Documento Conpes 3701

Consejo Nacional de Política Económica y Social
República de Colombia
Departamento Nacional de Planeación

LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA

Ministerio de Interior y de Justicia
Ministerio de Relaciones Exteriores
Ministerio de Defensa Nacional
Ministerio de Tecnologías de la Información y las Comunicaciones
Departamento Administrativo de Seguridad
Departamento Nacional de Planeación-DJSG-DIFP-DIES-OI
Fiscalía General

Versión aprobada

Bogotá D.C., 14 de julio de 2011

Resumen

Este documento busca generar lineamientos de política en ciberseguridad[1] y ciberdefensa[2] orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

La problemática central se fundamenta en que la capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia. Así lo ha entendido el Gobierno Nacional al incluir este tema en el Plan Nacional de Desarrollo 2010-2014 “Prosperidad para Todos”, como parte del Plan Vive Digital.

Clasificación: H011, H411, R011

Palabras claves: Amenaza informática – Ciberespacio - Ciberdefensa – Ciberseguridad - Seguridad de la información – Infraestructura crítica – CERT - colCERT.

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

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

CONTENIDO

I. INTRODUCCIÓN

El uso de las tecnologías de la información y las comunicaciones trae consigo cambios y retos permanentes y se constituye como uno de los pilares del mundo globalizado. De manera simultánea el avance de estas tecnologías ha incrementado el uso de medios tecnológicos con fines delictivos alrededor del mundo.

La continua evolución, crecimiento y sofisticación de los ataques cibernéticos, al igual que la convergencia tecnológica[3], ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger al Estado ante estas nuevas amenazas[4]. El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil.

Trabajar en temas de ciberseguridad y ciberdefensa implica un compromiso del Gobierno Nacional por garantizar la seguridad de la información. Por ello, si bien este documento busca sentar las bases de política para los tópicos de ciberseguridad y ciberdefensa en particular, las entidades involucradas tendrán la responsabilidad de desarrollar estas bases y generar mecanismos que permitan garantizar la seguridad de la información a nivel nacional. Para lo anterior, se tendrán en cuenta las normas técnicas y los estándares nacionales e internacionales, así como iniciativas internacionales sobre protección de infraestructura crítica y ciberseguridad.

Teniendo en cuenta que el Gobierno Nacional requiere conocer y actuar de una forma integral frente a las amenazas informáticas, es necesario contar con una estrategia que incluya la creación de instancias adecuadas que permitan ejercer una labor de ciberseguridad y ciberdefensa frente a

---

[3] Es la tendencia para que diversos sistemas tecnológicos se desarrollen hacia la ejecución de tareas similares. La convergencia puede referirse a las tecnologías previamente separadas tales como voz (y características de la telefonía), datos (y usos de la productividad) y vídeo que ahora comparten recursos y obran recíprocamente (Jenkins, Henry (2006) Convergence Culture, New York University Press, New York).

[4] Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización. (ISO/IEC 13335-1:2004).

cualquier amenaza o incidente informático[5] que pueda comprometer información, afectar la infraestructura crítica del país y poner en riesgo la seguridad y defensa del Estado. La adopción de una Política Nacional de ciberseguridad y ciberdefensa que involucre a todos los sectores de la sociedad, bajo el liderazgo del Ministerio de Defensa Nacional y en coordinación con las demás entidades del Estado, es un imperativo al que debe darse la mayor de las prioridades.

Dentro de este documento se traza como objetivo central de esta política el fortalecimiento de la capacidad del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, y a su vez se definen tres objetivos específicos: 1) Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional; 2) Diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa; y 3) Fortalecer el cuerpo normativo y de cumplimiento en la materia.

Este documento define un plan de acción para la ejecución de la política en ciberseguridad y ciberdefensa, el cual estará a cargo de las entidades involucradas.

II. ANTECEDENTES

En el mes de abril de 2007, el gobierno de Estonia sufrió el que es considerado el mayor ataque cibernético de la historia, en el cual se vieron afectados la presidencia, el parlamento, la mayoría de los ministerios, los partidos políticos y dos de sus grandes bancos. Este ataque desató una gran crisis que requirió la intervención de la comunidad internacional y alertó a la Organización del Tratado del Atlántico Norte (OTAN), la cual en agosto de 2008, puso en marcha el Centro de Excelencia para la Cooperación en Ciberdefensa (CCD), con el fin de proteger a sus miembros de

[5] Amenaza Informática: La aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (Ministerio de Defensa Nacional de Colombia).
Incidente Informático: Evento único o serie de eventos de seguridad de la informática inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de una entidad y amenazar la seguridad de la información. (Ministerio de Defensa Nacional de Colombia).

este tipo de ataques y entrenar a personal militar, investigar técnicas de defensa electrónica y desarrollar un marco legal para ejercer esta actividad.

Vale mencionar otros dos ataques cibernéticos representativos. El primero, fue en contra de los Estados Unidos en el mes de julio de 2009, cuando una serie de ataques afectaron la Casa Blanca, el Departamento de Seguridad Interna (DHS), el Departamento de Defensa, la Administración Federal de Aviación y la Comisión Federal de Comercio.[6] Otro suceso fue el que reportó la Guardia Civil española en marzo de 2010, cuando desmanteló a una de las mayores redes de computadores "zombies",[7] conocida con el nombre de 'BotNet[8] Mariposa', compuesta por más de 13 millones de direcciones IP[9] infectadas, distribuidas en 190 países alrededor del mundo. Colombia ocupó el quinto puesto entre los países más afectados por esta red.

No.	PAÍS	%
1	INDIA	19.14
2	MÉXICO	12.85
3	BRASIL	7.74
4	COREA	7.24
5	**COLOMBIA**	**4.94**
6	RUSIA	3.14
7	EGIPTO	2.99
8	MALASIA	2.86
9	UCRANIA	2.69
10	PAKISTAN	2.55

No.	PAÍS	%
11	PERÚ	2.42
12	IRÁN	2.07
13	ARABIA SAUDÍ	1.85
14	CHILE	1.74
15	KAZAKHSTAN	1.38
16	EMIRATOS ARABES	1.15
17	MARRUECOS	1.13
18	ARGENTINA	1.10
19	ESTADOS UNIDOS	1.05

TABLA No. 1: Países Latinoamericanos más afectados por una red de zombies en marzo 2010
Fuente: www.infospyware.com

6 Reporte al Congreso de la Oficina de Control del gobierno de los Estados Unidos, Marzo de 2010, http://www.gao.gov/new.items/d10338.pdf

7 Denominación que se asigna a computadores personales que tras haber sido infectados por algún tipo de malware, pueden ser usadas por una tercera persona para ejecutar actividades hostiles. Este uso se produce sin la autorización o el conocimiento del usuario del equipo.

8 Es el nombre que se le da a una red de ordenadores que combina sus recursos para realizar una tarea común repartiendo la carga de trabajo entre todos los ordenadores (FireEye – Arbornet). El artífice de la botnet puede controlar todos los computadores/servidores infectados de forma remota y normalmente lo hace a través del IRC: Las nuevas versiones de estas botnets se están enfocando hacia entornos de control mediante HTTP, con lo que el control de estas máquinas será muchos más simple. Sus fines normalmente son poco éticos.

