Lineamientos, Tendencias y Estrategias sobre Ciberseguridad y Ciberdefensa en Colombia

Alirio Mayorga Delgado
almade87@gmail.com
Universidad Piloto de Colombia

Resumen—En un mundo globalizado como el de hoy, las relaciones sociales, económicas, políticas y culturales dependen cada vez más, de las tecnologías e infraestructuras de la información y las comunicaciones (ciberespacio), que por su característica transversal se han convertido en el principal vehículo de la sociedad, lo que ha obligado a la articulación de un sistema en el ámbito nacional en lo que concierne a seguridad y defensa (ciberseguridad y ciberdefensa), que fortalezca al estado colombiano en su capacidad de gestionar los riesgos que amenazan su funcionamiento, así como en el establecimiento de mecanismos que permitan gestionar el uso adecuado de las tecnologías de la información y las comunicaciones como activo más importante de la sociedad moderna.

Abstract—In a globalized world of today, social, economic, political and cultural relations are increasingly dependent on the technologies and infrastructures of information and communication (cyberspace) which cross-feature have become the main vehicle of the company, which has forced the articulation of a system at the national level regarding security and defense (cybersecurity and cyberdefense), to strengthen the Colombian state in its ability to manage risks that threat its operation as well as the establishment of mechanisms to manage the proper use of information and communications technology as the most important asset of modern society.

Índice de Términos—Ciberespacio, Ciberseguridad, Ciberdefensa, Infraestructura crítica, Seguridad de la información, colCERT.

I. INTRODUCCIÓN

Con el creciente aumento en el uso de las tecnologías de la información y las comunicaciones en Colombia y en general en todo el mundo, el ciberespacio se ha convertido en un espacio ideal para realizar ataques organizados que pueden originarse desde cualquier lugar del territorio nacional o de otros paises contra las redes civiles y militares, los servicios, las infraestructuras críticas (la energía, el suministro de agua, el transporte, el sistema financiero, las telecomunicaciones, etc), entre otros. Sabiendo que para ello, solamente es necesario disponer de tecnología y de los conocimientos necesarios para llevarlos a cabo. De esta manera, dejar sin comunicación, electricidad o transporte a una región entera, o penetrar redes informáticas ilegalmente e introducir virus capaces de infectar miles de computadoras, sin el riesgo de ser descubiertos y mucho menos detenidos.

De ahí, que Colombia ha establecido una política en ciberseguridad y ciberdefensa, la cual tiene como base el documento conpes 3701 de julio 14 de 2011, orientada a la adopción de medidas y controles que permitan proteger al estado ante estas nuevas amenazas informáticas, política que compromete diversas entidades que trabajan para garantizar la seguridad de la información a nivel nacional. La política establecida contempla como objetivo central, el fortalecimiento de la capacidad del estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético. Con el propósito de entender y ahondar en el tema es importante conocer la definición de los términos:

Ciberseguridad. Es la capacidad que tiene un Estado de minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberdefensa. Es la capacidad que tiene un Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte su soberanía. [1].

Ciberespacio. Es un espacio tanto físico como virtual que contiene todos los recursos de información y comunicación disponibles en la red, que permiten la interacción entre sí de los usuarios a través de las nuevas tecnologías. El internet es el mayor ámbito del ciberespacio en donde las barreras físicas desaparecen.

Infraestructura Crítica. Conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, la salud pública, o la combinación de ellas, en una nación.

colCERT. Grupo de Respuesta a Emergencias Cibernéticas de Colombia [1].

En el ámbito internacional, los Estados conscientes de los problemas que traen consigo el avance de la tecnología y las comunicaciones, están prestando más atención a sus sistemas de ciberseguridad y ciberdefensa. Aunque también es cierto, que aún son muchos los países que no han analizado las consecuencias potenciales de un posible ataque cibernético, y ni si quiera se están preparando para ello.

