Fecha de recepción: 12 de julio de 2015 / Fecha de aprobación: 29 de septiembre de 2015

Revista de Derecho Comunicaciones y Nuevas Tecnologías

Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia

Rodrigo Cortés Borrero

Artículo de reflexión

DOI: http://dx.doi.org/10.15425/redecom.14.2015.06

Universidad de los Andes
Facultad de Derecho
Rev. derecho comun. nuevas tecnol.
No. 14, julio - diciembre de 2015. ISSN 1909-7786

Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia

Resumen

En las últimas décadas, con la materialización de la era digital, el Internet y la sociedad de la información han emergido nuevos desafíos para los Estados y los distintos sectores de la sociedad, que han hecho necesario implementar políticas públicas que permitan hacerles frente. Colombia no es ajena a estos fenómenos y, como tal, el objeto de esta investigación es describir la política pública de ciberseguridad y ciberdefensa implementada en los últimos años, concretamente en los organismos y entidades encargadas de estas funciones y los distintos instrumentos jurídicos que permiten que el país tenga una seguridad cibernética que garantice a los sectores tanto público como privado la salvaguarda de sus derechos, patrimonio e información.

Palabras claves: política pública, ciberseguridad, ciberdefensa, Estado.

The current status of public policy on cyber security and cyber defense in Colombia

Abstract

In recent decades, with the realization of the digital age, the Internet and the information society new challenges have emerged for States and different sectors of society, which have made it necessary to implement public policies to address these challenges. Colombia is no stranger to this phenomenon and, as such, the object of this research is to describe its public policy on cyber defense and cyber security which has been implemented in recent years, particularly in the agencies and entities responsible for these functions and in the various legal instruments that allow the country to have guarantees of cyber security for both the public and private sector to safeguard their rights, property and information.

Keywords: public policy, cyber security, cyber defense, State.

Estado atual da política pública de ciberseguridade e ciberdefesa na Colômbia

Resumo

Nas últimas décadas, com a materialização da era digital, a Internet e a sociedade da informação têm emergido novos desafios para os Estados e os distintos setores da sociedade, sendo necessário implementar políticas públicas que permitam enfrentá-los. A Colômbia não é alheia a estes fenômenos e, como tal, o objeto desta investigação é descrever a política pública de ciberseguridade e ciberdefesa implementada nos últimos anos, concretamente, nos organismos e entidades encarregadas destas funções e os distintos instrumentos jurídicos que permitem que o país tenha uma seguridade cibernética que garanta aos setores tanto público quanto privado a salvaguarda de seus direitos, patrimônio e informação.

Palavras-chave: política pública, ciberseguridade, ciberdefesa, Estado.

Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia*

Rodrigo Cortés Borrero**

Sumario

Introducción – I. PROYECTO DE INVESTIGACIÓN – II. MARCO TEÓRICO – *A Política pública – B. Ciberseguridad – C. Ciberdefensa – D. Ciberespacio – E. Consejo Nacional de Política Económica y Social (Conpes)* – III. METODOLOGÍA – IV. ANTECEDENTES Y DESARROLLO NORMATIVO DE LA POLÍTICA PÚBLICA DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA – V. ORGANISMOS ENCARGADOS DE LA CIBERSEGURIDAD Y LA CIBERDEFENSA EN COLOMBIA – *A. Organismos de orden nacional* – 1. Presidencia de la República – 2. Ministerio de Defensa nacional – 3. Ministerio de Tecnologías de la Información y las Comunicaciones - *B. Organismos especializados* – 1. Comando Conjunto Cibernético de las Fuerzas Militares – 2. Centro Cibernético Policial – 3. Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) – VI. CONCLUSIONES – Referencias.

* Cómo citar este artículo: Cortés Borrero, R. (Diciembre, 2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* 14. Universidad de los Andes (Colombia).

** Abogado *Cum Laude* Universidad Santo Tomás, sede Villavicencio. Especialista en Derecho Administrativo, conciliador en Derecho, estudiante de la Maestría en Derecho Contractual Público y Privado, docente investigador y director del semillero de Derecho Informático y de las Tecnologías en la Sociedad de la Información (DITSI) de la Facultad de Derecho de la misma Institución.