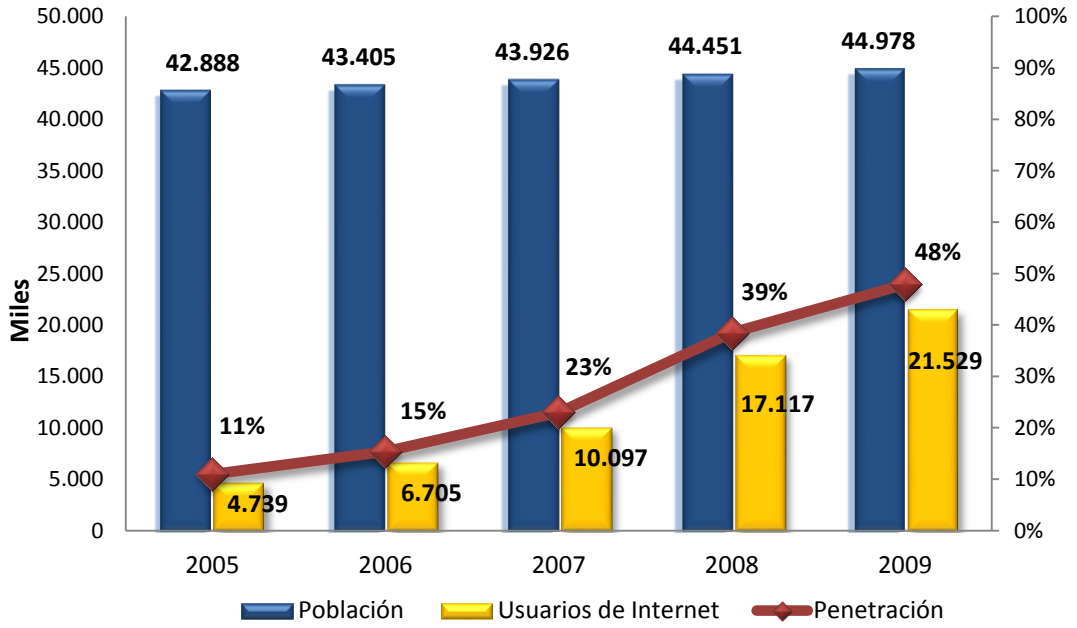
9 Etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol). www.iso.org

Con respecto al sector privado, un estudio realizado determinó que los ataques cibernéticos de los que han sido víctimas las empresas le ha costado a cada una de ellas, un promedio de dos millones de dólares al año.[10] El 42% de las organizaciones involucradas calificó a la seguridad informática como su principal prioridad, teniendo en cuenta que el 75% de ellas sufrió algún tipo de quiebre en su seguridad durante los 12 meses anteriores a la realización del estudio. Adicionalmente, se identificó que la escasez de personal, las nuevas iniciativas de tecnologías de la información y los problemas de cumplimiento de las normas de tecnologías de la información son factores críticos para la seguridad.[11]

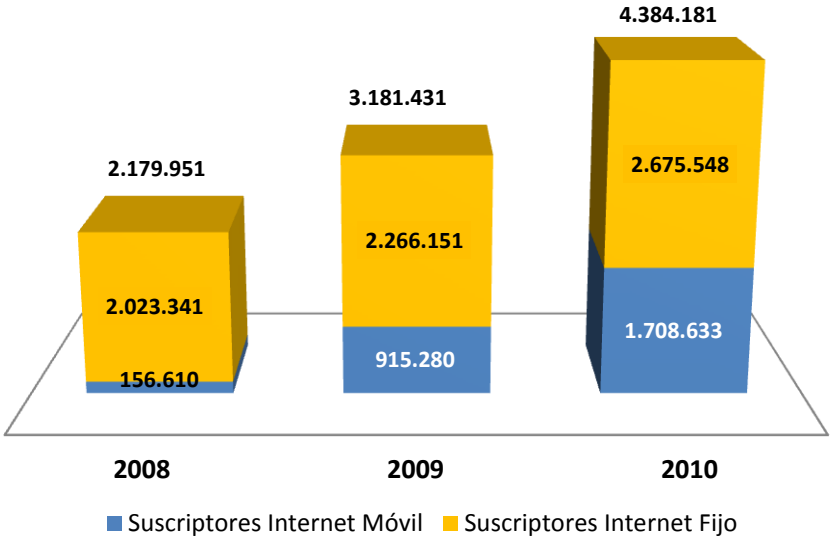
Ahora bien, en Colombia se ha incrementado considerablemente el uso de tecnologías de la información y las comunicaciones elevando su nivel de exposición a amenazas cibernéticas. El número de usuarios de internet aumentó en 354% entre el 2005 y el 2009, de acuerdo a la gráfica No.1. El número de suscriptores a internet se incrementó en 101% entre el 2008 y el 2010 alcanzando un total de 4.384.181 suscriptores de internet fijo y móvil. De estos, el 39% corresponde a suscriptores de Internet fijo y el 61% a suscriptores internet móvil, como se aprecia en la gráfica No. 2.

[10] Fuente: http://www.symantec.com/es/mx/business/theme.jsp?themeid=state_of_enterprise_security

[11] Fuente: http://www.symantec.com/es/mx/business/theme.jsp?themeid=state_of_enterprise_security



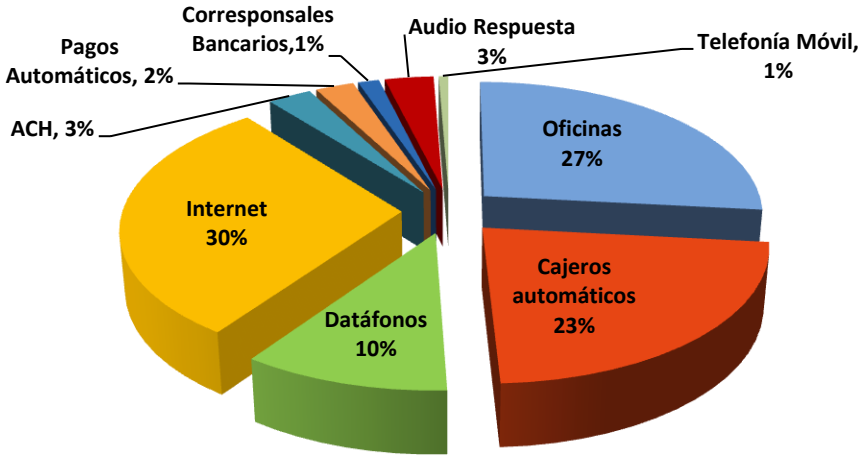
Gráfica No. 1 Usuarios a Internet 2005 - 2009
Fuente: Datos reportados por los proveedores de redes y servicios al SIUST, DANE



Gráfica No. 2 Suscriptores a Internet 2008 - 2010
Fuente: Datos reportados por los proveedores de redes y servicios al SIUST

Internet ha demostrado ser un medio de comunicación cada vez más utilizado por usuarios de servicios bancarios. Según la Superintendencia Financiera de Colombia, en el 2010 el 30% de las transacciones monetarias y no monetarias se realizaron utilizando el internet como medio de

ejecución, lo que representa un incremento del 12% en el número de operaciones realizadas por este canal, respecto al 2008, como lo muestra la gráfica No.3.



Gráfica No. 3 Operaciones Monetarias y no Monetarias por Canal 2010
Fuente: Informe de Transacciones y Operaciones Superintendencia Financiera de Colombia

El monto de las operaciones monetarias realizadas por internet en el 2010 alcanzaron los 1.237 billones de pesos, que representan un incremento del 121% frente al monto reflejado en las transacciones realizadas en el 2008.

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

También se pueden mencionar las denuncias reportadas por los ciudadanos a la Policía Nacional. De enero a diciembre de 2009, con base en la Ley 1273/09[12], se atendieron 575 delitos informáticos, que van desde el acceso abusivo a un sistema informático (259) hasta el hurto por medios informáticos y semejantes (247), la interceptación de datos informáticos (17), la violación de datos personales (35), la transferencia no consentida de activos (8), la suplantación de sitios Web (5), el daño informático (3) y la obstaculización ilegítima de un sistema informático (1). Así mismo, durante el 2010, la cantidad de delitos y contravenciones aumentó en 73% al alcanzar un total de 995 delitos informáticos, siendo el hurto por medios informáticos el incremento más representativo al pasar de 247 a 502[13] delitos, equivalentes al 103%.