II. LINEAMIENTOS SOBRE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA

Desde la expedición de la Ley 527 en 1999, Ley de comercio electrónico, Colombia empezó a darse cuenta que la revolución de la informática y de las comunicaciones tendrían un impacto fuerte con el paso de los años, que transformaría social, política y económicamente la vida de todos los nacionales, y con el ánimo de ponerse a la par de países desarrollados en esta materia, en el año 2009 expide la Ley 1273 y 1341, que crean la protección de la información y de los datos, como un bien jurídico tutélable, y se organizan las tecnologías de la información y las comunicaciones–TIC, además de la creación de la Agencia Nacional del Espectro.

Es mediante la modificación del código penal (Ley 1273 de 2009, [2].), que se establece una tipificación de delitos que protegen los datos y los sistemas informáticos de atentados contra la confidencialidad, la integridad y la disponibilidad como pilares de la seguridad de la información, así como atentados informáticos y otras infracciones. Los delitos establecidos en la norma y que actualmente se aplican a quienes incurran en ello son:

1. Acceso abusivo a un sistema informático.
2. Obstaculización ilegítima de sistema informático o red de telecomunicación.
3. Interceptación de datos informáticos.
4. Daño informático.
5. Uso de software malicioso.
6. Violación de datos personales.
7. Suplantación de sitios web para capturar datos Personales.
8. Hurto por medios informáticos y semejantes.
9. Transferencia no consentida de activos. [2].

Colombia en 2011 se dio cuenta que tenia muchas debilidades en el uso del ciberespacio, con lo que se podría poner en riesgo la seguridad de los ciudadanos y la propia seguridad nacional, esto motivo a tomar algunas recomendaciones hechas por entidades como: la Organización de Estados Americanos – OEA, la comisión de Regulación de Telecomunicaciones, la Cámara Colombiana de Informática y Telecomunicaciones, entre otros, y como estrategia expidió unos lineamientos de política para Ciberseguridad y Ciberdefensa que pudiera dar respuesta a los incidentes y delitos cibernéticos que afectarían a la nación y a la estabilidad del estado Colombiano; política que finalmente lidero Ministerio de Defensa Nacional y quedo en cabeza del mismo, de acuerdo con el documento conpes 3701 de 2011. [1].

Esta política lo que busca es una coordinación interinstitucional entre diferentes ministerios y organizaciones del sector privado para poder hacer frente a las amenazas cibernéticas que puedan en determinado momento debilitar la infraestructura critica del país, a partir de ello se crea la comisión intersectorial que permite reaccionar ante cualquier circunstancia que pueda poner en peligro la seguridad nacional a través del ciberespacio. Lo que se busca es prevenir y controlar el incremento de las amenazas informáticas que crecen de manera exponencial con el desarrollo imparable de las tecnologías de la información y de las comunicaciones. Esta comisión es responsable de fijar la visión estratégica para la gestión de la información en todos sus frentes, así como la gestión de la infraestructura tecnológica. [1].

Fig. 1. Modelo de Coordinación de la política para ciberseguridad y ciberdefensa de Colombia.
Fuente: Documento Conpes 3701

Como parte de la política, se crea el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT como organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa, el cual presta su apoyo y colaboración a las demás instancias nacionales tales como el Centro Cibernético Policial - CCP y el Comando Conjunto Cibernético – CCOC. La misión y objetivo central del colCERT es 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. [1].

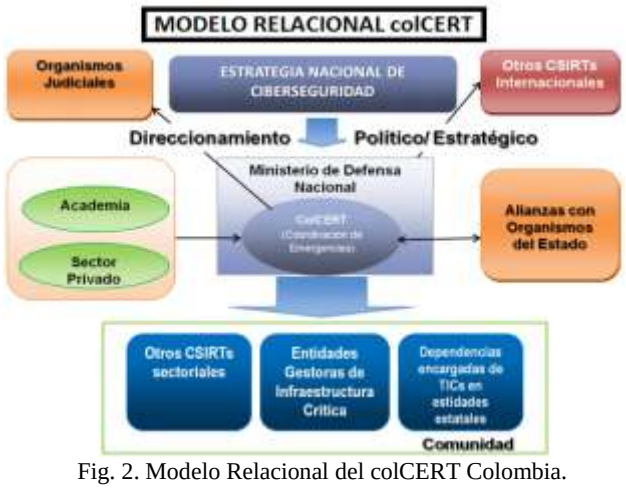

Fig. 2. Modelo Relacional del colCERT Colombia.
Fuente: Documento Conpes 3701

Además de las dos instancias anteriormente descritas, se establece el Centro Cibernético Policial - CCP., el cual está encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos. Desarrolla labores de prevención, atención,

investigación y judicialización de los delitos informáticos en el país, despliega información en su página web sobre vulnerabilidades cibernéticas. Además recibe y atiende los lineamientos nacionales en ciberseguridad y trabaja de forma coordinada con el colCERT. [1].