Introducción

El advenimiento en las últimas cuatro décadas del desarrollo de las comunicaciones y de las tecnologías ha presentado un reto para las naciones, pues han surgido nuevas problemáticas en cuanto al uso de estas, representadas en amenazas desde la seguridad nacional hasta la economía del ciudadano de a pie.

Este no es un fenómeno aislado de países subdesarrollados, pues se han evidenciado vulneraciones a la seguridad nacional y a la economía en distintas latitudes del globo, que han forzado la creación y fortalecimiento de políticas públicas en materia de ciberseguridad y ciberdefensa por parte de los distintos gobiernos a nivel mundial.

Un ejemplo de ello:

> En el 2009, luego del ataque a las páginas del Departamento del Tesoro y de Estado, de la Comisión Federal de Gobierno, del Pentágono y de la Casa Blanca, el gobierno de los Estados Unidos creó un Centro de Ciber-Comando Unificado que depende de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), DHS: National Cyber Security Division, US-CERT: United States Computer Emergency Readiness Team y la oficina de Seguridad Cibernética de la Casa Blanca, para hacer posible la defensa de la infraestructura tecnológica del país y llevar a cabo operaciones ofensivas. Según un estudio de la Empresa de Análisis INPUT del 2009, el presupuesto para ciberseguridad de US 7.9 billones de ese año, ha ido incrementando en un 8.1% anual, siendo en el 2010 de US 8.54 billones, que representan el 0,25% del Presupuesto Nacional de los Estados Unidos. (Santiago, 2012).

En nuestro entorno regional tampoco somos ajenos a esta problemática, como lo expone la misma autora:

> En los últimos dos años el aumento en los ataques cibernéticos en Latinoamérica fue de un 470%, asegura Dmitry Bestuzhev, director para América Latina del Equipo Global de Investigación y Análisis de Kaspersky Lab.
>
> (...)
>
> Sin embargo, en el ciberespacio aumenta un riesgo mayor que pocos han percibido. Se trata de los ataques criminales que desde el mundo virtual están encaminadas [sic] a destruir infraestructuras, entidades públicas, sistema financiero y toda la economía de una nación (Santiago, 2012).

Por ende, se ha visto la necesidad de implementar políticas públicas que permitan mitigar y hacer frente a estas nuevas amenazas que se presentan para el mismo Estado, el sector privado y la ciudadanía.

Según Santiago (2012):

> El Comité Interamericano Contra el Terrorismo, CICTE, muestra que en Latinoamérica hay 13 países con Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT), entre los que se encuentran el ARCERT, en Argentina, creado en 1999, el CLCERT de Chile en el 2001, el CTIR-GOV en Brazil desde el 2004, el CTIRGT de Guatemala del 2006, el CERTUY de Uruguay y el VENCERT de Venezuela desde el 2008, y el PERCERT, creado en Perú durante el 2009. Quiere decir que desde hace varios años estos países cuentan con una estrategia nacional y un marco legal para la ciberseguridad y la ciberdefensa.

Como lo presenta Tecnósfera (2014):

> Seis millones de personas fueron víctimas de alguna modalidad de crimen digital en Colombia el año pasado, según la firma de seguridad digital Norton. La compañía calcula que el costo de los delitos informáticos en 2013 alcanzó 874 mil millones de pesos.
>
> (...)
>
> La situación para las entidades públicas y privadas no es mejor, pues el más elemental diagnóstico sugiere que existe un alto reto en temas de ciberseguridad. Durante el 2013 se detectaron 1.551 desfases, una modalidad de ataque cibernético que cambia la página principal de un sitio de internet. En lo que va del 2014 se han reportado 801 de esos ataques: 507 a portales comerciales, 186 de sitios web educativos y 108 de sitios web de entidades.