A. Marco Nacional

Como referentes de la normativa nacional en la materia, es importante hacer mención a los esfuerzos realizados por Colombia en su legislación de manera cronológica, tal como se observa a continuación:

LEY / RESOLUCIÓN CIRCULAR	TEMA
Ley 527 de 1999 - COMERCIO ELECTRÓNICO	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"
Ley 599 DE 2000	Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."

[12] Por medio de la cual se crearon nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos.

[13] Datos reportados por el Sistema de Información Estadístico Delincuencial, Contravencional y Operativa de la policía Nacional "SIEDCO"

LEY / RESOLUCIÓN CIRCULAR	TEMA
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública, Secop.
Ley 1273 de 2009	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.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009	Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.
Circular 052 de 2007 (Superintendencia Financiera de Colombia)	Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

Tabla No. 2: Normatividad Nacional en la materia.

Se han formulado diferentes iniciativas en algunos sectores, las cuales han sido tomadas como documentos de consulta y referencia para la elaboración del presente documento CONPES:

INICIATIVA	ENTIDAD LÍDER	ALCANCE
Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea	Programa Gobierno en Línea - Ministerio de las Tecnologías de Información y las Comunicaciones	Este Modelo de Seguridad hace referencia al conjunto de políticas estratégicas que soportan objetivos de Gobierno en Línea como la "Protección de información del individuo" y la "credibilidad y confianza en el Gobierno en Línea". Establece como elementos fundamentales de la seguridad de la información para los Organismos Gubernamentales: 1) La disponibilidad de la información y los servicios. 2) La integridad de la información y los datos. 3) Confidencialidad de la información.
Recomendaciones al Gobierno Nacional para la implementación de una Estrategia Nacional de Ciberseguridad	Comisión de Regulación de Telecomunicaciones	Mediante este documento la Comisión de Regulación de Comunicaciones da al Gobierno Nacional recomendaciones para la creación de una Estrategia Nacional de Ciberseguridad y a su vez proporciona instrumentos idóneos para la colaboración y cooperación entre el gobierno y todos los niveles del sector privado; identifica caminos para la disuasión del crimen cibernético; recomienda la implementación y desarrollo de marcos jurídicos relacionados con la ciberseguridad que sean consistentes con los parámetros internacionales; da recomendaciones para la elaboración de sistemas de respuesta ante incidentes de seguridad en la red, incluyendo la vigilancia, análisis y respuesta a estos incidentes y propone lineamientos para la implementación de una cultura nacional de ciberseguridad que mejore los niveles de protección de la infraestructura crítica de la información en Colombia.
CSIRT- CCIT - Centro de coordinación de atención a incidentes de Seguridad Informática Colombiano para proveedores de servicios de Internet (ISP).	Cámara Colombiana de Informática y Telecomunicaciones (CCIT)	Centro de coordinación de atención a incidentes de seguridad informática colombiano, el cual está en contacto directo con los centros de seguridad de sus empresas afiliadas (las más grandes empresas proveedoras de Internet en Colombia). Está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas.

Tabla No.3: Iniciativas Nacionales en la materia

Adicionalmente, las instituciones del Estado colombiano han venido socializando la importancia de generar una política de ciberseguridad y ciberdefensa desde el año 2007. Para este fin, el Gobierno Nacional, con el acompañamiento internacional de la Organización de Estados Americanos -OEA a través del Comité Interamericano contra el Terrorismo – CICTE, organizó en mayo de 2008 un taller de concienciación en materia de seguridad cibernética y, en octubre de 2009, una mesa de diálogo nacional. Como conclusiones de las actividades realizadas, las instituciones del Estado solicitaron al Ministerio de Defensa Nacional asumir un liderazgo nacional que permitiera impulsar políticas en seguridad cibernética, así como crear mecanismos que pudieran dar respuesta a los incidentes y delitos cibernéticos que afectaran a la nación. Esta solicitud surgió como resultado de un profundo análisis de las particularidades del esquema de seguridad nacional, las capacidades técnicas existentes en el Ministerio de Defensa y un estudio del contexto internacional. El diagnóstico final indicó que el Ministerio de Defensa tenía la mayor capacidad para manejar de manera eficiente y coordinada estos temas.

Por ello, en los últimos dos años, el Ministerio de Defensa Nacional ha hecho un trabajo tendiente a posicionar el tema de ciberseguridad y ciberdefensa dentro de la agenda nacional.

No obstante Colombia no tenga aún los organismos de respuesta a incidentes cibernéticos, cuenta con capacidades y conocimientos que le han permitido hacer parte de comisiones que han asistido a otros gobiernos de la región (Panamá, República Dominicana y México) en la proyección de sus respectivos Centros Nacionales de Respuesta Técnica a Incidentes Informáticos.

Por último, cabe destacar que el tema de ciberseguridad y ciberdefensa fue incluido en el Plan Nacional de Desarrollo 2010-2014 “Prosperidad para Todos”, como parte del Plan Vive Digital liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones, cuyo fin es impulsar la masificación del uso de internet, para dar un salto hacia la prosperidad democrática.

B. **Marco Internacional**

Los principales instrumentos internacionales en materia de ciberseguridad y ciberdefensa son:

INSTRUMENTO	MATERIA
Convenio sobre Ciberdelincuencia[14] del Consejo de Europa – CCC (conocido como en convenio sobre cibercriminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004.	El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas. 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. El Consejo considera que el delito cibernético exige una política penal común destinada a prevenir la delincuencia en el ciberespacio[15] y en particular, hacerlo mediante la adopción de legislación apropiada y el fortalecimiento de la cooperación internacional. Cabe resaltar que si bien el CCC 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 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos.	Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética. Estipula tres vías de acción: • Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores - CSIRT[16]. Este cometido fue asignado al Comité Interamericano Contra el Terrorismo - CICTE. • Identificación y adopción de normas técnicas para una arquitectura segura de Internet. Esta labor es desarrollada por la Comisión Interamericana de Telecomunicaciones. • 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.

[14] Acciones ilícitas que han sido cometidas mediante la utilización de un bien o servicio informático (Ministerio de Defensa Nacional de Colombia).

[15] Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización de la electrónica, la informática y la cibernética.(Academia de la Lengua Española)

[16] Por sus siglas en inglés: Computer Security Incident Response Team o Equipo de Respuesta a Incidentes de Seguridad Cibernética (www.first.org).

INSTRUMENTO	MATERIA
Decisión 587 de la Comunidad Andina, adoptada el 10 de julio de 2004.	Por la cual se establecen los lineamientos de la Política de Seguridad Externa Común Andina. Dentro de los objetivos de dicha política se encuentra el prevenir, combatir y erradicar las nuevas amenazas a la seguridad y cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.
Consenso en materia de ciberseguridad[17] de la Unión Internacional de Telecomunicaciones - UIT, en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005.	Busca la promoción del examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.
Resolución 64/25 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional" Asamblea General de las Naciones Unidas. (2009)	La Asamblea General exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información Esta resolución continúa el seguimiento de la Asamblea, con las resoluciones 53/70, de 4 de diciembre de 1998; 54/49, de 1° de diciembre de 1999; 55/28, de 20 de noviembre de 2000; 56/19, de 29 de noviembre de 2001, 57/53, de 22 de noviembre de 2002; 58/32, de 8 de diciembre de 2003; 59/61, de 3 de diciembre de 2004; 60/45, de 8 de diciembre de 2005; 61/54, de 6 de diciembre de 2006; 62/17, de 5 de diciembre de 2007; y 63/37, de 2 de diciembre de 2008.