Fig. 3. Centro Cibernético Policial Colombia
Fuente: Antecedentes de la política de ciberseguridad y ciberdefensa - Ministerio de Defensa Nacional

Colombia con la adopción de la política para ciberseguridad y ciberdefensa y la inclusión de la misma en el plan de desarrollo 2010-2014, lo que buscó fue fortalecer la capacidad del estado para enfrentar las manazas que atentan contra su seguridad y defensa en el ámbito cibernético, la cual depende de las tres instancias mencionadas y de un cuarto organismo denominado equipo encargado de la defensa del país en el ciberespacio, o "Comando conjunto cibernético".

Como lo contempla el documento conpes 3701, cada una de estas instancias se proponen fijar estrategias que permitan contrarrestar las amenazas que enfrenta el país en el ámbito de la protección de la información y de la infraestructura critica que lo conforma, estas estrategias si no se llevan acabo siguiendo estándares internacionales pueden ocasionar que el país entre en un verdadero colapso en determinado momento, cuando los delincuentes del ciberespacio se den cuenta de las debilidades que todavía se tienen en materia de seguridad al usar los medios electrónicos y las redes de comunicación.

Es importante tener presente que en la actualidad y hacia futuro, el ciberespacio ha pasado y seguirá siendo otro frente de guerra que tienen que defender los Estados, en el que se libran todo tipo de batallas desde el punto de vista de las tecnologías de la información y las comunicaciones, en el que los atacantes son cuantiosos, sofisticados y en la mayoría de los casos anónimos; para nadie es un secreto que los delincuentes cuentan con tecnología informática y sistemas de comunicación de avanzada muchas veces desconocidos por los estados blanco de estos ataques. Es por esto que el consenso internacional sitúa a los Equipos de Respuesta a Incidentes telemáticos (CERTs) como una de las principales herramientas para hacer frente a este tipo de amenazas. Sus servicios, contribuyen sin lugar a dudas a proteger el funcionamiento normal de un país, la información almacenada en todos sus sistemas y la defensa y seguridad nacional.

Hoy en día, Colombia al igual que la mayor parte de los países ha decidido adecuar su "Seguridad Nacional" a los nuevos tiempos, incluyendo un nuevo espacio a defender, con unas fronteras poco intangibles, y con un enemigo en constante evolución y perfeccionamiento: el ciberespacio.

Precisamente, la defensa de la Nación, que tradicionalmente ha estado soportada por las Fuerzas Militares y de Policía, la Armada y la Fuerza Aérea Colombiana, está siendo "repensada" ante este nuevo escenario en el que, la información se ha convertido en un arma estratégica de primer orden, cuyo manejo puede poner en cuestión la gobernabilidad del país. Por ello, la ciberdefensa es un factor clave dentro de cualquier Estrategia Nacional de Defensa que se precie.

Así lo han entendido buena parte de los gobiernos y así lo recomiendan organizaciones internacionales expertas en la materia, como la Unión Internacional de Telecomunicaciones (UIT), la Agencia Europea de Seguridad de las Redes y la Información (ENISA), y la Organización de Estados Americanos (OEA). La UIT, por ejemplo, señala que "*un buen programa de ciberseguridad nacional contribuirá a proteger el funcionamiento normal de la economía de un país, a promover la continuidad de la planificación en todos los sectores, proteger la información almacenada en los sistemas de información, preservar la confianza pública, mantener la seguridad nacional y garantizar la salud y la seguridad públicas*". [3].