Esta gravísima problemática que está afectando tanto al sector público como al sector privado ha repercutido en el Gobierno nacional en los últimos cinco años. A partir de allí el Estado colombiano ha implementado una serie de estrategias desde la inclusión de nuevos tipos penales como delitos informáticos hasta la consolidación de una política pública plasmada en el Conpes 3701 "Lineamientos de política para ciberseguridad y ciberdefensa". (Conpes, 2011).

Dichas estrategias se han convertido en una política pública que permitiría al Estado colombiano y al sector privado enfrentar las nuevas amenazas del entorno digital, fortaleciendo las instituciones, los recursos físicos y de talento humano, entre otros.

Este artículo se inicia con un interrogante, ¿en qué consiste la política pública de seguridad y defensa cibernética que ha estado implementando Colombia en los últimos años?

I. PROYECTO DE INVESTIGACIÓN

El objetivo general de la investigación fue describir el estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia.

La investigación tuvo tres objetivos específicos:

- Describir los antecedentes y el marco normativo de la política pública de ciberseguridad y ciberdefensa en Colombia.
- Determinar quiénes son los responsables de la ciberseguridad y la ciberdefensa en Colombia y sus funciones.
- Diagnosticar la realidad que está enfrentando Colombia en cuanto a ciberseguridad y ciberdenfesa, sus principales desafíos y el panorama próximo.

II. MARCO TEÓRICO

A. Política pública

> Las políticas públicas son el conjunto de objetivos, decisiones y acciones que lleva a cabo un gobierno para solucionar los problemas que en un momento determinado los ciudadanos y el propio gobierno consideran prioritarios.
>
> Desde este punto de vista, las políticas públicas se pueden entender como un proceso que

> se inicia cuando un gobierno o un directivo público detecta la existencia de un problema que, por su importancia, merece su atención y termina con la evaluación de los resultados que han tenido las acciones emprendidas para eliminar, mitigar o variar ese problema. (Tamayo, 1997, pág. 2).

Siguiendo a Guerrero (2007, pág. 27):

> Las políticas públicas ponen de manifiesto la naturaleza y la composición interna del sistema jerárquico de autoridades y dan cuenta del régimen de competencias y responsabilidades en el ejercicio del poder institucionalizado. Constituyen el referente crucial que fundamenta su razón de ser gubernamental en la acción estatal y la acción pública. Es decir, los gobiernos (vías las políticas) hacen que la interacción orgánica entre el Estado y la sociedad se exprese y cumpla un propósito definido; estas deben ser comprendidas como el vector que sintetiza el conjunto de proposiciones, decisiones y operaciones dinámicas e interdependientes entre actores políticos, sociales e institucionales, a través de las cuales se busca imprimir un rumbo a la sociedad.

Entendiendo qué es una política pública paso a presentar su tipología según Guerrero (2007), quien la clasifica en tres corrientes de tendencia estructuralista:

> 1. Hegemónicas, que reflejan los intereses del proyecto político hegemónico.
>
> 2. Transaccionales, producto de negociación entre sectores de poder.
>
> 3. Dominación, que buscan preservar un orden establecido.

En la perspectiva de incorporar en el análisis las tensiones y conflictos que se originan y desarrollan en los procesos de estructuración y trazado de políticas públicas, estas pueden clasificarse de acuerdo con dos grandes criterios: su inscripción en el régimen político y su finalidad.

Por su inscripción en el régimen político pueden ser:

1. Estructurales. Dan cuenta de la razón de ser del Estado y del ejercicio de gobierno. Por su naturaleza, son continuas, no descentralizables ni delegables, y expresan claramente la función gubernativa del Estado (por ejemplo, la política monetaria, fiscal o de defensa nacional).

2. Sectoriales. Dan cuenta de la manera en que está dividido orgánica y funcionalmente el aparato estatal. No necesariamente son continuas, pueden ser descentralizadas o delegables en otros niveles e instancias de la administración pública o de la sociedad (por ejemplo, la política social, industrial, etc.).