Tabla No.4: Referentes normatividad internacional en seguridad informática

Por otra parte, en la región 13 países cuentan con Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT), entre los que se encuentran Argentina (ArCERT), Bahamas (Policía Real), Bolivia (CRISIS), Brasil (CTIR-GOV), Canadá (CCIRC), Chile (CORE/ Min. Interior), Estados Unidos (USCERT), Guatemala (CSIRT- GT), Paraguay (CSIRT-Py), Perú (PerCERT), Suriname (SurCSIRT), Uruguay (CERTUy) y Venezuela (VenCERT)[18]. A nivel mundial se cuentan 55

[17] Respuesta operacional, colectiva y coordinada de una nación, que reconociendo la información como un activo crítico para salvaguardar su gobernabilidad, desarrolla y asegura estándares y prácticas sistemáticas orientadas a los individuos, las tecnologías, los procesos y los aspectos normativos y de cumplimiento.

[18] CICTE - OEA

CERTS nacionales, de acuerdo a la base de datos de la Universidad Carnegie Mellon (CERT- CC, www.cert.org/csirts/national/contact.html#).

Así mismo, a nivel mundial se han empezado a lanzar políticas en materia de ciberseguridad y ciberdefensa, se han incorporado nuevas capacidades tecnológicas y se han activado organismos para desarrollar estas funciones, como se muestra en la siguiente tabla:

PAÍS	ACCIÓN TOMADA POR EL GOBIERNO
ALEMANIA	En febrero de 2011, el gobierno alemán lanzó su Estrategia de Seguridad Cibernética. En abril de 2011 el Ministerio del Interior puso en marcha el Centro Nacional de Ciberdefensa.
AUSTRALIA	Creó el Centro de Operaciones Cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio.
CANADÁ	El Departamento de Seguridad Pública implementó el Centro Canadiense de Repuesta a Incidentes Cibernéticos (CCIRC), y en octubre de 2010 adoptó la Estrategia Canadiense de Seguridad Cibernética.
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. En mayo de 2011 fue adoptada la Estrategia Internacional para el Ciberespacio.
ESTONIA	En 2008 creó conjuntamente con otros países de Europa, la OTAN y EE.UU. el Centro Internacional de Análisis de Ciber amenazas. En este mismo año es adoptada una Estrategia de Seguridad Cibernética.
FRANCIA	Creó la Agencia de Seguridad para las Redes e Información (ANSSI), que vigila las redes informáticas gubernamentales y privadas con el fin de defenderlas de ataques cibernéticos. En febrero de 2011 fue adoptada una Estrategia de Defensa y Seguridad de los Sistemas de Información.

Tabla No. 5: Acciones tomadas para afrontar la Ciberdefensa a nivel mundial

III. DIAGNÓSTICO

A. Problema Central

Las instituciones involucradas en el desarrollo de este documento han identificado que la capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta grandes debilidades. Pese a que existen iniciativas gubernamentales, privadas y de la sociedad civil que buscan contrarrestar su efecto, no hay una coordinación interinstitucional apropiada.

Colombia es uno de los países que actualmente no cuenta con una estrategia nacional en ciberseguridad y ciberdefensa, que incluya un sistema organizacional y un marco normativo e institucional lo suficientemente fuerte para afrontar los nuevos retos en aspectos de seguridad cibernética. A diferencia de la mayoría de países latinoamericanos, Colombia aún no ha implementado un CSIRT o CERT[19] Nacional.

El creciente aumento de usuarios de internet, la elevada dependencia de la infraestructura crítica nacional a los medios electrónicos, así como el notable incremento de incidentes y delitos contra la seguridad cibernética, ha permitido identificar el elevado nivel de vulnerabilidad del país ante amenazas cibernéticas, tales como el uso de internet con fines terroristas, el sabotaje de servicios, espionaje y hurto por medios electrónicos, entre otros.

B. Efectos del problema central

El problema descrito anteriormente tiene como principales efectos el incremento de delincuencia cibernética y el riesgo de acceso indebido a la información, la afectación del normal funcionamiento y continuidad en la prestación de servicios y la persistencia de impunidad para manejar este tipo de delitos.

Se identifican tres (3) ejes problemáticos:

---

[19] Equipo de Respuesta a Emergencias Computacionales (CERT), equivalente al CSIRT pero con la marca registrada por la Universidad Carnegie Mellon.

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.

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.

   El entrenamiento y formación de los funcionarios públicos y privados para reaccionar como primeros respondientes ante la comisión de los delitos informáticos es deficiente. En muchas ocasiones se pierde la cadena de custodia de la evidencia digital y se generan dificultades en la realización de las investigaciones forenses. Así mismo, existe una oferta limitada de programas de capacitación para entidades que realizan funciones de policía judicial en el tema

   .

3. Debilidad en regulación y legislación de la protección de la información y de los datos.

Pese a que existen instrumentos legales y regulatorios en seguridad de la información, persisten falencias que impiden responder oportunamente a incidentes y delitos cibernéticos.

Recientemente el Congreso de la República aprobó la Ley de Inteligencia y contrainteligencia, estableciendo mecanismos de vigilancia y control para estas actividades. A pesar de ello, ésta es una regulación que requiere particularizarse para el ejercicio de la ciberseguridad y la ciberdefensa, sobre el cual existe muy poco en términos de alcance y operatividad.

En cuanto a normatividad internacional, dentro de los instrumentos que le permitirían al país integrarse a la comunidad mundial está la Convención del Consejo de Europa en Delito Cibernético, que requiere cumplir con aspectos como el establecimiento de mecanismos de cooperación judicial como la extradición, la creación de puntos de contacto localizables las 24 horas del día los 7 días a la semana para facilitar la investigación y el mantenimiento de los logs[20] por parte de los ISPs[21], durante el tiempo necesario.

Casos puntuales como el de la regulación de los ISPs, en los que la normatividad tuvo un avance importante a finales del año 2009. De acuerdo con las características y necesidades propias de su red, se creó para dichas empresas la obligación de implementar modelos de seguridad, con el fin de contribuir a mejorar la seguridad de sus redes de acceso, cumpliendo los principios de confidencialidad e integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio, y obligaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información. Sin embargo, se ha identificado, por ejemplo, que en lo relacionado a la seguridad de las redes de los ISPs, los logs no son almacenados por el

---

[20] Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

[21] Proveedores de servicios de internet (hoy en día en Colombia estos entes también brindan adicionalmente servicios de telefonía y televisión. Convirtiéndose de esta manera en unos prestadores de servicios integrales de telecomunicaciones).

tiempo adecuado para que sirvan en determinado momento como prueba o contribuyan en las investigaciones de ciberdelitos.

IV. OBJETIVOS

A. Objetivo Central

Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.

Para este fin es necesario involucrar a todos los sectores e instituciones del Estado con responsabilidad en el campo de ciberseguridad y ciberdefensa, creando un ambiente participativo donde todos los actores de la sociedad actúen con propósitos comunes, estrategias concertadas y esfuerzos coordinados. Igualmente, es de vital importancia crear conciencia y sensibilizar a la población en todo lo referente a la seguridad de la información; fortalecer los niveles de cooperación y colaboración internacional en aspectos de ciberseguridad y ciberdefensa; apoyar investigaciones relacionadas con ataques informáticos y proteger a la ciudadanía de las consecuencias de estos ataques.

B. Objetivos específicos

1. **Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional.**

   Este objetivo permitirá conformar organismos con la capacidad técnica y operativa necesaria para la defensa y seguridad nacional en materia cibernética. Para alcanzarlo se hace necesario que el Gobierno Nacional implemente las siguientes instancias:

Gráfica No. 5 Modelo de Coordinación
Fuente: Ministerio de Defensa Nacional

a. Una Comisión Intersectorial encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica (hardware, software y comunicaciones), información pública y ciberseguridad y ciberdefensa. Esta Comisión estaría encabezada por el Presidente de la República e integrada como mínimo por el Alto Asesor para la Seguridad Nacional, el Ministro de Defensa Nacional, el Ministro de Tecnologías de Información y Comunicaciones, el Director del Departamento Administrativo de Seguridad – DAS o quien haga sus veces, el Director de Planeación Nacional y el Coordinador del ColCERT.