Además de o anterior, es importante resaltar que en materia de ciberseguridad y ciberdefensa, Colombia no se quedó solo con lo contemplado en el documento conpes 3701 de 2011, sino que en el año 2012 expidió la Ley estatutaria 1581, una nueva normativa para proteger todo lo relacionado con los datos personales y el tratamiento de estos, efectuados en el territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. [7]. Si bien es cierto que cualquier entidad pública o privada captura en sus bases de datos información íntimamente relacionada con las personas , estas últimas con la expedición de la Ley antes citada por derecho constitucional, pueden conocer, actualizar y rectificar los datos que se hayan recogido y almacenado en las bases de datos.

En junio de 2013 se expide el Decreto 1377, que reglamenta la Ley 1581 de 2012, el cual contempla que toda persona titular de la información es el único que puede autorizar la captura y el tratamiento de sus datos personales, así mismo el Decreto contempló las políticas de tratamiento por parte de los responsables y encargados del manejo de la información. [7].

Todo lo anterior enmarca el trasegar estratégico interno y normativo que Colombia ha venido implementando en materia de política cibernética para hacer frente a conductas ilícitas que ponen en riesgo la seguridad de la información y la seguridad y estabilidad de la infraestructura crítica del país.

III. COLOMBIA Y LA COOPERACIÓN INTERNACIONAL EN LOS DELITOS INFORMÁTICOS Y EL CIBERESPACIO

El primer paso en la lucha contra los delitos cibernéticos es la cooperación internacional, en esta materia, Colombia hace parte de los tratados de asistencia mutua, con el fin de participar de manera cooperativa en asuntos de delitos transnacionales y en investigaciones criminales globales. Colombia firmo el Acuerdo por la ciberptotección durante el foro económico mundial para ciberptotección realizado en china en el año 2012, el cual agrupa varios sectores de la industria y trabaja múltiples iniciativas para mejorar la ciberseguridad desde distintos aspectos; en este mismo sentido trascendió que a finales de septiembre del año 2013, Colombia fue invitada por el Consejo de Europa a adherirse a la convención sobre delito cibernético o Convención de Budapest, como se le conoce a nivel global, lo cual complementará su política y avances técnicos con un conjunto robusto de legislación sobre delincuencia cibernética. [4].

El Convenio de Budapest se presenta como una solución internacional existente para atacar los delitos informáticos y/o electrónicos, y a pesar de sus deficiencias, se convierte en una adecuada herramienta para la armonización legislativa internacional y su lucha contra el ciberdelito. Este Convenio es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional), así mismo es el único a nivel internacional que se encarga de la seguridad de la información y trata los delitos contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y los sistemas informáticos.

Colombia también ha establecido lasos estrechos con el comando sur de los Estados unidos, a través del cual se han impartido capacitaciones sobre conocimiento e identificación de las nuevas amenazas latentes en el ciberespacio, capacitaciones impartidas a comandantes de la fuerza pública y altos directivos del gobierno que se desempeñan en cargos estratégicos de seguridad nacional; Así mismo mantiene estrecha cooperación con la INTERPOL en la lucha contra el delito cibernético.

Aunque Colombia ha avanzado en políticas de ciberseguridad y ciberdefensa, en como contrarrestar y penalizar los delitos informáticos y en normas sobre la protección a los datos personales; es impensable precisar que todo está contralado, hace falta dar pasos muy importantes en temas como la prevención, la sensibilización, la capacitación del personal del sector judicial y la puesta en marcha de técnicas más sofisticadas de recolección de evidencia digital, falencias que seguramente Colombia superará con su adhesión al convenio de Budapest y con la puesta en marcha de la agenda estratégica de innovación sobre el tema impulsada por el Ministerio de tecnologías de la Información y las Comunicaciones. [6].

IV. LINEAMIENTOS SOBRE CIBERSEGURIDAD Y CIBERDEFENSA EN PAISES DE AMERICA LATINA Y EL CARIBE

Para Colombia y para cualquier país, es importante conocer las políticas que sobre el tema se estén implementando a nivel global y regional, ya que esto ayuda a consolidar estrategias conjuntas de lucha contra la ciberdelincuencia. Es por esto que nace la necesidad de conocer y analizar lo que hasta ahora se implementado en algunos países de América latina y el Caribe.