2. Territoriales. Dan cuenta de la distribución de competencias y responsabilidades entre niveles de gobierno. Hacen relación a la razón de ser del Estado y el gobierno en los escenarios de mayor relación con los ciudadanos, involucra los elementos mínimos requeridos para la vida en comunidad (por ejemplo, las políticas de servicios públicos, políticas de seguridad y orden público).

Por su finalidad:

1. Inerciales: por su naturaleza, buscan mantener el rumbo de la acción del Estado y de la sociedad en la consecución de un propósito (por ejemplo, la lucha contra la inflación, las políticas de justicia y bienestar social).

2. Promocionales: por su naturaleza, buscan recomponer la correlación de fuerzas (sectorial o territorial) presentes en la gestión de determinadas acciones del Estado o de la sociedad (por ejemplo, las políticas de distribución del ingreso, la política de paz).

3. Compensatorias: se encaminan hacia la restitución de los equilibrios sectoriales o de la dinámica del crecimiento.

4. Contingentes: buscan enfrentar, con carácter estructural, problemas o situaciones inesperadas que por su magnitud o general desestabilización producen conmoción social.

B. Ciberseguridad

"Se define como la capacidad del Estado para minimizar el nivel de riesgo cibernético al que están expuestos los ciudadanos, en áreas como transacciones financieras, protección a la información y propiedad intelectual" (Rogers, 2014).

Las tendencias en ciberseguridad las podemos definir siguiendo a Rojas (2014):

> **Movilidad**: las ventajas de contar con información en tiempo real han preparado el terreno para la implementación de iniciativas alrededor del BYOD (*Bring Your Own Device*) pues pretenden incrementar la productividad de los empleados aumentando su grado de conectividad, acortando así los tiempos de respuesta. Como consecuencia de esto encontramos en Colombia una mayor disposición a flexibilizar el perímetro de las compañías mediante el establecimiento de regulaciones destinadas a estimular, y proteger, el teletrabajo.
>
> **Internet de las Cosas**: el mayor uso de dispositivos conectados a la red y que pueden terminar haciendo parte de una red corporativa incrementa la exposición de información confidencial a ciberatacantes atentos al descuido de los usuarios.
>
> **Cloud Computing**: la necesidad de ahorrar en costos, (...) las empresas han optado por tercerizar algunos procesos y herramientas confiando el almacenamiento de la información y la administración de aplicaciones a entidades ajenas a las organizaciones, con la pretensión de tener una operación más enfocada a las tareas claves del negocio. [Negritas en el original].

C. Ciberdefensa

Se define como la capacidad del Estado para prevenir y contrarrestar cualquier incidente o amenaza cibernética que afecte la soberanía nacional, en el uso de la internet con fines terroristas, actos de espionaje y guerra cibernética (...) En los últimos años la ciberseguridad y ciberdefensa han cobrado mayor interés en la agenda política global, ya que la internet y las TIC se vuelven cada vez más esenciales para el desarrollo social y económico. Asimismo, crece la importancia por infraestructura de TIC y las amenazas cibernéticas evolucionan a un ritmo acelerado, de acuerdo con un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE). (Rogers, 2014).

Es preciso hacer énfasis en la diferenciación de estos conceptos, pues la ciberdefensa tiende a dirigirse a las acciones tendientes a la protección de la soberanía nacional y el uso de las fuerzas militares y de inteligencia para contrarrestar distintas amenazas, mientras que ciberseguridad hace relación a todas esas acciones que ponen en marcha tanto el Estado como el sector privado para minimizar los riesgos de amenaza que puedan sufrir entidades de cualquier naturaleza y el ciudadano del común.

D. Ciberespacio

Tomando el concepto dado por Feliu (2013, pág. 4):

> El Ciberespacio es el espacio artificial creado por el conjunto de CIS [Sistemas de Información y Telecomunicaciones que utilizan las TIC o Tecnologías de la Información (informática) y las Comunicaciones (telecomunicaciones)] es decir de redes de ordenadores y de telecomunicaciones interconectados directa o indirectamente a nivel mundial. El ciberespacio es pues mucho más que Internet, más que los mismos sistemas y equipos, el hardware y el software e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio.