De acuerdo con las temáticas a discutir, dentro de esta Comisión existirá la posibilidad de invitar a otros actores nacionales que representen al sector académico, al sector privado, expertos internacionales, así como otras instituciones del Estado.

b. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT será el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa. Prestará su apoyo y colaboración a las demás instancias nacionales tales como el Centro Cibernético Policial - CCP y el Comando Conjunto Cibernético - CCOC.

El colCERT será un grupo del Ministerio de Defensa Nacional, integrado por funcionarios civiles, personal militar y en comisión de otras entidades. Recibirá los lineamientos de la comisión intersectorial mencionada anteriormente.

La misión y objetivo central del colCERT será 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.

Los objetivos específicos del colCERT serán:

- Coordinar con la comisión intersectorial el desarrollo y promoción de políticas, procedimientos, recomendaciones, protocolos y guías de ciberseguridad y ciberdefensa, en conjunto con los agentes correspondientes y velar por su implementación y cumplimiento.
- Promover el desarrollo de capacidades locales/sectoriales así como la creación de CSIRTs sectoriales para la gestión operativa de los incidentes de ciberseguridad en la infraestructura crítica nacional, el sector privado y la sociedad civil.
- Coordinar y asesorar a CSIRTs y entidades tanto del nivel público, privado y de la sociedad civil en la respuesta a incidentes informáticos.

- Ofrecer servicios de prevención ante amenazas informáticas, respuesta frente a incidentes informáticos[22], así como aquellos de información, sensibilización y formación en materia de seguridad informática a todas las entidades que así lo requieran.
- Coordinar la ejecución de políticas e iniciativas público-privadas de sensibilización y formación de talento humano especializado, relativas a la ciberseguridad y ciberdefensa.
- Apoyar a los organismos de seguridad e investigación del Estado en 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 ciberseguridad y ciberdefensa, orientado a la mejora de los servicios prestados por el colCERT.
- Proveer al CCP y al CCOC la información de inteligencia informática que sea requerida.
- Actuar como punto de contacto internacional con sus homólogos en otros países, así como con organismos internacionales involucrados en esta temática.

El colCERT deberá iniciar operaciones en el segundo semestre del 2011 de acuerdo al siguiente modelo relacional:

[22] Evento no deseado y/o inesperado que suceden a través del ciberespacio, el cual bajo diferentes circunstancias, puede generar lesiones a personas, afectar o generar pérdidas en procesos y negocios

Modelo Relacional colCERT

Gráfica No. 6 Modelo Relacional del colCERT
Fuente: Ministerio de Defensa Nacional

El ColCERT, también liderará e implementará la "Red Nacional de CSIRTS y Cuerpos de Investigación". Esta red estará conformada por los CSIRTs sectoriales y los cuerpos de investigación del Estado, y tendrá como objeto facilitar y estrechar los lazos de cooperación y apoyo nacionales para la solución de incidentes de seguridad cibernética, a través de una plataforma con niveles altos de seguridad.

c. El Comando Conjunto Cibernético de las Fuerzas Militares – CCOC estará en cabeza del Comando General de las Fuerzas Militares, quien podrá delegar sus funciones dentro de las Fuerzas Militares dependiendo de las especialidades existentes en el sector. Este deberá prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales.

Las funciones generales del CCOC serán:

- Fortalecer las capacidades técnicas y operativas del país que permitan afrontar las amenazas informáticas y los ataques cibernéticos, a través de la ejecución de medidas de defensa a nivel de hardware y/o software y la implementación de protocolos de ciberdefensa.
- Defender la infraestructura crítica y minimizar los riesgos informáticos asociados con la información estratégica del país, así como reforzar la protección de los sistemas informáticos de la Fuerza Pública de Colombia.
- Desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional.

El CCOC deberá seguir los lineamientos nacionales y trabajará de manera coordinada con el ColCERT.

d. El Centro Cibernético Policial - CCP. Estará encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos. Desarrollará labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país, informando en su página web sobre vulnerabilidades cibernéticas. Recibirá y atenderá los lineamientos nacionales en ciberseguridad y trabajará de forma coordinada con el colCERT.

El CCP estará conformado por el equipo que designe la Policía Nacional, el cual estará encargado de dar respuesta operativa a los delitos cibernéticos. Para su operación, el CCP incorporará en su estructura el Comando de Atención Inmediata Virtual - CAI Virtual, un grupo de prevención, uno de gestión de incidentes y otro de investigación. El CAI virtual tendrá la labor de recibir toda la información y reportes de delitos cibernéticos, clasificando las conductas delictivas encontradas. Adicionalmente, podrá recibir solicitudes de charlas, cursos o visitas para difundir temas de seguridad pues está a cargo de los procesos de difusión y prevención del delito cibernético, siempre en coordinación con el colCERT.

El CCP se encargará de la investigación y apoyará la judicialización de los casos que se materialicen y se tipifiquen como delitos informáticos.

De manera general, las funciones que desarrollará serán las siguientes:

- Proteger a la ciudadanía de las amenazas y/o delitos cibernéticos.
- Responder operativamente ante los delitos cibernéticos, desarrollando labores coordinadas de prevención, atención, investigación y de apoyo a la judicialización de los delitos informáticos en el país.
- Dar asesoría sobre vulnerabilidades y amenazas en sistemas informáticos.
- Divulgar información a la ciudadanía, que permita prevenir lo concerniente a pérdida de disponibilidad, integridad y/o confidencialidad de la información.
- Apoyar e investigar en coordinación con el colCERT las vulnerabilidades, amenazas e incidentes informáticos que afecten la seguridad de la infraestructura informática crítica de la Nación.
- Fomentar la concienciación de políticas de seguridad cibernética, en coordinación con los actores involucrados.

Es importante indicar que el CCP deberá iniciar operaciones en el año 2011.

2. Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad.

Este objetivo permitirá generar y fortalecer las capacidades existentes en materia de seguridad cibernética, con el propósito de poder afrontar las amenazas que atentan contra los propósitos planteados.

Inicialmente, se capacitará a los funcionarios que estén directamente involucrados en la atención y manejo de incidentes cibernéticos. Gradualmente se extenderá esta capacitación a las demás instituciones del Gobierno. Entre los planes de capacitación, el colCERT con el apoyo del Comité Interamericano Contra el Terrorismo (CICTE) de la

OEA, entre otros, adelantará un plan de capacitación para los demás funcionarios del Estado, así como programas de sensibilización y concienciación para los ciudadanos en general. De la misma forma, el Ministerio de Defensa Nacional buscará la implementación gradual de asignaturas en seguridad de la información, ciberseguridad y ciberdefensa teórico-prácticas en las escuelas de formación y de capacitación de oficiales y suboficiales.

En esta misma línea, el CCP buscará la colaboración de programas que apoyan la implementación del sistema penal oral acusatorio tales como el International Criminal Investigative Training Assistance Program - ICITAP, ATA, OPDAT y organismos nacionales como la Escuela de Investigación Criminal, Criminalística y de Ciencias Forenses de la Fiscalía General de la Nación, la Escuela Judicial Rodrigo Lara Bonilla, entre otros, para establecer planes de capacitación jurídica en lo referente a la seguridad informática para policía judicial, fiscales y jueces.

3. **Fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.**

Este objetivo busca desarrollar las herramientas jurídicas necesarias para una efectiva y eficiente prevención, investigación y judicialización de los delitos cibernéticos.

Así, se propenderá por la expedición de la normatividad necesaria para dar cumplimiento a los tratados internacionales sobre la materia en cuestión en la medida que hagan parte del bloque de constitucionalidad, así como por la debida reglamentación de lo dispuesto en la legislación nacional. Las instituciones responsables de la ciberseguridad y ciberdefensa deberán buscar y evaluar la participación en diferentes redes y mecanismos internacionales de cooperación (Consejo de Europa, OEA y FIRST), que permitan preparar al país para afrontar los crecientes desafíos del entorno internacional en el área de seguridad cibernética, así como responder de una forma más eficiente a incidentes y delitos de seguridad cibernética.