Brasil: Es uno de los países de América Latina que más ha avanzado en el desarrollo de capacidades para contrarrestar la amenaza cibernética. En Brasil la Policía Federal (DPF) es la principal autoridad en materia de delitos cibernéticos a través de su Servicio de Represión de Delitos Cibernéticos (SRCC), aunque también cuenta con un segundo grupo que se encarga de tareas especializadas en la lucha contra los delitos relacionados con la pornografía infantil en Internet, el GECOP. En el plano cibernético Brasil según los estudios representa el 7 mercado online del planeta, lo que hace a este país bastante atractivo para los ciberdelincuentes. [5].

Analizando al ciberespacio como un entorno estratégico para el desarrollo del país, el Gobierno brasileño en el año 2010 aprobó la creación en Brasilia del Centro de Defensa Cibernética del Ejército (CDCiber) así mismo cuenta con un Departamento de Seguridad de la Información y las Comunicaciones (DSIC), el cual hace parte de la oficina de la presidencia.

Argentina: El organismo líder a cargo de la seguridad cibernética en Argentina es el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) que forma parte de la Oficina Nacional de Tecnología de Información (ONTI), a esta Oficina se le asigno en 2011 el Equipo de Respuesta ante Emergencias Informáticas (CERT), el cual había sido fundado en 1994, que hizo de Argentina uno de los primeros países en América Latina en operar un CSIRT nacional. La División de Crímenes Tecnológicos de la Policía federal Argentina (PFA), es la unidad responsable de las investigaciones referentes a delitos cibernéticos. [5].

Ecuador: En este país suramericano todavía no se estableció un CSIRT nacional, ha venido trabajando en el establecimiento del mismo con el nombre tentativo de EcuCERT. En Ecuador la responsabilidad principal en la investigación de la ciberdelincuencia y de las actividades criminales que involucren TIC, recae en la Unidad de Investigación del Delito Cibernético de la Policía Judicial, que depende de la Policía Nacional. En algunos casos, la Unidad de Investigaciones Cibernéticas de la Procuraduría General del Estado se involucra en las investigaciones.

Jamaica: El Ministerio de Ciencias, Tecnología, Energía y Minería (MSTEM) es el principal organismo que trata los asuntos relacionados con la seguridad cibernética. En 2012, Jamaica revisó su legislación sobre delincuencia cibernética y amplió la capacidad de la Unidad de Comunicación Forense y Delincuencia Cibernética (CFCU) de la policía y avanzó en el

establecimiento formal de un CSIRT. En la actualidad Jamaica ha establecido un Equipo de Trabajo Nacional de Seguridad cibernética (NCSTF), encargado de establecer un marco que ayude a generar confianza en el uso del ciberespacio. [5].

Panamá: En este país, la institución responsable de la supervisión y la dirección de asuntos relativos a la seguridad cibernética es la Autoridad Nacional para la Innovación Gubernamental (AIG), que funciona a través del Centro de Respuesta a Incidentes de Seguridad Cibernética (CSIRC) de Panamá. En marzo de 2013, Panamá adoptó oficialmente su Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas (ENSC+IC), con lo que se unió a Colombia como el único país latinoamericano con un plan integral de seguridad cibernética. [5].

México: según las estadísticas, México ocupa el último lugar en materia de ciberseguridad entre los países que conforman la OCDE, va rezagado en la tipificación de delitos informáticos y no cuenta con recursos humanos especializados. México está bastante atrasado en la adopción de estrategias de seguridad en comparación con el resto del mundo; Se tiene poca conciencia sobre este tema, tanto del lado del gobierno como por parte de la alta dirección de las empresas, lo que hace que falte inversión en tecnología de seguridad para poder hacer frente a las amenazas cibernéticas que existen y que van creciendo. [8].

En México, la Policía Federal es la principal autoridad operacional en lo que respecta a iniciativas sobre seguridad y el delito cibernético, dentro de la Policía Federal, la División Científica mantiene una unidad responsable de coordinar actividades para investigar, prevenir y procesar toda conducta considerada delictiva que utiliza medios electrónicos y cibernéticos. [5].