E. Consejo Nacional de Política Económica y Social (Conpes)

Esta es la máxima autoridad nacional de planeación. Se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país. Además, coordina y orienta a los organismos encargados de la dirección económica y social en el Gobierno, a través del estudio y aprobación de documentos sobre el desarrollo de políticas generales que son presentados en sesión (Departamento Nacional de Planeación, s. f.).

Existe, pues, una realidad, y es que los Estados y Colombia como tal, han implementado políticas públicas que se direccionan a la ciberseguridad y la ciberdefensa, porque como lo expone el Ministerio de Defensa Nacional (2009, pág. 3):

> Al beneficiarnos de los ilimitados recursos de las redes públicas de datos como Internet y de la infraestructura tecnológica interconectada, también nos enfrentamos a nuevos escenarios para el delito, el terrorismo y la guerra, lo cual exige la creación de nuevas herramientas de prevención, reacción y defensa.

III. METODOLOGÍA

En el desarrollo de esta investigación de carácter cualitativo se aplicó el método analítico-descriptivo, que permitió consolidar un marco normativo a nivel internacional y nacional, identificando los distintos organismos encargados de la política pública que Colombia viene implementando en materia de ciberseguridad y ciberdefensa, mediante la consulta de distintos documentos y fuentes.

IV. ANTECEDENTES Y DESARROLLO NORMATIVO DE LA POLÍTICA PÚBLICA DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA

NORMATIVIDAD INTERNACIONAL	Convenio sobre la Ciberdelincuencia (cc). Consejo de Europa. (Convenio sobre Cibercriminalidad de Budapest). Adoptado en noviembre de 2001 entró en vigor el 1° de julio de 2004.	Único instrumento vinculante vigente sobre el tema en el ámbito internacional, y su protocolo para la criminalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos. Cabe resaltar que si bien el cc tuvo su origen en el ámbito regional europeo, es un instrumento abierto para su adhesión a todos los países del mundo.
	Resolución AG/RES 2004 (XXXIVO/04) de la Asamblea General de la Organización de los Estados Americanos.	Estrategia integral para combatir las amenazas a la seguridad cibernética: - Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores. - Identificación y adopción de normas técnicas para una arquitectura segura de Internet. - Adopción y/o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA).

NORMATIVIDAD NACIONAL	Constitución Política de 1991	- Artículos 2, 15, 20, 75,78.
	Leyes	- Ley 527 de 1999 – Comercio Electrónico. - Ley 599 de 2000 – Código Penal Colombiano. - Ley 603 de 2000 – Control de legalidad de software. - Ley 962 de 2005 – Ley Antitrámites. - Ley 1150 de 2007 – Modificación al Estatuto de Contratación Pública. - Ley 1266 de 2008 – Habeas Data. - Ley 1273 de 2009 – Delitos informáticos. - Ley 1341 de 2009 – Sociedad de la Información y las TIC. - Ley 1581 de 2012 – Protección de Datos Personales.
	Decretos reglamentarios	- Decreto 2693 de 2012 – Gobierno en Línea. - Decreto reglamentario 1377 de 2013 – Protección de datos Personales.
	Normatividad especializada	- Documento Conpes 3701 de 2011. - Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009. - Circular 052 de 2007 (Superintendencia Financiera de Colombia). - Norma Técnica NTC-ISO/IEC Colombiana 27001.

V. ORGANISMOS ENCARGADOS DE LA CIBERSEGURIDAD Y LA CIBERDEFENSA EN COLOMBIA

A. Organismos del orden nacional

1. Presidencia de la República

En sus funciones constitucionales y legales el poder ejecutivo, en cabeza del Presidente de la República como suprema autoridad administrativa y comandante de las fuerzas militares, ha liderado la concreción de una política pública de ciberseguridad y ciberdefensa en el Estado colombiano. Desde la llegada del presidente Juan Manuel Santos a la Presidencia se ha demostrado gran voluntad política para enfrentar los nuevos desafíos a la sociedad y al propio Estado en materia de seguridad, implementando distintos instrumentos y mecanismos.