Colombia afrontará el reto de posicionarse como líder regional en el área de seguridad cibernética a través del intercambio de buenas prácticas, conocimiento y experiencias, prestando especial atención a la promoción de la experiencia nacional en el proceso de desarrollo de la política de ciberseguridad y ciberdefensa. Para ello, los líderes y expertos del tema deberán participar en conferencias, talleres y reuniones especializadas en los que se discutan temas de seguridad cibernética a nivel internacional.

Para todo lo anterior, el colCERT y el CCP deberán articular iniciativas con el sector privado y la sociedad civil.

V. PLAN DE ACCIÓN

# A	Acción concreta	Información del Responsable de la ejecución		Fecha de inicio	Fecha de finalización
		Entidad	Dependencia		
	Implementar la Institucionalidad Adecuada:				
1	Aprobar los lineamientos de Política para el desarrollo e impulso de la estrategia de ciberseguridad y la ciberdefensa, presentados en este documento.	Departamento Nacional de Planeación	Subdirección General	14/07/2011	14/07/2011
2	Solicitar al Ministerio de Defensa Nacional y al Ministerio de Tecnologías de la Información y las Comunicaciones adoptar el mecanismo de coordinación intersectorial más adecuado para emitir los lineamientos rectores del colCERT. En caso de no existir uno, se solicita su creación.	Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y las Comunicaciones	Despacho de Ministro de Defensa Nacional / Despacho de Ministro de Tecnologías de la Información y las Comunicaciones	14/07/2011	31/12/2012
3	Solicitar al Ministerio de Defensa Nacional crear el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT.	Ministerio de Defensa Nacional	Despacho de Ministro de Defensa Nacional	14/07/2011	31/12/2011
4	Solicitar al Ministerio de Defensa Nacional que una vez creado el colCERT, emita los modelos de seguridad en el ciberespacio que minimicen el nivel de riesgo al que las entidades están expuestas.	Ministerio de Defensa Nacional	Despacho de Ministro de Defensa Nacional	14/07/2011	30/06/2012
5	Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones y a la Comisión de Regulación de Comunicaciones realizar el acompañamiento al Ministerio de Defensa Nacional en las actividades que se consideren pertinentes para la conformación y el desarrollo de las actividades del colCERT.	Ministerio del Tecnologías de Información y las Comunicaciones, Comisión de Regulación de las Comunicaciones	Despacho del Ministro de Tecnologías de la Información y las Comunicaciones, Director Ejecutivo de la Comisión de Comunicaciones	14/07/2011	31/12/2015
6	Solicitar al Ministerio del Interior y de Justicia, al Ministerio del Tecnologías de Información y las Comunicaciones, y al Departamento Administrativo de Seguridad o quien haga sus veces, destinar recurso humano con conocimientos técnicos y/o jurídicos en el tema de seguridad de la información y ciberseguridad, para apoyar la ejecución de actividades del colCERT.	Ministerio del Interior y Justicia, Ministerio del Tecnologías de Información y las Comunicaciones, DAS o quien haga sus veces	Despacho del Ministro de Tecnologías de la Información y las Comunicaciones / Dirección General Departamento Administrativo de Seguridad	14/07/2011	31/12/2012
7	Solicitar al Ministerio de Defensa Nacional crear el Centro Cibernético Policial – CCP.	Ministerio de Defensa Nacional	Despacho de Ministro de Defensa Nacional	14/07/2011	31/12/2011
8	Solicitar al Ministerio de Defensa Nacional crear el Comando Conjunto Cibernético – CCOC.	Ministerio de Defensa Nacional	Despacho de Ministro de Defensa Nacional	14/07/2011	31/12/2011
9	Solicitar al Ministerio de Defensa Nacional realizar en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones estudios en seguridad de la información, así como la identificación de la infraestructura crítica nacional.	Ministerio de Defensa Nacional	Despacho de Ministro de Defensa Nacional	14/07/2011	31/12/2012
10	Solicitar al Ministerio de las Tecnologías de la Información y las Comunicaciones emitir un documento con las directrices en temas de seguridad de la información basado en estándares internacionales, que deberán ser implementadas por las entidades del sector público.	Ministerio de Tecnologías de la Información y Comunicaciones	Despacho de Ministro de Tecnologías de la Información y las Comunicaciones	14/07/2011	31/12/2013

# A	Acción concreta	Información del Responsable de la ejecución		Fecha de inicio	Fecha de finalización
		Entidad	Dependencia		
11	Solicitar a la Comisión de Regulación de Comunicaciones realizar un análisis regulatorio acerca de los aspectos técnicos que deben cumplir los proveedores de redes y servicios de telecomunicaciones para garantizar los principios de confidencialidad de datos, integridad de datos y disponibilidad, así como las medidas para autenticación y acceso de los usuarios a la red y el no repudio de las comunicaciones y, en caso de ser requerido a partir de tal análisis, llevar a cabo los ajustes a que haya lugar frente al marco regulatorio vigente.	Comisión de Regulación de las Comunicaciones	Director Ejecutivo de la Comisión de Comunicaciones	14/07/2011	31/12/2015
Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberseguridad y ciberdefensa:					
12	Solicitar al Ministerio de las Tecnologías de la Información y las Comunicaciones, facilitar los canales institucionales para que el colCERT pueda realizar la sensibilización y concienciación en temas de seguridad cibernética.	Ministerio de Tecnologías de la Información y las Comunicaciones	Despacho de Ministro de Tecnologías de la Información y las Comunicaciones	14/07/2011	31/12/2012
13	Solicitar al Ministerio de Defensa Nacional en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones, diseñar las campañas de sensibilización y concienciación en temas de seguridad cibernética.	Ministerio de Defensa Nacional	Despacho de Ministro de Defensa Nacional	14/07/2011	31/12/2012
14	Solicitar al Ministerio de Defensa Nacional implementar gradualmente asignaturas en seguridad de la información, ciberdefensa y ciberseguridad (teórico-prácticas), en las escuelas de formación y de capacitación de oficiales y suboficiales.	Ministerio de Defensa Nacional	Despacho de Ministro de Defensa Nacional	14/07/2011	31/12/2015
15	Solicitar al Ministerio de Defensa Nacional adelantar un plan de capacitación en temas de seguridad de la información para los funcionarios del Estado, con el apoyo de organismos internacionales.	Ministerio de Defensa Nacional	Despacho de Ministro de Defensa Nacional	14/07/2011	31/12/2015
16	Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones, al Ministerio de Defensa Nacional y al Departamento Administrativo de Seguridad o a quien haga sus veces, diseñar e implementar planes de capacitación en lo referente a seguridad informática, investigación y judicialización de delitos informáticos, para policía judicial.	Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional, DAS o quien haga sus veces	Despacho del Ministro de Tecnologías de la Información y las Comunicaciones, Despacho del Ministro de Defensa Nacional, Dirección General DAS	14/07/2011	31/12/2015
17	Sugerir a la Fiscalía General de la Nación en coordinación con el Consejo Superior de la Judicatura diseñar e implementar planes de capacitación sobre temas de investigación y judicialización de delitos informáticos, para policía judicial, jueces y fiscales.	Fiscalía General de la Nación	Coordinador Nacional de Delitos Informaticos	14/07/2011	31/12/2014
18	Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones realizar las gestiones necesarias con el Ministerio de Educación Nacional y el SENA, para la generación de un plan de capacitación para el sector privado en temas de ciberseguridad y de seguridad de la información.	Ministerio de Tecnologías de la Información y Comunicaciones	Despacho de Ministro de Tecnologías de la Información y las Comunicaciones	14/07/2011	31/12/2013