V. TENDENCIAS DE LA DELINCUENCIA CIBERNÉTICA EN COLOMBIA

Según el informe presentado en el mes de junio de 2014 por la Organización de Estados Americanos - OEA y la empresa Symantec sobre tendencias de seguridad Cibernética en América latina y el Caribe, Colombia de acuerdo con lo reportado en el año 2013, alcanzo altos costos en cuanto a delitos cibernéticos cometidos, los cuales alcanzaron unos USD 462 millones, siendo los ataques dirigidos (ataques de phishing), el uso de código malicioso y el robo de información las principales causas de estos delitos.

Colombia registró en el 2013, un aumento de los incidentes cibernéticos cometidos con relación al año 2012 y 2011. Lo anterior se explica un poco por el mayor acceso de los ciudadanos a las nuevas tecnologías de la información y a la expansión del dominio cibernético, además según los reportes de las autoridades, se observa un incremento paralelo y sistemático de la transición de las actividades delictivas del mundo físico al mundo virtual; Este fenómeno fue sumamente evidente en el ámbito del fraude electrónico, que afectó considerablemente a usuarios y entidades del sistema bancario colombiano.

De acuerdo con el informe presentado por la Organización de Estados Americanos - OEA, y la empresa Symantec en 2014, la tendencia creciente de los incidentes que se reportan involucran el uso de keyloggers (registradores de teclas), spyware y otros programas maliciosos semejantes. La misma dinámica se vio reflejada en el campo de la suplantación de identidad, donde los autores del hecho se inclinan a delitos cada vez más sofisticados, como ransomware (secuestro informático) y el uso del programa malicioso Cryptolocker, para atacar a la comunidad de pequeñas y medianas empresas (PyME), así como a empresas más grandes. [5].

Según datos detallados en el informe, entregados por la Policía Nacional, en 2013 hubo 16.789 páginas web bloqueadas por pornografía infantil; se registraron 2.652 nuevas alertas de amenazas cibernéticas; 422 personas detenidas por delitos cibernéticos y se recibieron un total de 4.290 reclamos en relación con incidentes asociados a las TIC, lo cual representa un aumento en las quejas respecto del año 2012. Además en 2013, el Centro Cibernético de la Policía respondió a 1.647 ataques o incidentes cibernéticos, de los cuales el 62% involucró a ciudadanos particulares y el 21%, a entidades del sector bancario. El resto de los incidentes involucró a una combinación casi igual de entidades pertenecientes a los sectores de gobierno, fuerzas de seguridad, comunicaciones, energía, salud y educación. [5].

Además de lo anterior y por información consolidada por la Dirección de Estudios Estratégicos del Ministerio de Defensa Nacional, la estadística de los delitos informáticos cometidos en Colombia desde el 01 de enero de 2009 al 31 de agosto de 2014, se detalla de acuerdo con la tipificación de delitos contemplados en la Ley 1273 de 2009 según la siguiente tabla:

POR CONDUCTA DELICTIVA	2009	2010	2011	2012	2013	2014
Artículo 269A. Acceso abusivo a un sistema informático	6	3	1		8	4
Artículo 269C. Interceptación de datos informáticos		1	1	1	1	
Artículo 269F. Violación de datos personales	1	1				
Artículo 269G. Suplantación de sitios web para capturar datos personales	1					
Artículo 269I. Hurto por medios informáticos y semejantes	212	401	841	2343	3448	1830
Artículo 269J. Transferencia no consentida de activos	7	1		1	206	104
Total general	**227**	**407**	**843**	**2345**	**3663**	**1938**

Tabla 1. Registro de delitos informáticos
Fuente: Observatorio del delito-DIJIN-Policía Nacional

En Colombia las principales tendencias para la ocurrencia de los delitos cibernéticos cometidos, se dan principalmente, por los bajos niveles de conciencia de los usuarios hacia la seguridad cibernética, por una débil cultura de la seguridad, y como tercera tendencia sigue siendo el uso creciente de internet, las redes sociales y el uso del correo electrónico, lo

cual ha precipitado hábitos de navegación inseguros y provocado la defraudación de usuarios de la internet que se muestran vulnerables ante delincuentes comunes y del crimen organizado que utilizan el ciberespacio para llevar a cabo estos hechos ilícitos.