2. Ministerio de Defensa Nacional

La misión del Ministerio de Defensa Nacional (Mindefensa) le define como un deber "contribuir a la gobernabilidad democrática, la prosperidad colectiva y la erradicación de la violencia, mediante el ejercicio de la seguridad y la defensa, la aplicación adecuada y focalizada de la fuerza y el desarrollo de capacidades mínimas disuasivas." (Mindefensa, 2014).

Sus funciones específicas, según el Decreto 1512 de 2000, art. 5 son, entre otras:

> 1. Participar en la definición, desarrollo y ejecución de las políticas de defensa y seguridad nacionales, para garantizar la soberanía nacional, la independencia, la integridad territorial y el orden constitucional, el mantenimiento de las condiciones necesarias para el ejercicio y el derecho de libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz.

Así las cosas, esta institución es la llamada a concretar los lineamientos que materialicen la ciberseguridad y la ciberdefensa en el Estado colombiano, en conjunto con las fuerzas militares y de policía, así como los organismos de seguridad e inteligencia.

3. Ministerio de Tecnologías de la Información y las Comunicaciones

Según la Ley 1341 de 2009 o Ley de TIC, este Ministerio es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las tecnologías de la información y las comunicaciones.

Dentro de sus funciones está incrementar y facilitar el acceso de todos los habitantes del territorio nacional a las tecnologías de la información y las comunicaciones y a sus beneficios.

Su misión es promover el acceso, uso efectivo y apropiación masivos de las TIC, a través de políticas y programas para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país (MinTic, 2014).

Siendo esta institución la entidad especializada designada para ayudar a la concreción de las políticas de ciberseguridad y ciberdefensa, se constituye en un aliado primordial del Ministerio de Defensa para que estas puedan implementarse, desarrollarse y generar los efectos esperados frente a las nuevas problemáticas que la modernidad nos presenta.

B. Organismos especializados

La política de ciberseguridad y ciberdefensa en Colombia se soporta en una Comisión Intersectorial formada por los siguientes tres organismos creados a partir del Documento Conpes 3701 de 2011:

1. Comando Conjunto Cibernético de las Fuerzas Militares

Dependencia adscrita al Comando de las Fuerzas Militares, la cual se encarga de coordinar la respuesta a incidentes de seguridad que afecten la seguridad nacional.

Objetivos:

- Análisis forense básico.
- Operaciones de ciberdefensa.
- Operaciones de inteligencia.
- Auditorías y evaluaciones de seguridad.
- Aseguramiento de portales FF. MM.
- Capacitación especializada en ciberseguridad y ciberdefensa.
- Cooperación internacional.
- Membresía al FIRST.

2. Centro Cibernético Policial

Es la dependencia de la Dirección de Investigación Criminal e INTERPOL encargada del desarrollo de estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos (Centro Cibernético Policial, 2014).

Objetivos:

- Implementación del Centro Cibernético Policial (C. C. P.).
- Respuesta en línea a incidentes de ciberseguridad - Cuadrante Virtual (CAI Virtual).
- Coordinación internacional Interpol-Europol Grupo de Trabajo de Delitos Tecnológicos.
- Atención de incidentes informáticos DIJIN Laboratorios móviles de informática forense.
- Implementación CSIRT PONAL: equipo de respuesta a incidentes informáticos de la Policía Nacional.
- Laboratorio de investigación de malware (sector bancario).
- Análisis forense equipos Tablet Mac-Servidores-Smarthphones.
- Atención, judicialización de incidentes cibernéticos (afectación en distintos niveles y sectores).

- Unidades de investigación tecnológica UDITE (44) Cobertura nacional de la problemática.

3. Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT)

Tiene como responsabilidad central la coordinación de la ciberseguridad y ciberdefensa nacional, la cual estará enmarcada dentro del proceso misional de gestión de la seguridad y defensa del Ministerio de Defensa Nacional. Dicha coordinación corresponde a 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.

Objetivos:

- Coordinar y asesorar a CSIRT y entidades tanto del nivel público como privado y de la sociedad civil para responder ante incidentes informáticos.

