de 2014.

[11] COLOMBIA, MINISTERIO DE TECNOLOGÍAS DE LAS COMUNICACIONES, Decreto 032 de 2013.

[12] COLOMBIA, MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO, Decreto 2364 de 2012.

[13] RESOLUCIÓN DE LA COMISIÓN DE REGULACIÓN DE COMUNICACIONES 2258 de 2009.

[14] SUPERINTENDENCIA FINANCIERA DE COLOMBIA, Circular 052 de 2007.

[15] REPÚBLICA DE COLOMBIA, Departamento Nacional de Planeación, Consejo Nacional de Política Económica y Social – CONPES 3701, Bogotá 14 de Julio de 2011.

[16]. MINISTERIO DE DEFENSA NACIONAL, Dirección de Estudios Sectoriales, Dirección de Programas, Nota de investigación 03, Octubre 2009.

[17] MINISTERIO DE DEFENSA NACIONAL, Logros de Colombia en Ciberseguridad y Ciberdefensa, Bogotá Enero de 2012.

[18] GRUPO DE RESPUESTA A EMERGENCIAS CIBERNÉTICAS DE COLOMBIA – colCERT, http://www.colcert.gov.co/

[19] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, Agenda Estratégica de Innovación: Ciberseguridad, Bogotá, Julio de 2012.

[20] GRUPO DE RESPUESTA A EMERGENCIAS CIBERNÉTICAS DE COLOMBIA – colCERT, "Colombia, líder en Latinoamérica a través de su Política Nacional en Ciberseguridad y Ciberdefensa", http://www.colcert.gov.co/, 03 de Mayo de 2013.

[21] ARCHIVO EL TIEMPO – Sección Ciencia y Tecnología: El 'Plan Colombia' para la ciberseguridad, "http://www.eltiempo.com/archivo/documento/CMS-3797815, 07 de Abril de 2014.

[22] ISO/IEC, "International Standard ISO/IEC 27005", 2008.

Yolanda Quintero Agudelo, Ingeniera de Sistemas Escuela Colombiana de Carreras Industriales, estudiante de la "Especialización en Seguridad de la Información" Universidad Piloto de Colombia 2014.