Además, la insuficiente capacitación que brinda la policía sobre ataques avanzados o especializados, las dificultades para preservar y examinar evidencias digitales y la falta de cooperación de los proveedores de servicios de internet y otras organizaciones privadas constituyen impedimentos importantes para poner freno a la delincuencia cibernética en Colombia. [5].

En cuanto al aumento creciente de las actividades ilícitas en el mundo cibernético en Colombia y contemplando lo reportado a la Organización de Estados Americanos - OEA, por las autoridades competentes, el principal impedimento para aumentar la seguridad cibernética del País, ha sido y sigue siendo la ausencia de una cultura de la información y la seguridad cibernética entre los ciudadanos usuarios y las empresas. También se destaca la falta de políticas de uso de las TIC con soporte en Internet y su capacidad limitada para actuar en este ámbito, puesto que las sedes de la mayoría de los proveedores y operadores de servicios de Internet se encuentran fuera del territorio nacional y las relaciones de cooperación son limitadas. [5]

VI. COLOMBIA Y EL NUEVO PLAN ESTRATÉGICO PARA FORTALECER LA CIBERSEGURIDAD Y CIBERDEFENSA EN LOS PRÓXIMOS AÑOS

Teniendo en cuenta el despliegue tecnológico que vive el país y en general el mundo entero, y consientes de las nuevas amenazas y riesgos que se deben enfrentar en el escenario digital, el País en la actualidad construye el denominado Plan Vive Digital 2014 – 2018 liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC; plan que tendrá como principio promover el desarrollo del sector privado para expandir infraestructura y ofrecer servicios, además de incentivar de forma integral la oferta y la demanda de servicios digitales, lo cual requiere del estado priorizar recursos para inversiones de capital.

Aunque Colombia según expertos mundiales, es líder en protección de infraestructuras informáticas, también es cierto que presenta altos índices de criminalidad digital que afecta tanto a entidades públicas como a las privadas, poniendo en riesgo la defensa y protección de los activos informáticos lo cual conlleva un alto reto en cuanto a ciberseguridad y ciberdefensa se refiere.

Por lo anterior, el Gobierno Nacional con la participación activa del Ministerio de la Defensa, el de Justicia, la Cancillería y el de las TIC, entre otros, prepara lo que será la nueva estructura que tendrá, tanto en el alto Gobierno como a nivel nacional y regional, el nuevo plan de ciberseguridad y ciberdefensa, con el cual se pretende formalizar una Comisión Digital, que dependerá directamente del Presidente de la República y de la Agencia Nacional de Seguridad Cibernética que igualmente se pretende crear. [9].

Los dos nuevos entes que posiblemente se creen, serán los encargados de acopiar todos los esfuerzos públicos, privados, regulatorios, de relacionamiento internacional y de creación de políticas de ciberseguridad y ciberdefensa del país, así como para fortalecer a las oficinas de seguridad digital de las fuerzas militares y de Policía; También, para acordar convenios internacionales y articular al empresariado, la academia y la ciudadanía en torno a una política pública única sobre seguridad digital.

Se ha filtrado que con el nuevo plan, en apoyo con el sector privado y las universidades, se formaran centros de innovación y excelencia, que harán investigación y desarrollo de herramientas para mejorar la ciberseguridad o atender casos de ciberdefensa.

De acuerdo con lo que se ha dado a conocer en los medios de comunicación y que será anunciado por el presidente de la republica posiblemente antes de finalizar el año 2014, el nuevo plan sobre ciberseguridad y ciberdefensa tendría como puntos importantes los siguientes: [9].

1. Colombia tendría un sistema de seguridad externa (ciberdefensa) y otro de políticas internas (ciberseguridad). Ambos con coordinación unificada y con enlace directo a Presidencia.
2. El pie de fuerza en seguridad digital crecerá. Se destinarán más recursos a los comandos y grupos de investigación de defensa y seguridad digitales.
3. Según el ministro de Tecnologías de la Información y las Comunicaciones el país cuenta con tecnología de punta para la lucha contra el cibercrimen. En este aspecto se aumentará el presupuesto y el trabajo con expertos privados.
4. Judicializar a tiempo y de manera efectiva a los delincuentes digitales será punto clave. El marco legislativo actual requiere de revisión y endurecimiento.
5. Las entidades que controlan y vigilan la seguridad y la defensa nacional en el campo digital estarán mejor ‘armadas’ a la hora de recabar información y datos que permitan evitar riesgos para la Nación.

VII. CONCLUSIONES

1. La ciberseguridad se está convirtiendo poco a poco en un elemento esencial de la seguridad en Colombia así como internacionalmente. El riesgo de estar en un mundo sumamente hiperconectado, y ante las posibles consecuencias de ataques a nivel cibernético, está conduciendo a establecer buenas políticas de seguridad en el ciberespacio.

2. Es necesario ahondar en la concientización de todos los nacionales sobre los hábitos cibernéticos y la sensibilidad general hacia la seguridad de la información, lo cual dificultará que los ciberdelincuentes puedan perpetuar fácilmente ataques. La sensibilización se proyecta como una de las estrategias más económicas y eficaces de minimizar los riesgos

a la seguridad cibernética y cerrar brechas de seguridad que siguen estando totalmente abiertas.

3. Todo Estado debe construir un marco normativo que regule la seguridad en el ciberespacio y Colombia no es la excepción, en el que intervengan todas las partes (entidades y ciudadanos), siguiendo estándares acordes con las regulaciones a nivel internacional. Lo más importante trabajar en forma conjunta y no hacer una guerra por cuenta propia en contra de los delincuentes cibernéticos.

4. El ciberespacio nunca estará seguro al cien por ciento aunque se implementen estrategias de seguridad, esto se puede ver reflejado en el ámbito Colombiano a pesar de estar en marcha la política contemplada en el documento conpes 3701 de 2011, continúa manteniéndose una alta tendencia de delitos informáticos con el trascurrir de los años.

REFERENCIAS

[1] Documento Conpes 3701. Lineamiento de politica para ciberseguridad y ciberdefensa, Julio 2011.
[2] Ley 1273. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "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, entre otras disposiciones. Enero 2009
[3] ITU STUDY GROUP Q.22/1 REPORT ON BEST PRACTICES FOR A NATIONAL APPROACH TO CYBERSECURITY: A MANAGEMENT FRAMEWORK FOR ORGANIZING NATIONAL CYBERSECURITY EFFORTS [Online]. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf.
[4] Consejo de Europa invitó a Colombia a adherir a la Convención sobre Delito Cibernético. [Online]. Available: http://www.cancilleria.gov.co/newsroom/news/consejo-europa-invito-colombia-adherir-la-convencion-sobre-delito-cibernetico.
[5] Tendencias de seguridad cibernética en América Latina y el Caribe. [Online]. Available: http://www.oas.org/es/ssm/cyber/documents/OAS-Symantec_Cyber_Security_Report_SPA.pdf.
[6] AGENDA ESTRATÉGICA DE INNOVACIÓN: CIBERSEGURIDAD Y CIBERDEFENSA. [Online]. Available: http://www.vivedigital.gov.co/idi/wp-content/uploads/2012/08/CS_AEI__Vectores_v_205.pdf
[7] Decreto número 1317. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, junio 2013.
[8] México, 'en pañales' en Ciberseguridad. [Online]. Available:http://www.cnnexpansion.com/tecnologia/2014/05/13/mexico-lejos-del-promedio-en-seguridad
[9] Colombia se prepara para enfrentar los ciberataques. [Online].Available:http://www.eltiempo.com/tecnosfera/novedades-tecnologia/gobierno-prepara-plan-estatal-de-ciberseguridad/14233838

Autor.
Alirio Mayorga Delgado, Ingeniero de Sistemas, Universidad Francisco de Paula Santander. Esp.c. Especialización en Seguridad Informática, Universidad Piloto de Colombia.