- Ofrecer servicios de prevención ante amenazas informáticas, respuesta frente a incidentes informáticos, así como a aquellos de información, sensibilización y formación en materia de seguridad informática.

- Actuar como punto de contacto internacional con sus homólogos en otros países, así como con organismos internacionales involucrados en esta técnica.

- Promover el desarrollo de capacidades locales/sectoriales, así como la creación de CSIRT sectoriales para la gestión operativa de los incidentes de ciberseguridad en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.

- Desarrollar y promover procedimientos, protocolos y guías de buenas prácticas y recomendaciones de ciberdefensa y ciberseguridad para las infraestructuras críticas de la nación, en conjunto con los agentes correspondientes y velar por su implementación y cumplimiento.

- Coordinar la ejecución de políticas e iniciativas público-privadas de sensibilización y formación de talento humano especializado, relativas a la ciberdefensa y ciberseguridad.

- Apoyar a los organismos de seguridad e investigación del Estado para la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.

- Fomentar un sistema de gestión de conocimiento relativo a la ciberdefensa y ciberseguridad, orientado a la mejora de los servicios prestados por el colCERT.

VI. CONCLUSIONES

Es evidente que en Colombia existe una política pública líder en la región de Latinoamérica, respecto de la forma como el Estado ha venido enfrentando los desafíos que plantean la ciberseguridad y la ciberdefensa al propio Estado y a la sociedad en general. En ello hay que des-

tacar la importancia de hacer de dicha política un esfuerzo sin precedentes que debe reunir al sector privado, al sector público, al sector militar, la academia y la ciudadanía en torno de ella. Muestra de este liderazgo es que Colombia, según la clasificación global de la UIT en materia de ciberseguridad, en el año 2014 logró situarse en el noveno lugar a nivel mundial, no muy lejos de países como Francia, España, Egipto y Dinamarca, y en el quinto lugar en el ámbito de las Américas, luego de Chile y México.

Reconociendo la realidad que está enfrentando Colombia, y tomando lo comunicado por la Redacción de Tecnología del diario *El Tiempo* (7 de abril de 2014) a manera de diagnóstico:

> 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 exministro de las TIC, Diego Molano Vega.

Sin embargo este balance positivo contrasta con lo expresado por el mismo medio de comunicación:

> 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.

En razón de lo anterior el Gobierno colombiano está ultimando la nueva estructura que tendrá tanto en el alto Gobierno como a nivel nacional y regional el plan de ciberseguridad y ciberdefensa. Los lineamientos más relevantes según el artículo de *El Tiempo* (2014) que se viene comentando son:

> Puntos del 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 Molano 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.

> 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 respectivos decretos, el Presidente Santos.

Entre las novedades cabe resaltar la creación de la Agencia Nacional de Seguridad Cibernética y la Comisión Digital.

De igual manera:

> El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert), que hoy forma parte del Ministerio de Defensa Nacional, pasará a integrar la nueva agencia. Se crearán fiscalías especializadas en ciberdelitos y se capacitarán a los jueces de la República en el manejo de este tipo de casos.
>
> En apoyo con el sector privado y las universidades, se formarán centros de innovación y excelencia, que harán investigación y desarrollo de herramientas para mejorar la ciberseguridad o atenderán casos de ciberdefensa.
>
> Este nuevo plan es transversal a todo el Estado colombiano, tanto a nivel central como regional, con la participación activa del Ministerio de la Defensa, el de Justicia, la Cancillería y el de las TIC, entre otros. Dentro del plan también se contemplarán planes de formación sectorial en temas de ciberseguridad y un esquema de cooperación internacional. (Tecnosfera, 2014).

Es claro que los desafíos a los cuales nos estamos viendo expuestos son de gran magnitud y ameritan la respuesta que le está dando el Gobierno nacional, pues la globalización, la sociedad de la información y el desarrollo tecnológico exigen la implementación permanente de este tipo de políticas públicas, y el avance en la creación de organismos, mecanismos e instrumentos que permitan hacer frente a las amenazas que la modernidad y la era digital nos presentan como Estado y como sociedad.

Referencias

1. Centro Cibernético Policial. (2014). *Misión*. Recuperado el 30 de octubre de 2014 de ccp: http://www.buango.com/dijin/mision.php

2. Consejo Nacional de Política Económica y Social [Conpes]. (Julio 14 de 2011). *Documento Conpes 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa*. Recuperado el 25 de octubre de 2014 de mintic: http://www.mintic.gov.co/portal/604/articles3510_documento.pdf

3. Departamento Nacional de Planeación. (s. f.). *El Consejo Nacional de Política Económica y Social, Conpes.* Recuperado en junio de 2014 de dnp: https://www.dnp.gov.co/CONPES.aspx

4. *El Tiempo*. (Abril 7 de 2014). *El "plan Colombia" para la ciberseguridad*. Obtenido de El Tiempo: http://www.eltiempo.com/archivo/documento/CMS-13797815

5. Feliú Ortega, L. (Enero 21 de 2013). *Seguridad nacional y ciberdefensa. Aproximación conceptual: ciberseguridad y ciberdefensa.* Obtenido de catedraisdefe: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf

6. Grupo de Respuesta a Emergencias Cibernéticas de Colombia [colCERT]. (2014). Recuperado el 30 de octubre de 2014 de colcert: http://www.colcert.gov.co

7. Guerrero, L. F. (2007). *Los derechos humanos como política pública: Colombia, una salida democrática en un país violento*. Bogotá: Universidad Nacional de Colombia, Sede Bogotá, Facultad de Derecho, Ciencias Políticas y Sociales, Departamento de Ciencia Política.

8. Ministerio de Defensa Nacional [Mindefensa]. (Octubre de 2009). *Ciberseguridad y ciberdefensa: una primera aproximacion*. Recuperado el 20 de septiembre de 2014 de mindefensa: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

9. Ministerio de Defensa Nacional [Mindefensa]. (2014). *Misión y visión*. Recuperado el 30 de octubre de 2014 de mindefensa: https://www.mindefensa.gov.co/irj/portal/Mindefensa/contenido?guest_user=Guest_MDN&NavigationTarget=navurl://4fecd1a2e5aacd380ce74f217d1c0127

10. Ministerio de Tecnologías de la Información y las Comunicaciones [MinTic]. (2014). *Misión y visión*. Recuperado el 30 de octubre de 2014 de mintic: http://www.mintic.gov.co/portal/604/w3-propertyvalue-540.html

11. Rogers, A. (Marzo 31 de 2014). *Colombia elabora política de ciberdefensa y ciberseguridad*. Recuperado el 10 de noviembre de 2014 de bnamericas: http://www.bnamericas.com/es/news/tecnologia/colombia-elabora-politica-de-ciberdefensa-y-ciberseguridad

12. Rojas, D. (Septiembre 11 de 2014). *Ciberseguridad: tendencias y desafíos para el próximo cuatrienio en Colombia*. Recuperado el 5 de noviembre de 2014 de reportedigital: http://reportedigital.com/seguridad/tendencias-ciberseguridad-proximo-cuatrenio/

13. Santiago Pacheco, E. J. (Enero 1 de 2012). *Ciberseguridad: Colombia ante un ataque*. Recuperado el 15 de noviembre de 2014 de gerente.com: http://www.gerente.com/detarticulo.php?CodArticl=385

14. Tamayo, M. (1997). El análisis de las políticas públicas. En R. Bañón y E. Carrillo (Comp.), *La Nueva Administración Pública* (págs. 281-312). Madrid: Alianza. Recupera-

do en junio de 2014 de uca.edu: http://uca.edu.sv/mcp/media/archivo/f98099_tamayosaezelanalisisdelaspoliticaspubl icas.pdf

15. Tecnósfera. (Julio 11 de 2014). *Colombia se prepara para enfrentar los ciberataque*s. Recuperado el 15 de noviembre de 2014 de eltiempo: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/gobierno-prepara-planestatal-de-ciberseguridad/14233838