# A	Acción concreta	Información del Responsable de la ejecución		Fecha de inicio	Fecha de finalización
		Entidad	Dependencia		
Fortalecer la legislación y la cooperación internacional en materia de ciberseguridad y ciberdefensa:					
19	Solicitar al Ministerio del Interior y de Justicia realizar en coordinación con el el Ministerio de Defensa Nacional y el Ministerio de Tecnologías de Información y Comunicaciones, un documento en el que se analice la normatividad actual y se propongan las modificaciones necesarias en materia de seguridad de la información y protección de datos, para prevenir el ciberdelito, identificando las dificultades de interpretación y aplicación.	Ministerio del Interior y Justicia	Despacho de Ministro del Interior y Justicia	14/07/2011	31/12/2013
20	Solicitar al Ministerio del Interior y Justicia, en coordinación con el Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones, con base en el análisis realizado, adelantar las iniciativas tendientes a expedir o reformar las leyes que sean necesarias así como reglamentar aquellas a que haya lugar, en aras de garantizar el marco normativo adecuado para la ciberseguridad, la ciberdefensa y la seguridad de la información.	Ministerio del Interior y Justicia	Despacho de Ministro del Interior y Justicia	14/07/2011	31/12/2013
21	Solicitar al Ministerio de Relaciones Exteriores apoyar al colCERT, en materia de cooperación internacional, en los temas de ciberseguridad, ciberdefensa y seguridad informática, en los que se incluya la designación del colCERT como punto de contacto internacional en temas referentes a la ciberseguridad y la ciberdefensa.	Ministerio de Relaciones Exteriores	Despacho de Ministra de Relaciones Exteriores	14/07/2011	31/12/2012
22	Solicitar al Ministerio de Relaciones Exteriores, estudiar la viabilidad y conveniencia para Colombia de adherir a los principales instrumentos internacionales en materia de seguridad de la información y protección de datos, con el directo apoyo del Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones. En caso de que el estudio produzca una recomendación positiva, iniciar los trámites de adhesión al instrumento que corresponda.	Ministerio de Relaciones Exteriores	Despacho de Ministra de Relaciones Exteriores	14/07/2011	31/12/2012
		Ministerio de Relaciones Exteriores	Dirección de Asuntos Políticos Multilaterales	14/07/2011	31/12/2012

[1] Las Leyes se consideraran implementadas con la presentación del proyecto.

VI. FINANCIAMIENTO

El costo que genere la implementación de los lineamientos que posteriormente emita el colCERT en materia de ciberseguridad y ciberdefensa para las entidades públicas, también provendrá del presupuesto asignado a cada entidad.

La implementación inicial del colCERT, el CCP y el CCOC en el Ministerio de Defensa Nacional, implicará la asignación de los siguientes recursos por parte del Ministerio:

2011	2012	2013	2014
$ 1.428.444.328	$ 5.400.000.000	$ 5.000.000.000	$ 4.600.000.000

En este presupuesto se incluye, adicionalmente, la operación del colCERT con un equipo de seis (6) funcionarios del Ministerio de Defensa Nacional y de otras entidades públicas[23]. Sobre la marcha, el colCERT, con el aval del mecanismo de coordinación Intersectorial de Seguridad Cibernética que se adopte, podrá determinar la necesidad de ampliar dicho grupo para lo cual se deberá hacer una revisión del presupuesto aquí indicado y del apoyo de cada entidad.

Es importante precisar que se destinarán recursos adicionales para el año 2011, con el fin de apoyar al Comando General de las Fuerzas Militares en la implementación del CCOC.

Para el 2011 el presupuesto de los tres centros será financiado con recursos de funcionamiento. A partir de 2012, los recursos serán financiados por inversión con tres proyectos que ya se encuentran inscritos en el Banco de Proyectos de Inversión.

[23] Los funcionarios de otras entidades públicas harán parte del grupo bajo la figura de comisión temporal.

VII. RECOMENDACIONES

El Ministerio de Defensa Nacional, El Ministerio de Tecnologías de la Información y las Comunicaciones, El Ministerio de Interior y Justicia, el Ministerio de Relaciones Exteriores, el Departamento Nacional de Planeación, Departamento Administrativo de Seguridad, recomiendan al Consejo Nacional de Política Económica y Social - CONPES:

Implementar la institucionalidad apropiada:

1. Aprobar los Lineamientos de Política para el desarrollo e impulso de la estrategia de ciberseguridad y la ciberdefensa, presentados en este documento.

2. Solicitar al Ministerio de Defensa Nacional y al Ministerio de Tecnologías de la Información y las Comunicaciones adoptar el mecanismo de coordinación intersectorial más adecuado para emitir los lineamientos rectores del colCERT. En caso de no existir uno, se solicita su creación.

3. Solicitar al Ministerio de Defensa Nacional crear el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT.

4. Solicitar al Ministerio de Defensa Nacional que una vez creado el colCERT, emita los lineamientos de seguridad en el ciberespacio que minimicen el nivel de riesgo al que las entidades están expuestas.

5. Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones y a la Comisión de Regulación de Comunicaciones realizar el acompañamiento al Ministerio de Defensa Nacional en las actividades que se consideren pertinentes para la conformación y el desarrollo de las actividades del colCERT.

6. Solicitar al Ministerio del Interior y de Justicia, al Ministerio del Tecnologías de Información y las Comunicaciones, y al Departamento Administrativo de Seguridad o quien haga sus veces, destinar recurso humano con conocimientos técnicos y/o jurídicos en

el tema de seguridad de la información y ciberseguridad, para apoyar la ejecución de actividades del colCERT.

7. Solicitar al Ministerio de Defensa Nacional crear el Centro Cibernético Policial – CCP.

8. Solicitar al Ministerio de Defensa Nacional crear el Comando Conjunto Cibernético – CCOC.

9. Solicitar al Ministerio de Defensa Nacional realizar en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones estudios en seguridad de la información, así como la identificación de la infraestructura crítica nacional.

10. Solicitar al Ministerio de las Tecnologías de la Información y las Comunicaciones emitir un documento con las directrices en temas de seguridad de la información basado en estándares internacionales, que deberán ser implementadas por las entidades del sector público.

11. Solicitar a la Comisión de Regulación de Comunicaciones realizar un análisis regulatorio acerca de los aspectos técnicos que deben cumplir los proveedores de redes y servicios de telecomunicaciones para garantizar los principios de confidencialidad de datos, integridad de datos y disponibilidad, así como las medidas para autenticación y acceso de los usuarios a la red y el no repudio de las comunicaciones y, en caso de ser requerido a partir de tal análisis, llevar a cabo los ajustes a que haya lugar frente al marco regulatorio vigente.

Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberseguridad y ciberdefensa:

12. Solicitar al Ministerio de las Tecnologías de la Información y las Comunicaciones, facilitar los canales institucionales para que el colCERT pueda realizar la sensibilización y concienciación en temas de seguridad cibernética.

13. Solicitar al Ministerio de Defensa Nacional en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones, diseñar las campañas de sensibilización y concienciación en temas de seguridad cibernética.

14. Solicitar al Ministerio de Defensa Nacional implementar gradualmente asignaturas en seguridad de la información, ciberseguridad y ciberdefensa (teórico-prácticas), en las escuelas de formación y de capacitación de oficiales y suboficiales.

15. Solicitar al Ministerio de Defensa Nacional adelantar un plan de capacitación en temas de seguridad de la información y ciberseguridad para los funcionarios del Estado, con el apoyo de organismos internacionales.

16. Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones, al Ministerio de Defensa Nacional y al Departamento Administrativo de Seguridad o a quien haga sus veces, diseñar e implementar planes de capacitación en lo referente a seguridad informática, investigación y judicialización de delitos informáticos, para policía judicial.

17. Sugerir a la Fiscalía General de la Nación en coordinación con el Consejo Superior de la Judicatura diseñar e implementar planes de capacitación sobre temas de investigación y judicialización de delitos informáticos, para policía judicial, jueces y fiscales.

18. Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones realizar las gestiones necesarias con el Ministerio de Educación Nacional y el SENA, para la generación de un plan de capacitación para el sector privado en temas de ciberseguridad y de seguridad de la información.

Fortalecer la legislación y la cooperación internacional en materia de ciberseguridad y ciberdefensa:

19. Solicitar al Ministerio del Interior y de Justicia realizar en coordinación con el Ministerio de Defensa Nacional y el Ministerio de Tecnologías de Información y Comunicaciones un documento en el que se analice la normatividad actual y se propongan las modificaciones necesarias en materia de seguridad de la información y protección de datos, para prevenir el ciberdelito, identificando las dificultades de interpretación y aplicación.

20. Solicitar al Ministerio del Interior y Justicia, en coordinación con el Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones, con base en el análisis realizado, adelantar las iniciativas tendientes a expedir o reformar las leyes que sean necesarias así como reglamentar aquellas a que haya lugar, en aras de garantizar el marco normativo adecuado para la ciberseguridad, la ciberdefensa y la seguridad de la información.

21. Solicitar al Ministerio de Relaciones Exteriores apoyar al colCERT, en materia de cooperación internacional, en los temas de ciberseguridad, ciberdefensa y seguridad informática, en los que se incluya la designación del colCERT como punto de contacto internacional en temas referentes a la ciberseguridad y la ciberdefensa.

22. Solicitar al Ministerio de Relaciones Exteriores, estudiar la viabilidad y conveniencia para Colombia de adherir a los principales instrumentos internacionales en materia de seguridad de la información y protección de datos, con el directo apoyo del Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones. En caso de que el estudio produzca una recomendación positiva, iniciar los trámites de adhesión al instrumento que corresponda.

VIII. BIBLIOGRAFÍA

usCERT – Estados Unidos: http://www.us-cert.gov

Carnegie Mellon University/CERT Coordination Center: http://www.cert.org/csirts/

U.S. National Strategy To Secure Cyberspace http://www.whitehouse.gov/pcipb/

Forum Of Incident Response Security Teams (FIRST): http://www.first.org

CICTE - Comité Interamericano Contra el Terrorismo – Organización de los Estados Americanos: http://www.cicte.oas.org

Portal Interamericano de Cooperación en Materia de Delito Cibernético: http://www.oas.org/juridico/spanish/cybersp.htm

ENISA Documento a Step-By-Step Approach On How To Set Up A CSIRT.

IX. GLOSARIO

Amenaza: Violación potencial de la seguridad. (Rec. UIT-T X.800, 3.3.55)

Amenaza informática: La aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (Ministerio de Defensa de Colombia)

Ataque cibernético: Acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia)

BotNet: Es el nombre que se le da a una red de ordenadores que combina sus recursos para realizar una tarea común repartiendo la carga de trabajo entre todos los ordenadores (FireEye – Arbornet).

CERT: (Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas. (Universidad Carnegie – Mellon)

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

Ciberdelincuencia: Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia)

Ciberdelito / Delito Cibernético: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia)

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Cibernética: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Academia de la Lengua Española)

Cibernético: Adjetivo masculino y femenino para denominar todo cuanto tiene relación con la cibernética: órgano cibernético, proceso cibernético o que está especializado en cibernética, así como también a la persona que se dedica a ella. (Academia de la Lengua Española)

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

Ciberterrorismo: La convergencia del terrorismo y ciberespacio con el fin de atacar ilegalmente ordenadores, redes e información almacenada en ellos, incluye violencia contra personas o propiedades o, al menos, genera el miedo. Abarca asesinatos, explosiones, contaminación de aguas o grandes pérdidas económicas, entre otras acciones. (Dorothy Denningal, profesora de la Universidad de Georgetown.)

Convergencia: Evolución coordinada de redes que antes eran independientes hacia una uniformidad que permita el soporte común de servicios y aplicaciones. (Rec. UIT-T Q.1761, 3.1)

CSIRT: (Computer Security Incident Response Team) Equipo de Respuesta a Incidentes de Seguridad cibernética, por su sigla en inglés. (http:// www.first.org)

DDoS: De las siglas en inglés Distributed Denial of Service. Ataques Distribuidos de Denegación de Servicio. (http://www.rediris.es)

DOS (Denial of Service): Denegación de servicio. Servicio no disponible a una persona o proceso (aplicación) cuando es necesario (disponibilidad). (http://www.rediris.es)

Incidente Informático: Cualquier evento adverso real o sospechado en relación con la seguridad de sistemas de computación o redes de computación http://www.cert.org/csirts/csirt_faq.html CERT/CC.

Infraestructura crítica: Es el 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, salud pública, o la combinación de ellas, en una nación. (Resolución CRC 2258 de 2009)

IP (Internet Protocol): Etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP. (http://www.iso.org)

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares. (http://www.iso.org)

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. (http://www.iso.org)

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. (http://www.iso.org)

ISP: Proveedores de servicios de internet. En Colombia estos entes brindan adicionalmente servicios de telefonía y televisión, convirtiéndose de esta manera en unos prestadores de servicios integrales de telecomunicaciones.

Logs: Registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

NAP (Network Acces Point) Colombia: Punto de conexión nacional de las redes de las empresas que proveen el servicio de acceso de Internet en Colombia, con el cual se logra que el tráfico de Internet que tiene origen y destino en nuestro país, utilice solamente canales locales o nacionales. (www.nap.com.co)

NTC5411- 1 Gestión de la seguridad de la tecnología de la información y las comunicaciones. (Catálogo publicaciones ICONTEC Internacional)

Riesgo Informático: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (ISO Guía 73:2002)

Seguridad Lógica: Consiste en la aplicación de barreras que resguarden el acceso a los datos y sólo se permite acceder a ellos a las personas autorizadas. (http://www.segu-info.com)

Servicios Electrónicos: e-Services, se refiere a la mejora en la facilitación de los servicios públicos a los ciudadanos a través del ciberespacio. (United Nations Educational, Scientific and Cultural Organization UNESCO)

Telecomunicaciones: Toda transmisión y recepción de signos, señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos. (Resolución MinTIC 202 de 2010).

TI: Tecnologías de la información.

TIC (Tecnologías de la Información y las Comunicaciones): Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ley 1341/2009 TIC)

Zombies: Nombre que se da a los ordenadores que han sido infectados de manera remota por un usuario malicioso con algún tipo de software que, al infiltrarse dentro del propio ordenador manipulado y sin consentimiento del propio usuario, un tercero puede hacer uso del mismo ejecutando actividades ilícitas a través de la Red. (Instituto Nacional de Tecnologías de la Comunicación España - INTECO – CERT).

SIGLAS INSTITUCIONALES

CCD: Centro de Excelencia para la Cooperación en Ciberdefensa.

CCIT: Cámara Colombiana de Informática y Telecomunicaciones.

CCOC: Comando Conjunto Cibernético.

CCP: Centro Cibernético Policial.

CICTE: Comité Interamericano Contra el Terrorismo.

COINFO: Comisión Intersectorial de Política y Gestión de Información en la Administración Pública.

ColCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Ministerio de Defensa de Colombia).

CONPES: Consejo Nacional de Política Económica y Social.

CRC: Comisión de Regulación de Comunicaciones.

DAS: Departamento Administrativo de Seguridad.

FIRST: Forum on Incident Response Teams

FBI: Federal Bureau of Investigation (Oficina Federal de Investigación

IEC: International Electrotechnical Commission (Comisión Electrotécnica Internacional).

ISO: International Organization for Standarization (Organización Internacional de Normalización).

MDN: Ministerio de defensa Nacional.

MinTIC’s: Ministerio de Tecnologías de la Información y las comunicaciones.

OEA: Organización de los Estados Americanos.

OTAN: Organización del Tratado del Atlántico Norte.

UIT: Unión Internacional de Telecomunicaciones.

UNESCO: United Nations Educational, Scientific and Cultural Organizational (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura).